ESCOLA DE DIREITO DE SÃO PAULO FUNDAÇÃO GETULIO VARGAS

Vitor Honofre Bellotto

PRESSUPOSTOS DO TRATAMENTO DE DADOS PESSOAIS EXTRAÍDOS DE SMARTPHONES PARA FINS DE PERSECUÇÃO PENAL À LUZ DA DOGMÁTICA CONSTITUCIONAL

Versão intermediária da dissertação como requisito parcial para aprovação no Mestrado Profissional em Direito Penal Econômico, da Escola de Direito de São Paulo da Fundação Getulio Vargas.
Data: 26.09.2024

Orientadora: Profa. Dra. Heloisa Estellita

São Paulo
2024

LISTA DE ABREVIATURAS

ANPD	Agência Nacional de Proteção de Dados
ART	Artigo
CC	Código Civil
CPC	Código de Processo Civil
CPP	Código de Processo Penal
CP	Código Penal
CF/88	Constituição Federal
DPO	*Data Protection Officer*
LGPD	Lei Geral de Proteção de Dados
LIT	Lei de Interceptações Telefônicas
MCI	Marco Civil da Internet
STJ	Superior Tribunal de Justiça
STF	Supremo Tribunal Federal

1. Problema

Apontar as bases normativas existentes para o tratamento de dados pessoais no processo penal e a aplicabilidade ou não à coleta forçada de dados pessoais - sigilos ou não - extraídos de smartphones apreendidos no contexto de investigações criminais e ações penais. Em razão da aparente incompatibilidade entre os marcos normativos existentes e tal medida interventiva, a pesquisa também se ocupa de apresentar quais pressupostos mínimos deveriam ser atendidos de *lege ferenda* para assegurar o direito fundamental à proteção de dados pessoais em face do recorte, isto é, dados obtidos de smartphones no contexto de uma persecução penal.

2. Desafios do tema proposto

Introduzir a linguagem da proteção de dados de outros marcos normativos, como a LGPD e o Regulamento Europeu de Proteção de Dados, para o ambiente do processo penal, bem como a relação entre medidas probatórias de caráter interventivo em direitos fundamentais com os direitos de titulares e limitações ao tratamento de dados pessoais para fins de investigação criminal. A existência de pouco material dogmático com essa abordagem interdisciplinar é um dos desafios centrais do tema.

3. Explicação justificada e fundamentada do provável conteúdo de cada capítulo com a respectiva bibliografia preliminarmente selecionada.

O primeiro capítulo aborda, inicialmente, a dogmática constitucional da intervenção em direitos fundamentais, admissível quando fundada em lei aliada a um juízo de proporcionalidade em face a outros valores de hierarquia constitucional. Em seguida, desenvolvemos a ideia de que a proteção de dados pessoais é direito fundamental que abrange não só os dados sob sigilo, mas quaisquer informações sobre pessoa natural identificada ou identificável, em que pese a regulamentação do acesso a tais tipos de dados esteja ligada a requisitos mais ou menos intensos previstos na legislação infraconstitucional. Enfim, analisamos o quadro infraconstitucional, o que se entende imprescindível para abordar o problema central da pesquisa, porquanto diferentes níveis de tratamento e pressupostos exigidos em diferentes leis a respeito de dados de natureza distinta, podem, em princípio, conduzir à conclusão de que o acesso

a tais dados em aparelhos celulares estará sujeito a maior ou menor necessidade de justificação, ainda que sob o amparo de autorização judicial.

No segundo capítulo, apresentamos a ideia de *hacking* governamental, que pode ser desenvolvida, fundamentalmente, em duas frentes: acesso remoto a dispositivos informáticos e acesso forçado a dados de dispositivos informáticos apreendidos por meio de softwares que rompem as barreiras de segurança, limitando-se o trabalho à segunda hipótese, que contempla smartphones apreendidos no contexto de uma persecução penal. Em seguida, testamos a compatibilidade normativa do instituto da busca e apreensão com tal medida intrusiva, bem como a possibilidade de que seja utilizada no processo penal, a despeito de previsão, com base num suposto poder geral de cautela do juiz criminal.

Por fim, no terceiro capítulo apontamos que há um aparente antagonismo entre as visões que defendem o tratamento de dados para uma melhor e mais eficiente prestação de serviços públicos, incluindo o processamento de infrações penais, de um lado, e a proteção da privacidade e dos dados pessoais, de outro. A superação dessa dicotomia depende da criação de regras claras quanto às possibilidades de tratamento legítimo para fins de persecução penal dos dados obtidos de aparelhos de telefonia móvel. Abordamos a edição de ato normativo que contemple, no mínimo, os requisitos discriminados item a item, conforme consta do sumário.

4. Estágio atual da pesquisa

A dissertação já possui introdução e todos os capítulos foram concluídos, estando pendente a elaboração de conclusão com a retomada das conclusões parciais e do caso hipotético apresentado na introdução.

5. Cronograma de trabalho

Elaborar a conclusão do trabalho e realizar os ajustes sugeridos pelos avaliadores em até 90 dias de realização da banca de qualificação, em caso de aprovação.

ANEXO I

VERSÃO PRELIMINAR

Sumário

INTRODUÇÃO 9

1. PANORAMA DO TRATAMENTO DE DADOS PESSOAIS NO PROCESSO PENAL 13

1.1. A dogmática constitucional de intervenção em direitos fundamentais 14

1.1.1. A reserva legal e o imperativo de determinação e clareza 15

1.1.2. O princípio da proporcionalidade 17

1.1.3. A separação informacional de poderes e as atividades de persecução penal em matéria de tratamento de dados pessoais 19

1.2. Superação da dicotomia existente entre os dados em fluxo e dados estáticos e o alcance da garantia inscrita no art. 5º, XII, da Constituição Federal 20

1.3. A proteção dos dados pessoais como direito fundamental autônomo. 23

1.3. O tratamento de dados pessoais na legislação infraconstitucional. 27

1.3.1. A lei de interceptações telefônicas e telemáticas. 27

1.3.2. O Marco Civil da Internet 28

1.3.3. Proteção de dados cadastrais e disposições especiais esparsas: art. 15 da Lei nº 12.850/13, art. 17-B da Lei nº 9.613/96 e arts. 13-A e 13-B do CPP. 30

1.3.4. Devido processo informacional e reflexos da LGPD no tratamento de dados para fins penais. 33

1.4. Síntese parcial 38

2. A busca e apreensão no contexto da extração forçada de dados 40

2.1. Medidas probatórias na Convenção de Budapeste e internalização de tratados interventivos em direitos humanos 43

2.2. A busca e apreensão de dados e elementos informáticos 45

2.2.1. Os limites da busca e apreensão 48

2.2.1.1. O conceito de domicílio: (im)possibilidade de equiparação ao smartphone 53

2.3. Encontro fortuito de provas na busca e apreensão virtual de dados pessoais e a doutrina da visibilidade imediata 56

2.4. O poder geral de cautela e os meios atípicos de produção de prova no processo penal 58

2.5. Síntese parcial 60

3. Pressupostos de lege ferenda para o acesso a dados armazenados em smartphones apreendidos 62

3.1. Edição de lei prévia 62

3.1.1. Hipóteses de cabimento à luz do princípio da proporcionalidade 63

3.1.2. Responsabilidades dos agentes responsáveis pelo tratamento de dados 64

3.1.2.1. O controlador e o operador de dados 64

3.1.2.2. O encarregado de dados e a figura do *Data Privacy Officer*..... 66
3.1.3. Direitos do titular de dados pessoais afetado 68
3.1.4. Regras de anonimização e pseudoanonimização de dados pessoais..... 69
3.1.5. Regras de compartilhamento e eliminação dos dados 69
3.1.6. Cadeia de custódia da prova digital decorrente de dados extraídos de aparelhos de celular . 72
3.2. Síntese parcial 76
Conclusão 78
REFERÊNCIAS 79

INTRODUÇÃO

Imagine-se que determinado órgão da Polícia Judiciária, no âmbito de uma investigação de cartel de empresas conluiadas para fraudar licitações para a realização de obras viárias em uma grande metrópole brasileira, obtém autorização judicial para empreender busca na sede das empresas e nos endereços residenciais dos respectivos representantes legais, na condição de investigados. O mandado judicial autoriza, além da apreensão de dispositivos informáticos, como computadores portáteis, tablets e, sobretudo, celulares localizados em posse das pessoas alvo da operação, que a autoridade policial encaminhe os objetos à Polícia Científica, que poderá fazer uso das tecnologias disponíveis para o acesso aos perfis de usuários e extração forçada – isto é, sem que tenha sido fornecida a senha, de forma voluntária e consentida, pelos suspeitos - de todos os dados pessoais julgados pertinentes e relacionados aos fatos em apuração, incluindo comunicações privadas armazenadas em serviços de mensageria instantânea e correspondência eletrônica, histórico de localização dos aparelhos, arquivos de áudio, texto e vídeo em sistemas de armazenamento do tipo *cloud* etc.

A partir do material obtido e examinado, foi possível estabelecer vínculos entre os suspeitos, mediante conversas mantidas entre si, troca de minutas de propostas de preço para as licitações combinadas, visita de uns ao local de trabalho dos outros para reuniões, agenda de contato comum e outros elementos confirmadores da materialidade e autoria delitivas, o que resultou no oferecimento de denúncia. Além disso, o Ministério Público requisitou o compartilhamento de todos os dados pessoais do sócio X da empresa Y com a Receita Federal do Brasil, diante de indícios de que diversos bens pessoais de alto valor não constam das suas declarações de imposto de renda, para melhor apuração pelo ente fiscal e constituição do crédito tributário previamente à persecução do delito tributário material.

No curso do processo, as defesas questionaram a licitude da prova, ao argumento de que a autorização judicial extrapolou os limites democraticamente estipulados às medidas interventivas no processo penal, diante da ausência de previsão legal expressa para a extração forçada de diversos tipo de dados pessoais. Além disso, que o uso de ferramenta tecnológica adquirida de empresa privada não estabelecida no país – e cujos processos internos não são públicos nem auditáveis - com a qual os dados pessoais

podem ter sido compartilhados no ato de extração, fere os princípios da prevenção e da segurança, por meio de medidas administrativas e tecnológicas, desde a concepção do sistema de tratamento de dados (*privacy by desing*), o que não permitiria garantir a integridade e confidencialidade dos dados tratados.

O Tribunal de Justiça, em sede de apelação, manteve as condenação proferida com base em tais elementos aos argumentos de que (i) cabe ao Judiciário o exame de proporcionalidade, razoabilidade e adequação da medida, o que foi realizado no caso concreto; (ii) a medida está contemplada e é decorrência lógica da apreensão validamente autorizada; e (iii) ainda que assim não fosse, o poder geral de cautela garantido ao juiz criminal, mediante aplicação por analogia do CPC, permite a criação de medidas interventivas atípicas complementares aquelas legalmente tipificadas, como a busca e apreensão, a interceptação telefônica e telemática, o afastamento do sigilo dos registros de acesso e dados cadastrais; (iv) a respeito da alegação feita pelo sócio X da empresa Y - de que o compartilhamento de dados com a RFB, além de decorrer de obtenção ilegal, fere os princípios da proporcionalidade e finalidade previstos na Lei Geral de Proteção de Dados, que as disposições da Lei nº 13.709/18, conhecida como “Lei Geral de Proteção de Dados”, instituiu expressa hipótese de não incidência às atividades de investigação e repressão de infrações penais, motivo pelo qual as bases legais de tratamento.

A problemática do caso acima reflete as práticas atualmente institucionalizadas e difundidas nos órgãos de persecução penal voltados ao combate da criminalidade organizada, e cuja característica é de uso preferencial aos métodos ocultos e, geralmente, tecnológicos de investigação em detrimento das diligências policiais tradicionais. Em um cenário de uso massivo de smartphones no ambiente corporativo, as evidências geradas por aplicações de comunicação instantânea (WhatsApp, Gmail, Telegram, WeChat), arquivos em nuvem (Office, Google Workspace, Dropbox, OneDrive, Sharepoint e outros) geram oportunidades singulares às agências de investigação. A partir do acesso aos dados pessoais gerados pelos usuários, seja de forma remota ou mediante acesso (e recuperação de arquivos) em dispositivos móveis, é possível o cruzamento de grandes volumes de informação, traçar perfis, estabelecer vínculos entre pessoas e empresas, o que invariavelmente representa um ganho de eficiência na

investigação e repressão de delitos complexos, sobretudo aqueles praticados em ambientes corporativos de difícil acesso.

Essas práticas inserem-se no que se tem convencionado chamar de hacking governamental, e envolve "o acesso não autorizado a dados mediante a exploração de alguma vulnerabilidade por agentes públicos em superação a mecanismos de segurança"[1]. Em particular, interessa desse fenômeno político-social a análise dos pressupostos e bases de legalidade para a obtenção de dados pessoais extraídos de dispositivos celulares apreendidos no contexto de investigações criminais, ainda que mediante autorização judicial prévia.

Mais especificamente, a presente dissertação identificará o arcabouço normativo-protetivo, na legislação infraconstitucional, do recém constitucionalizado direito à proteção de dados pessoais, inclusive em ambiente digital. O estudo parte (i) da premissas de que, em um regime democrático, a execução de medidas interventivas em direitos fundamentais, pelo Estado, condiciona-se à prévia autorização legislativa; (ii) da distinção entre normas de competência – para investigar e reprimir uma infração penal – e de autorização – para a realização de uma busca domiciliar ou um afastamento de sigilo bancário; e (iii) da hipótese preliminar de que, se não há expressa previsão de uma medida cautelar probatória, no processo penal, que autorize a extração forçada de dados de dispositivos móveis apreendidos, tal possibilidade estaria abarcada pelas medidas interventivas já existentes[2], ou ainda, se estaria sob o amparo ou pode ser considerada decorrência lógica da busca e apreensão judicialmente autorizadas.

Além disso, examinaremos se e em que medida as regras de proteção de dados pessoais existentes hoje na legislação, na pendência da edição de uma "LGPD Penal", aplicam-se às atividades de persecução penal para solucionar casos como o descrito preambularmente, considerando que o art. 4º, § 1º, da Lei nº 13.709/18, impõe a

---

[1] DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. Hacking Governamental: uma revisão sistemática. Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: <https://bit.ly/3YdVcIL>. P. 10.

[2] Exemplificativamente, a interceptação de dados telemáticos e afastamento de sigilo de registros de acesso e de dados cadastrais.

incidência do regime principiológico geral de proteção de dados também a tais atividades alheias ao escopo e regulação específica da lei.

1. PANORAMA DO TRATAMENTO DE DADOS PESSOAIS NO PROCESSO PENAL

É papel do Estado intervir em direitos fundamentais e, mais especificamente, em espaços individuais protegidos, para realizar fins que lhe incumbem, por exemplo, aqueles elencados no artigo 3º da Constituição Federal[3]. Para a consecução desses interesses estatais, que sucedem aos direitos individuais – e, com o perdão da tautologia, não são anteriores a eles, portanto -, entende-se necessária uma justificação especial para as atividades que gerem intervenção aos bens jurídicos e interesses constitucionalmente tutelados dos cidadãos. Isso porque, se de um lado, os direitos fundamentais não são absolutos, por outro, não podem ser violados, isto é, as intervenções a que estiverem sujeitos devem ser justificadas segundo normas substantivas que regulamentem e limitem o exercício do poder estatal.

Ainda assim, o avanço tecnológico desafia a proteção constitucional em vista dificuldades entre preservar a privacidade dos indivíduos e de conter as intrusões feitas pelo Estado, por corporações e por outros indivíduos. As novas tecnologias rastreiam os interesses dos indivíduos em suas compras, leituras, pesquisas e movimentos. Registram sua imagem facial, digitais, mensagens e dados pessoais em bases de dados de duração eterna e cujo uso ninguém pode antever integralmente. Nesse cenário, vigilância e segurança são frequentemente invocados como valores que preponderariam sobre a privacidade do indivíduo e sobre a proteção de seus dados pessoais, ainda que não sigilosos. A possibilidade de estabelecer programas de vigilância de indivíduos pelo governo com acesso à correspondência privada ainda está em definição, assim como a possibilidade de uso de dados de celular pelo governo federal para rastrear movimentos dos cidadãos e fazer prova do mais grave ao mais comezinho delito, é questão indefinida no Brasil e em outros países.

---

[3] Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil: I - construir uma sociedade livre, justa e solidária; II - garantir o desenvolvimento nacional; III - erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais; IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação. BRASIL. Constituição da República Federativa do Brasil. Promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 01 ago. 2024.

A Constituição protege o cidadão contra o rastreamento dos vestígios de seus movimentos, de seus dados, de sua correspondência e de suas opiniões pelo Estado. Esta proteção é importante para garantia da liberdade de pensamento, de expressão, de opinião e de reunião. Sem uma causa provável da prática de um ilícito, todo indivíduo está protegido de busca pessoal pelo Estado.

O acesso a dados pessoais extraídos de telefones celulares apreendidos no contexto de um procedimento criminal é, inegavelmente, uma intervenção relevante em direitos fundamentais, em especial, à intimidade e ao sigilo das comunicações privadas e, inclusive, ao próprio direito à proteção de dados pessoais enquanto direito autônomo que traz uma série de implicações em relação às formas de obtenção, tratamento e eliminação dos dados, como veremos no decorrer desta dissertação.

1.1. A dogmática constitucional de intervenção em direitos fundamentais

A legitimidade de determinada intervenção deve se sujeitar aos estritos limites da autorização democrática, pois é o povo que escolherá o que o Estado pode ou não fazer. Disso decorre importante distinção a ser feita entre as normas autorizativas e normas de competência, sintetizada na máxima “de competências não se derivam autorizações”, para expressar que enquanto as normas de competência conferem atribuições às instituições de estado (por exemplo, à Polícia Judiciária a atribuição de investigar crimes), as normas de autorização são aquelas que autorizam intervenções em direitos fundamentais[4].

Nessa ordem de ideias, atividades de levantamento e de compartilhamento de dados pessoais têm por pressuposto que as informações reveladas pelos dados se encontrem no âmbito de proteção de direitos de jaez constitucional, e sujeitam-se a três requisitos: a) a reserva de lei; b) a proporcionalidade entre os meios utilizados pelo

[4] GRECO, Luís. O inviolável e o intocável no direito processual penal: considerações introdutórias sobre o processo penal alemão (e suas relações com o direito constitucional, o direito de polícia e o direito dos serviços de inteligência), in WOLTER, Jurger. O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal: organização e tradução Luís Greco; tradução Alaor Leite, Eduardo Viana - 1ª ed. - São Paulo: Marcial Pons, 2018, p. 36 e ss.

Estado na intervenção de direitos fundamentais e os fins perseguidos; e c) a separação informacional dos poderes.

1.1.1. A reserva legal e o imperativo de determinação e clareza

O princípio da reserva legal está previsto no artigo 5º, II, da Constituição Federal e dele se extrai a exigência de reserva de lei qualificada para justificar intervenções em direitos fundamentais com o propósito de atender finalidades legítimas. São exemplos a exceção ao sigilo de dados e das comunicações telefônicas e telemáticas para fins de investigação criminal, nos termos da legislação ordinária (art. 5º, XII, CF[5]) e a busca e apreensão, que mitiga a inviolabilidade do domicílio, em havendo ordem judicial fundamentada (art. 5º, XI, CF[6]). Os critérios para as regras especiais de autorização serão abordados no decorrer do trabalho.

Os dados pessoais, inclusive nos meios digitais, também são constitucionalmente protegidos como direitos fundamentais (art. 5º, LXXIX, CF), como garantia ao livre desenvolvimento da personalidade. Da mesma forma que a vida, a liberdade individual, e a integridade corporal, o direito à proteção de dados pessoais integra uma esfera de proteção normativa com relação à qual o Estado tem um dever geral de abstenção. Isso equivale a dizer que a proteção aos dados pessoais tem aplicação imediata e que, como regra, tal direito não poderá se sujeitar a intervenções que não estejam expressamente previstas em lei. Em outras palavras, considerando que os direitos fundamentais que asseguram as liberdades individuais – incluindo a autodeterminação informacional e a prerrogativa de decidir sobre o uso os próprios dados - refletem valores antecedentes aos interesses estatais, o Estado tem o dever de justificação especial para os atos de intervenção em tais direitos.

Logo, sendo o povo, por intermédio do Parlamento, o ente legitimado a definir o que o Estado – sob a conformação de Estado Democrático de Direito - pode ou não fazer, mediante o reconhecimento de direitos fundamentais na Constituição e as exceções que

---

[5] BRASIL. Constituição da República Federativa do Brasil. Promulgada em 5 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 1 ago. 2024.
[6] *Idem*.

atendam a outros interesses circunstanciais, ganha importância o conceito de normas autorizativas (art. 5º, II, CF[7]). Por meio das normas autorizativas, o Parlamento autoriza intervenções em direitos fundamentais para atender a finalidades legítimas e socialmente desejadas (como a persecução de condutas que atentem contra bens jurídicos penalmente tutelados). Duas consequências podem ser extraídas: em primeiro lugar, normas que instituem competências, como a de investigar delitos pela Polícia Judiciária (art. 144, § 2º, CF), não deflagram normas autorizativas automaticamente. Em segundo lugar, não se admite atos normativos outros que não a lei em sentido estrito, como portarias, resoluções, regulamentos, eis que não há autorização constitucional para agentes não parlamentares criarem medidas interventivas à margem do processo democrático. Não fosse assim, "a existência de direitos fundamentais reduzir-se-ia a nada, possibilitando a qualquer agente estatal realizar juízo próprio sobre a ponderação de seus interesses em relação a direitos alheios"[8].

A Lei Geral de Proteção de Dados brasileira, que será objeto de análise mais aprofundada adiante (1.3.4.), positivou uma lista de princípios, entre eles, o da licitude (art. 6º, I), cuja interpretação sob a ótica da proteção constitucional de dados pessoais, conjugada com a autodeterminação informacional enquanto direito fundamental, "não pode significar outra que não a exigência de reserva de lei". Essa rede principiológica e os efeitos que dela decorrem geram um modelo de persecução penal da "proibição com reserva de permissão"[9], sendo proibidas todas as medidas interventivas em direitos fundamentais não expressamente autorizadas e reguladas por lei [10] e,

---

[7] *Idem*.

[8] Cf. GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública - 1ª Ed - Rio de Janeiro: Marcial Pons, 2021, p. 43.

[9] *Ibid.*, p. 60/61.

[10] Em âmbito internacional, a Convenção Europeia de Direitos Humanos prevê, no art. 8º, n. 2, que quaisquer ingerências sobre a vida privada e outros direitos fundamentais devem estar previstas em lei. Segundo Weiblein, o TEDH interpreta lei em sentido amplo, incluindo a lei não escrita, como a existência de uma jurisprudência consolidada. Já a Convenção Americana de Direitos Humanos estabelece reserva legal para as hipóteses de restrição de liberdade, mas é possível extrair de precedentes da CIDH interpretação convergente à necessidade de reserva de lei: "Sobre interceptações telefônicas ilegais, já afirmou a Corte IDH, na linha do TEDH, que o direito à vida privada pode ser restringido, desde que não haja abuso ou arbitrariedade; logo as interferências "devem ser previstas em lei, perseguir uma propósito legítimo e atender aos requisitos de adequação, necessidade e proporcionalidade. Além disso". WEIBLEN, Fabrício Pinto. O uso de software espião na investigação criminal: interpretação aberta à tecnologia, (in)admissibilidade e tratamento jurídico adequado. Londrina, PR: Thoth, 2024, p. 42.

consequentemente, são insuficientes simples autorizações judiciais sem amparo em lei, apenas com base em um juízo de proporcionalidade feito caso a caso[11].

Ao princípio da reserva de lei, acopla-se o mandado de determinação e "qualidade da lei", consubstanciados na ideia de que quanto mais intensa a intervenção estatal no direito fundamental legalmente permitida, maior a necessidade de detalhamento normativo, a fim de que aos cidadãos seja assegurado saber em que circunstâncias e sob quais condições poderão ter seus direitos afetados para satisfazer determinado interesse estatal – como o de elucidar um crime -, bem como haja orientação suficiente aos agentes estatais para que guiar a conduta na aplicação da lei, bem como sujeitar os seus atos a controle judicial. Weiblein chama a atenção para entendimento do Tribunal Constitucional Federal alemão quanto à coexistência da regra da clareza da lei com as inovações tecnológicas, reconhecendo a possibilidade de que de meios de obtenção de prova sejam utilizados a partir de uma interpretação aberta da tecnologia. Assim, a intervenção do legislador somente será necessária quando tal método de interpretação não for suficiente para corrigir a situação. Já o TEDH aplica o preceito da *quality of law*, exigindo que a lei interventiva seja precisa, acessível e proporcional[12].

1.1.2. O princípio da proporcionalidade

A proporcionalidade "impõe exigências materiais à relação entre os meios de que se vale o Estado para a persecução de fins"[13], devendo essa relação ser proporcional. Derivam da ideia de proporcionalidade os demais princípios de tratamento de dados, como o da vinculação, o da necessidade de regramento específico para as distintas

---

[11] Compartilha dessa posição Weiblein, segundo o qual "toda a intervenção em direitos fundamentais demanda uma justificação, a qual tem, como primeiro pressuposto, um limite formal. *Ibid*., p. 40.

[12] Cf. Weinblein, os requisitos mínimos exigidos pelo TEDH para, por exemplo, a validade das interceptações de comunicações telefônicas no processo penal, consistem na previsão de a) hipóteses de admissibilidade da medida; b) pessoas afetadas por ela; c) prazo de duração e limites; d) procedimentos de preservação, análise e uso dos dados; e) medidas de precaução sobre o compartilhamento dos dados; e f) circunstâncias de eliminação dos dados. Tais pressupostos foram aplicados, por exemplo, no caso Huvig v. França, n. 11110584, de 24/04/1990. Idem, p. 47.

[13] Gleizer, *op. cit*., p. 49.

atividades estatais (persecução penal, segurança pública e inteligência), que veremos abaixo (1.1.3).

De acordo com a dogmática constitucional, a proporcionalidade – também referida na doutrina como princípio, máxima ou postulado – evoluiu como um mecanismo instrumental para aferir a legitimidade das restrições a direitos fundamentais em três etapas, nas quais se vai verificar:

> a *adequação* de uma medida para produzir determinado resultado (idoneidade do meio para realizar o fim visado), (ii) a *necessidade* da providência, sendo vedado o excesso (se houver meios menos gravosos para atingir o mesmo fim é ilegítimo o emprego do meio mais gravoso e (iii) a *proporcionalidade em sentido estrito*, pela qual se afere se o fim justifica o meio, vale dizer, se o que se ganha é mais valioso do que aquilo que se sacrifica[14].

Portanto, não basta que exista autorização legal para o levantamento de dados pessoais, mas que essa intervenção esteja calcada em finalidades determinadas, explícitas e legítimas. A Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/18), conquanto inaplicável as atividades de persecução penal no que diz respeito à regulamentação das atividades de tratamento de dados, ainda assim impõem a observância à principiologia normatizada, como veremos adiante (2.3.4). A LGPD previu os subprincípios da finalidade e da adequação (art. 6º, I e II[15]), que exprimem a ideia de que o tratamento de dados esteja vinculado a uma finalidade que revele propósitos legítimos, específicos e informados ao titular.

Ainda sob o manto da proporcionalidade, a LGPD também consagra o critério da necessidade (art. 6º, III[16]), que tem por vetor a limitação das intervenções em direitos fundamentais aos meios menos gravosos, o que significa dizer que, em matéria de proteção de dados pessoais, o levantamento e armazenamento de dados irrelevantes ou impertinentes para a persecução penal gera impactos desproporcionais à esfera privada do cidadão.

---

[14] BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo - 8. ed. - São Paulo: Saraiva, 2019, p. 512.
[15] BRASIL. Lei no 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados brasileira (LGPD). Disponível em: <http:// www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 4 dez. 2023.
[16] *Idem*.

1.1.3. A separação informacional de poderes e as atividades de persecução penal em matéria de tratamento de dados pessoais

As atividades de persecução penal, segurança pública e inteligência são funções estatais distintas, cujas estruturas e fundamentos de legitimidade são, igualmente, particulares. É premissa fundamental ao desenvolvimento do presente trabalho, portanto, a adequada distinção entre tais atividades, a fim de que possamos compreender de maneira específica como a problemática do tratamento de dados pessoais obtidos de telefones celulares apreendidos se apresenta em relação às regras de processo penal, que regulamentam as atividades de persecução penal.

Em linhas gerais, "a persecução penal está voltada para a confirmação de uma suspeita"[17]. A ideia fundamental por trás da atividade investigativa de persecução penal é, em retrospectiva, reconstruir um fato pretérito tipificado em lei como infração penal, viabilizando o exercício do direito punitivo estatal contra o autor de tal fato, em resposta à violação do bem jurídico penalmente tutelado. Como bem apontam Gleizer, Montenegro e Viana, é possível estabelecer um limite claro às intervenções em direitos fundamentais geradas pela atividade em questão: inexistindo qualquer suspeita factualmente fundada, não estão os órgãos de persecução penal autorizados iniciar investigações nem a impor restrições a direitos fundamentais dos cidadãos[18].

A persecução penal se distingue da segurança pública na medida em que os órgãos que compõem esta última têm por função a proteção contra perigos, numa orientação preponderantemente prospectiva. A finalidade é de prevenção a danos causados contra bens jurídicos ou que a lesão contra eles seja tão logo cessada. Por sua vez, o limite à atividade de segurança pública é a existência de um perigo, sem o qual não se justificam autorizações interventivas aos órgãos de segurança pública[19].

Finalmente, as atividades desenvolvidas pelos serviços de inteligência, como o Conselho de Controle de Atividades Financeiras (COAF) no Brasil, vinculado ao Banco Central, têm por finalidade "a coleta e a análise de informações necessárias para

---

[17] Gleizer, *op. cit.*, p. 52.
[18] *Ibid.*, p. 53
[19] *Ibid.*, p. 53.

antecipar-se a perigos ou formular políticas de segurança interna ou externa”[20]. Os órgãos de inteligência atuam, portanto, num cenário anterior à existência de perigos e de suspeitas, voltando-se à precaução – o que gera, no entendimento da doutrina, uma dicotomia entre as amplas possibilidades de atuação para além dos limites interventivos da persecução penal e da segurança, e a maiores restrições a nível de intervenções de caráter informacional traduzidos pela máxima de “quem detém muito conhecimento, deve ter o poder restringido”[21].

A existência de finalidades específicas para cada uma dessas atividades levou ao desenvolvimento, pelo direito alemão, do chamado princípio da separação informacional, já constitucionalmente reconhecido enquanto derivação do direito à autodeterminação informacional. Esse princípio, além de fundamentar a distinção entre a persecução penal, a segurança pública e as atividades de inteligência, impõe que o compartilhamento de informações entre os órgãos integrantes de cada uma delas seja a exceção, e não a regra. Mais do que isso, as exceções devem ser expressa e claramente regradas em normas de autorização, devidamente limitadas, na medida em que o desvio de finalidade no tratamento de dados originalmente autorizado para uma finalidade específica constituí nova intervenção no direito fundamental afetado, devendo ser normativamente justificado à luz dos critérios de proporcionalidade acima trabalhados (2.1.2).

1.2. Superação da dicotomia existente entre os dados em fluxo e dados estáticos e o alcance da garantia inscrita no art. 5º, XII, da Constituição Federal

O art. 5º, XII, da Constituição Federal, instituiu a garantia ao sigilo das comunicações, que é excepcionado para fins de investigação criminal, nos termos da Lei nº 9.296/96, editada para regulamentar a matéria. O entendimento doutrinário

[20] *Ibid*., p. 54
[21] *Ibid*., p. 54.

predominante[22], que também encontra eco em decisão do Supremo Tribunal Federal[23], é no sentido de que (i) a proteção do inciso XII do art. 5º não se refere ao conteúdo das informações comunicadas em correspondências, mensagens telegráficas, dados e telefonemas em si, mas sim à sua comunicação, isto é, ao seu fluxo enquanto ocorrem; e que (ii) apenas o sigilo da comunicação por telefonia, enquanto está em fluxo, poderia ser restringido para fins de investigação criminal e instrução processual penal, não se estendendo essa possibilidade para o fluxo de dados, telegrafias e cartas.

O escopo de incidência é restrito às interceptações telefônicas e telemáticas, ou seja, diz respeito às comunicações em tempo real, enquanto se realizam, e não as comunicações já realizadas e armazenadas ou gravadas. A grande controvérsia que esse entendimento suscita atualmente decorre do fato de que ficam excluídos do âmbito de proteção do sigilo das comunicações o conteúdo já armazenado, registrado ou gravado, razão pela qual há autores que sustentam interpretações mais elásticas do dispositivo constitucional. A principal razão é a quantidade massiva de dados de comunicação que passou a ser armazenada em serviços de mensageria eletrônica, instantânea, sistemas de armazenamento em nuvem ou nos próprios dispositivos informáticos, como computadores, tablets e smartphones.

Isso porque, diferentemente das comunicações realizadas por meio de ligações telefônicas, que pela própria natureza são instantâneas, as comunicações eletrônicas, realizadas por meio de troca de e-mails, mensagens instantâneas, mensagens em áudio etc. deixam registros e podem ser armazenadas pelos interlocutores[24]. A obtenção de mensagens realizadas por meios eletrônicos pode, portanto, ser realizada tanto de forma

---

[22] O Texto do professor Tércio Sampaio Ferraz Júnior foi, desde a sua publicação, uma referência no assunto. FERRAZ JR., Tercio Sampaio, Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado, in: Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, 1993, p. 439-459.

[23] No julgamento do Recurso Extraordinário 418.416-8/SC, de 10/05/2006, o Min. Rel. Sepúlveda Pertence afirma que a proteção do inciso XII do art. 5º não se refere às informações comunicadas em correspondências, mensagens telegráficas, dados e telefonemas em si, mas à comunicação, ao fluxo das mesmas enquanto ocorrem. BRASIL. Supremo Tribunal Federal. RE 418416, Tribunal Pleno, Relator Ministro Sepulveda Pertence, julgado em 10/05/2006, publicado em 19/12/2006.

[24] QUITO, Carina. Acesso a comunicações eletrônica armazenadas na prática judiciária. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (Ed.). Direitos fundamentais e processo penal na era digital: doutrina e prática em dabate [livro eletrônico]. São Paulo: InternetLab, 2022, p. 100-107.

instantânea quanto por meio da apreensão de conteúdos armazenados pelos usuários de aplicações de internet em suas contas ou na memória de dispositivos informáticos.

O anacronismo desse tratamento normativo conferido aos dados em fluxo e aos dados estáticos, e a necessidade de superação dessa dicotomia foram bem explorados por Souza Abreu em recente publicação, em que demonstra existir sobre todo e qualquer dado a tutela sob o manto da privacidade, não bastando a existência de lei prévia ou autorização judicial, mas a aplicação de critérios substantivos calcados na ideia de proporcionalidade e finalidade pretendidos com a medida interventiva[25]:

> Nesse sentido, além do abandono de testes binários para tratar da proteção constitucional, deve ser resgatada a noção de que o ônus de fundamentação para agir é do Estado, que precisa justificar que não está atuando arbitrariamente, descuidadamente, nem em excesso. Isso vale mesmo no combate ao crime – ser fundamentado, dentro das prerrogativas de um estado constitucional, afinal, é o que autoriza o monopólio do Estado do uso da força. O que pode ser feito em situações de normalidade ou de urgência, em um flagrante no policiamento ostensivo, na apreensão de objeto largado em cena de crime, no âmbito de uma medida cautelar em uma grande investigação, diretamente pelas autoridades ou por meio de empresas, para implementação de uma política pública, pode variar. A medida do que consideramos mais ou menos grave e interventivo e quais cuidados e protocolos requer, também. Os contextos importam. Nossas respostas regulatórias devem responder às preocupações com arbitrariedades, negligências e excessos de cada um deles: autorizações judiciais prévias que controlem a justa causa e o limite de restrição são, em muitos casos, vocacionadas a garantir salvaguardas, mas não necessariamente são aptas a lidar com todos os contextos ou a lidar com todas as preocupações. Na era da vigilância baseada em coleta massiva de dados, de políticas de segurança cada vez mais preventivas e preditivas, outras ferramentas voltadas a embutir salvaguardas e limites também terão de ser consideradas, ao lado do resgate do papel da reserva legal.

Para ela, esse teste binário causa estranheza na medida em que há natural expectativa de privacidade, por exemplo, em relação aos registros telefônicos que mantemos armazenados em nossos aparelhos celulares, assim como aos sítios eletrônicos que acessamos, cuja obtenção e tratamento de tais informações, em determinados contextos, acarreta maior exposição à vida íntima do sujeito de direitos que

[25] ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. Revista de Investigações Constitucionais, Curitiba, vol. 11, n. 1, e256, jan./abr. 2024. DOI: 10.5380/rinc.v11i1.89280, p. 23.

a própria interceptação do ato de se comunicar enquanto o processo comunicante ocorre[26].

Como veremos a seguir (2.3), a constitucionalização do direito à proteção de dados pessoais, inclusive nos meios digitais, reforça as críticas de Souza Abreu – às quais ora aderimos -, justificando que o novo paradigma da proteção de dados pessoais volte as atenções muito mais ao conteúdo das informações reveladas do que à forma em que os dados se encontram no espaço e no tempo, se em fluxo ou armazenados.

1.3. A proteção dos dados pessoais como direito fundamental autônomo

No que toca aos meios de obtenção de prova atualmente mais utilizados na persecução penal, a quebra de sigilo de dados[27], seja remotamente ou mediante o acesso a dispositivos móveis, a primeira ação estatal que demanda autorização é o levantamento de dados, que se subsume no conceito de tratamento de dados pessoais sob a denominação de coleta, nos termos do artigo 5º, X, da Lei nº 13.709/18. A regulação dessa atividade deve ser objeto de especial tratamento das normas de persecução penal. As atividades sucessivas ao levantamento, como a utilização, a transferência, o armazenamento e o descarte constituirão intervenções autônomas a demandar justificação específica.

A EC nº 115/2022 introduziu o inciso LXXIX ao rol de direitos e garantias fundamentais do art. 5º da Constituição Federal, assegurando, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais, a partir do qual se extraí a

---

[26] Nas palavras da autora "O paradigma de proteção constitucional reduzido a um teste binário do que está em fluxo ou não acaba por fundamentalmente facilitar a obtenção e uso dessas informações nos mais diversos contextos, dispensando até a exigência de observâncias a requisitos materiais – como discussão sobre indícios e causa provável – e a parâmetros de proporcionalidade vinculados a uma análise do contexto. Torna novas e inovadoras medidas de investigação, nunca tratadas em lei, uma não-questão, como se não merecessem maior debate. Na prática, isso significa uma erosão de direitos à privacidade. *Ibid*, p. 13.

[27] O relatório de transparência da Google, por exemplo, revela que no ano de 2022, foram realizadas 23.651 solicitações de acesso a dados de usuários de serviços da empresa, atingindo quase 100.000 contas. Disponível (on-line) em: <https://transparencyreport.google.com/user-data/overview?hl=pt&user_requests_report_period=series:requests,accounts;authority:BR;time:&lu=user_requests_report_period>. Acesso em: 24 set. 2023.

noção de autodeterminação informativa[28]. Conquanto o tema seja compatível com um estudo próprio, a proteção de dados não equivale a assegurar o sigilo desses dados, daí porque os contornos do direito à proteção não necessariamente convergem com o direito à intimidade ou ao sigilo das comunicações privadas, tendo em vista que as operações que envolvem o tratamento de dados pessoais já são objeto de regramento e compõem o microssistema da proteção de dados pessoais, ao que se ligam outras questões como agentes de tratamento, bases legais e consentimento do titular, medidas administrativas e tecnológicas que impeçam vazamentos ou tratamento abusivo, sem descuidar do fato de que muitos dos dados pessoais objeto de tratamento, inclusive no contexto de uma investigação criminal, são públicos.

Ao cidadão deve se conferir o controle sobre as próprias informações, bem como o direito de conhecer quem, quando e como as acessa e para quais finalidades legítimas. Dessa concepção decorrem duas importantes consequências, conforme aponta Pedro Amaral. A primeira, de que as operações de tratamento de dados realizadas por agentes estatais em rotinas de investigação sejam norteadas por sólida principiologia, composta ao menos pela finalidade, necessidade, qualidade dos dados, transparência, segurança, prevenção e prestação de contas, o que será mais bem aprofundado durante este capítulo. Em segundo lugar, que a legislação infraconstitucional e regulamentos que vierem a ser editados para normatizar procedimentos de acesso a dados pessoais para fins de investigação devem partir da premissa de que a salvaguarda do direito fundamental não tem uma dimensão apenas individual, mas coletiva em vista do número potencial de titulares de dados afetados por operações de coleta e tratamento com tal finalidade[29].

---

[28] De acordo com Rebelatto: “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 conferido a cada cidadão de ter, sob seu controle, as 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.” Cf. REBELLATO, Luiz Fernando Bugiga. A análise constitucional do sigilo e da privacidade nas investigações criminais: o acesso a dados armazenados em aparelhos celulares. Dissertação (Mestrado – Programa de Pós-Gradução em Direito Processual) – Faculdade de Direito. Universidade de São Paulo, 2020. P. 24-25.

[29] AMARAL, Pedro Mercadores da insegurança [livro eletrônico]: conjuntura e riscos do hacking governamental no Brasil / Pedro Amaral, Mariana Canto, Marcos César M. Pereira; coordenação André Ramiro. --1. ed. -- Recife, PE : IP.rec, 2022. PDF.

Embora o conceito de dado pessoal aparente ser simples, enquanto qualquer informação que permita identificar uma pessoa natural (art. 5º, I, da LGPD[30]), há uma miríade de dados e informações coletadas pelos provedores de aplicações de internet e armazenadas nos próprios dispositivos móveis, cada qual com um nível particular de relevo e potencial de afetação da intimidade. Pense-se, por exemplo, em dados de geolocalização, que, por si próprios, podem gerar percepções – nem sempre corretas – quanto às preferências religiosas, compras e estado de saúde de uma pessoa. Esse tipo de informação muitas vezes revelará mais informações que dados cadastrais contendo o nome e documentos pessoais – e que nem por isso são desprovidos de tutela legal específica. Igualmente, a extração de dados de celulares pode revelar informações de caráter comunicacional, como conversas em aplicativos de mensageria e e-mails, além de informações profissionais, razão pela qual Perez alerta para a potencial intervenção em múltiplos direitos fundamentais do titular:

> La cantidad y la calidad de información que contienen los dispositivos de almacenamiento masivo hace que resulten implicados diferentes derechos fundamentales. Estos dispositivos pueden contener información, datos sobre la vida personal y profesional de su titular pero, además, conversaciones o comunicaciones con otras personas. Así, estarían afectados el derecho a la intimidad o a la vida privada y el derecho al secreto de las comunicaciones junto con el derecho a la protección de los datos personales[31].

A autora espanhola ainda esclarece que, conquanto o Tribunal Constitucional de seu país tenha tentado segregar o conteúdo de cada direito fundamental afetado, muitas vezes eles estarão entrelaçados em razão do volume de dados contidos nos dispositivos de armazenamento. Assim, ainda que os dados pessoais individualmente considerados pudessem apresentar-se irrelevantes para a sua tutela jurisdicional, o tratamento conjunto desses dados justifica o reconhecimento de uma proteção especial na medida

---

[30] BRASIL. Lei no 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados brasileira (LGPD). Disponível em: <http:// www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 04 dez. 2023.

[31] Pérez Estrada, M. J. (2019). La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. *Revista Brasileira De Direito Processual Penal*, *5*(3), 1297-1330. https://doi.org/10.22197/rbdpp.v5i3.253.

em que afeta a própria personalidade do indivíduo - no cenário espanhol, chamado de "derecho a la protección del próprio entorno virtual"[32].

No Brasil, Gloeckner desenvolveu o argumento de que a intimidade, no cenário do ciberespaço, deixou de corresponder ao mero "direito de estar só", passando a clamar por proteção contra a vigilância e a ingerência estatal, que se exprime na concepção de autodeterminação informativa como um corolário da própria condição de cidadania. Para ele, a capacidade massiva de armazenamento de informações pessoais que o telefone celular carrega, o qualificam como "uma extensão informacional da própria pessoa", cujo acesso pelos órgãos do Estado representa intervenção grave na esfera dos direitos de personalidade da pessoa. Conclui, nessa ordem de ideias, que a regulamentação conferida pela Lei nº 9.296/96, no que tange à interceptação de dados telemáticos e ao sigilo das comunicações privadas, é insuficiente para captar essa rede complexa de direitos invariavelmente afetados pelas modernas técnicas de acesso aos dados armazenados em dispositivos celulares[33].

Portanto, é necessário analisar o quadro infraconstitucional, o que se entende imprescindível para abordar o problema central da pesquisa[34]. Afinal, diferentes níveis de tratamento e pressupostos exigidos em diferentes leis a respeito de dados de natureza distinta, podem, em princípio, conduzir à conclusão de que o acesso a tais dados em

---

[32] O conceito do direito a proteção do próprio entorno virtual, cunhado para assegurar os direitos do art. 18 da Constituição Espanhola, compreende "toda a informação em formato eletrônico que, através do uso das novas tecnologias, seja de forma consciente ou inconsciente, voluntária ou involuntariamente, o usuário vai gerando, até o ponto de deixar um rastro suscetível de acompanhamento pelos poderes públicos". Trata-se de contemplar de forma unificada mensagens, imagens, documentos e, em geral, todos os dados reveladores do perfil pessoal, reservado ou íntimo de qualquer acusado" (tradução livre). *Ibid*., p. 1.311.

[33] Em arremate, alerta que "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". Cf. GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. Revista Brasileira de Ciências Criminais. Vol 156/2019, p. 6

[34] De acordo com Abreu, há uma série de leis no Brasil que regulam o acesso a dados pessoais, "cada um deles governado por níveis de sigilo diferentes, sob a presunção de que quão mais sensíveis os dados, maior deve ser a proteção". ABREU, Jaqueline. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel Ferreira; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (org.). Tratado de proteção de dados pessoais. Rio de Janeiro, RJ: Editora Forense, 2021. p. 583–603.

aparelhos celulares estará sujeito a maior ou menor necessidade de justificação, ainda que sob o amparo de autorização judicial.

1.3. O tratamento de dados pessoais na legislação infraconstitucional.

Para tanto, dividiremos a análise em três blocos, fundamentalmente: dados de comunicação, que via de regra sempre estarão associados a ao menos uma pessoa natural; metadados, que constituem os registros circunstancias de tempo e espaço de uma determinada comunicação ou uso de determinada aplicação de internet; e dados cadastrais e demais dados passíveis de identificação pessoal, passando, ao final do capítulo, pela principiologia atinente ao tratamento de dados pessoais prevista na LGPD e que serve de substrato para as atividades de persecução penal (art. 4º, § 1º)[35].

1.3.1. A lei de interceptações telefônicas e telemáticas.

Com referência às considerações tecidas no tópico 1.2., a respeito da necessária releitura da proteção constitucional conferida ao sigilo das comunicações e de dados telemáticos, acrescentamos que a operacionalização de medidas interventivas no processo comunicante e na própria obtenção do conteúdo comunicado, esteja ele em fluxo ou armazenado, foi regulada pela Lei nº 9.296/96[36].

No que toca ao aspecto procedimental, a Lei de Interceptações Telefônicas prevê que a execução da medida se dá mediante a cooperação das empresas de telecomunicações e das provedoras de aplicação de internet, e também mediante a

---

[35] BRASIL. Lei no 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados brasileira (LGPD). Disponível em: <http:// www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 04 dez; 2023.

[36] A respeito da questionada constitucionalidade da lei, Souza Abreu recorda que “Em 1996, a discussão que chegou ao STF foi a constitucionalidade da previsão de interceptação telemática, estabelecida no parágrafo único do art. 1º da Lei nº 9.296/96 (Lei de Interceptações).26 Nesse caso, o segundo aqui destacado, a controvérsia seria reconhecida explicitamente. A Associação dos Delegados de Polícia do Brasil propôs a ADI 1.488, com pedido liminar para suspender o dispositivo – por “atentar contra a inviolabilidade do sigilo das comunicações no âmbito do processamento de dados (art. 5º, inciso XII, C.F.), inadmissível como prova (art. 5º, inciso LVI, C.F.)”. O receio era de que essa possibilidade “resultará em laudos de degravação de computadores que, no caso concreto, ocorrerá sempre ao arrepio da garantia de inviolabilidade da intimidade das pessoas (art. 5º, inciso X, C.F.)”. O pedido liminar foi julgado pelo Plenário no mesmo ano”. ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. Revista de Investigações Constitucionais, Curitiba, vol. 11, n. 1, e256, jan./abr. 2024. DOI: 10.5380/rinc.v11i1.89280, p. 8.

instalação de grampos e escutas ambientais. Já o art. 2º da Lei nº 9.296/96 estabelece como requisitos para a decretação de interceptações telefônicas e telemáticas: (i) indícios razoáveis de autoria e participação; (ii) a inexistência de meios menos gravosos e (iii) a investigação de crime punido com reclusão[37].

Um primeiro questionamento que se faz sobre o alcance da lei em relação ao conteúdo armazenado guarda imediata relação com o fato de que o Marco Civil da Internet, como se verá adiante, não introduziu requisitos substantivos para a proteção de tais conteúdos. Além disso, a Lei de Interceptações Telefônicas não autorizou a extração de dados de celulares ou outros dispositivos móveis, cujo armazenamento, aliás, comumente abarcará mais do que os dados de comunicação – como agenda de contatos, geolocalização, dados de cartão de crédito, fotos e vídeos, notas etc. -, o que gera um segundo questionamento sobre o alcance da lei no que toca à legalidade e proporcionalidade de estender sua aplicação a forma interventiva em direito fundamental não expressamente autorizada.

1.3.2. O Marco Civil da Internet

A Lei nº 12.965/14, popularmente conhecida como Marco Civil da Internet, positivou as relevantes regras de proteção de dados pessoais num momento as discussões sobre o assunto ainda eram incipientes no Brasil. Entre os direitos e garantias dos usuários – hoje compreendidos como titulares de dados -, instituiu-se, no art. 7º a vedação de fornecimento de dados pessoais sem o seu consentimento[38], salvo as hipóteses previstas em lei (inciso VII)[39]. Também exigiu que as operações de coleta, uso, armazenamento e tratamento sigam o princípio da finalidade, de maneira que a coleta de ser (i) justificada; (ii) não vedada em lei ou (iii) prevista em contrato de prestação de serviço ou termos de uso de aplicações de internet (inciso VIII). Por fim, destaque para o

---

[37] BRASIL. Lei no 9.296 de 24 de julho de 1996. Lei de Interceptações Telefônicas e Telemáticas. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 04 dez. 2023.

[38] Base legal de tratamento que veio a ser reproduzida no art. 7º, I, da Lei nº 13.709/18.

[39] BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 13 out. 2023.

direito à exclusão de definitiva dos dados pessoais coletados por determinada aplicação de internet ao término da relação, ressalvadas as hipóteses de guarda obrigatória (inciso X).

Enquanto o art. 7º, II, das comunicações em fluxo, salvo por ordem judicial, na forma da lei, o art. 7º, III, da Lei nº 12.965/14 ("Marco Civil da Internet") prevê a inviolabilidade do conteúdo de comunicações privadas armazenadas, salvo por ordem judicial, a partir do que já se argumentou que apenas o conteúdo em fluxo estaria sujeito aos ditames da Lei de Interceptações Telefônicas. Porém, na falta de requisitos substantivos para o acesso a dados de comunicação armazenados, há autores que entendem a aplicação, por analogia, dos requisitos previstos no artigo 2º, III, da Lei nº 9.296/96. Para Ricardo Sidi, por exemplo, as mensagens de e-mail armazenadas estão naturalmente inseridas no âmbito dessa proteção, inclusive sob o sentido linguístico da expressão "sigilo das comunicações"[40].

Essa posição nos parece correta, pois na ausência de regulamentação específica e de critérios de proporcionalidade a guiarem o magistrado prolator da autorização de devassada do sigilo comunicacional do cidadão, a prática da persecução penal tem se desenvolvido com grave desequilíbrio entre o grau de proteção de conferido às comunicações em tempo real e as comunicações armazenadas. Como consequência, pode-se citar que uma investigação de crime contra a honra não permitirá, como regra, a interceptação das comunicações por meios telemáticos do imputado, pelo prazo de 15 dias (art. 5º da Lei nº 9.296/96), mas poderá ser decretado o afastamento do sigilo de suas comunicações armazenadas em determinado serviço de e-mail por períodos indeterminados ou muito mais extensos que o autorizado por lei para acesso em tempo real, o que cria situação anacrônica no nível de proteção do sigilo de comunicações privadas.

---

[40] Nas palavras do autor "Não há ocorrência ou razoabilidade em retirar os e-mails armazenados do âmbito de proteção do direito ao sigilo de comunicações (artigo 5º, XII, CF). Afinal, por mais que sua arrecadação já não caracterize uma interceptação propriamente dita, por falta do requisito contemporaneidade, e por mais que se trate de mensagem já recebida pelo destinatário, é inegável que a preservação de seu conteúdo humano e demais detalhes ligados a ela não pode ser dissociada da expressão constitucional "sigilo das comunicações", dotada de tão claro sentido". Cf. SIDI, Ricardo. *A Interceptação das Comunicações Telemáticas no Processo Penal.* Belo Horizonte, 2016, Editora D'Plácido, p. 300.

O Marco Civil da Internet também conceituou e regulou o fornecimento de registros de conexão e de acesso às aplicações da internet não se confundem com o conteúdo de comunicações privadas. Na realidade, esses registros são metadados, isto é, informações acessórias aos conteúdos privados, que indicam data, hora e o número de *internet protocol* das conexões à rede mundial de computadores e dos acessos às aplicações de internet. O acesso a registros de conexão e acesso expõe a privacidade dos usuários em menor intensidade, o que justifica que as quebras de sigilo desses dados devam observar requisitos mais brandos que as quebras de sigilo de comunicações privadas.

Os registros de acesso a aplicações recebem proteção constitucional, na forma do 5º, X[41], e legal, conforme os artigos 3º, III 7º, VII e 10 § 1º da Lei nº 12.965/2014 ("Marco Civil da Internet"). A respectiva quebra de sigilo dependerá, assim, como regra, de prévia e expressa ordem judicial. Em menor intensidade, o artigo 22 da Lei nº 12.964/14 (popularmente conhecida como "Marco Civil da Internet") exige que o afastamento de sigilo sobre os registros de acesso[42] se dê mediante autorização judicial para formação de prova em processo civil ou criminal.

1.3.3. Proteção de dados cadastrais e disposições especiais esparsas: art. 15 da Lei nº 12.850/13, art. 17-B da Lei nº 9.613/96 e arts. 13-A e 13-B do CPP.

De acordo com a definição dada pelo art. 11, §2º, do Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet, constituem os dados cadastrais a filiação, o

---

[41] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

[42] Os registros de acesso, que abrangem os IPs (Internet Protocol), são também conhecidos como metadados, quais sejam, "todos os dados e registros gerados a partir de uma comunicação e que não constituam o seu conteúdo em si, como, por exemplo, data, hora e duração da comunicação, remetente, destinatários, eventuais dado de localização geográfica do dispositivo (como Estação Rádio Base), códigos de identificação de dispositivos (como IMEI), etc. ABREU, Jacqueline de Souza, ANTONIALLI, Dennys. *Vigilânica Sobre as Comunicações no Brasil*. INTERNETLAB, São Paulo, 2017. p. 23. A definição legal é dada pela Lei nº 12.965/14 ("Marco Civil da Internet"): Art. 5º Para os efeitos desta Lei, considera-se: VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados; VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

endereço e qualificação pessoal – que abrange o nome, o prenome, o estado civil e a profissão do usuário[43]. O artigo 10, § 3º, da Lei Federal nº 12.965/2014 admite "*o acesso aos dados cadastrais (...) pelas autoridades administrativas*" [44], previsão legal complementada pelo art. 11 do referido decreto, cujo caput preceitua que as requisições de acesso aos dados cadastrais podem ser formuladas diretamente pela a autoridade policial e membros do Ministério Público, mediante a indicação do "fundamento legal de competência expressa para o acesso e a motivação para o pedido". O parágrafo terceiro, por sua vez, veda pedidos coletivos, genéricos ou inespecíficos.

Os dados pessoais cadastrais – isto é, todos aqueles dados passíveis de se identificar alguém – são informações excluídas do acesso ao público e, portanto, protegidas pelo direito de privacidade (artigo 7º, VII, da Lei Federal nº 12.965/2014 e artigo 5º, X, da CF). A privacidade, dentre outras definições, pode ser entendida como um "conjunto de informações acerca do indivíduo que ele decide manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições"[45].

A limitação de referido direito, tal como a de qualquer outro de apreço constitucional faz-se mediante necessária e prévia análise, pelo Poder Judiciário, quanto à presença, em cada caso concreto, de requisitos mínimos e indispensáveis à decretação de medidas restritivas[46], conforme se extrai do texto do artigo 5º, LIV, da CF. Com efeito, tais dados, se não forem públicos para terceiros por expressa disposição de vontade de seu titular, somente poderão ter seus sigilos levantados por decisão judicial, diante do

---

[43] BRASIL. Decreto nº 8771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 24 set. 2024.

[44] BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 13 out. 2023.

[45] PEREIRA, José Matos. Apud José Afonso da Silva, *Curso de Direito Constitucional Positivo*, 11ª ed. São Paulo, Malheiros, 1996, p. 202.

[46] Conforme voto paradigmático do Min. Celso de Mello no MS 21.729-4/DF, "*a intervenção jurisdicional constitui fator de preservação do regime das franquias individuais e impede, pela atuação moderadora do Poder Judiciário, que se rompa, injustamente, a esfera de privacidade das pessoas".* BRASIL, Supremo Tribunal Federal. MS 21729, Tribunal Pleno, Relator Ministro Marco Aurélio, julgado em 05/10/1995, publicado em 19/10/2001.

postulado da reserva de jurisdição para a limitação a direito fundamental ou nas expressas e taxativas hipóteses legais.

As hipóteses legais de requisição direta de dados cadastrais pelas autoridades policiais estão definidas pelas Leis Federais nº 12.683/12[47] (que alterou a Lei 9.613/98), nº 12.850/13[48] e nº 13.344/16 (que alterou recentemente o Código de Processo Penal para nele incluir o artigo 13-A[49]).

Nota-se, portanto, que não há conflito aparente entre o Marco Civil da Internet e as hipóteses legais de requisição direta de dados cadastrais por autoridades policiais. Referidas leis especiais, bem como o artigo 13-A do CPP[50], complementam o sentido da exigência de indicação de "fundamento de competência expressa", disposto no artigo 10, §3º, da Lei Federal nº 12.965/2014 conjugado com art. 11 do Decreto Federal nº 8771/2016. Foi o que reconheceu o STF recentemente no julgamento da ADI 5642, que tinha por objeto justamente a constitucionalidade do art. 13-A do CPP. De acordo com o voto prevalente do relator, o Ministro Edson Fachin, o dispositivo é constitucional e: (i) Art. 13-A é *numerus clausus* e (ii) O conceito de dados cadastrais adotado pelo MCI deve prevalecer sobre definições genéricas (iii) Consequentemente, dados de IP (e outras informações) não se incluem no conceito de dados cadastrais (iv) Dados cadastrais de e-mail não se enquadram no conceito de dados cadastrais e o acesso depende de autorização judicial, limitado o poder requisitório de dados às hipóteses expressamente previstas[51].

---

[47] Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

[48] Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito.

[49] Art. 13-A. Nos crimes previstos nos arts. 148, 149 e 149-A, no § 3º do art. 158 e no art. 159 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), e no art. 239 da Lei no 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos.

[50] BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 01 ago. 2024.

[51] BRASIL. Supremo Tribunal Federal. ADI 5642. Tribunal Pleno. Relator Edson Fachin. Julgado em 18/04/2024. Publicado em 22/08/2024.

Assim, para os crimes de lavagem de dinheiro, organização criminosa, sequestro e cárcere privado, redução à condição análoga de escravo, tráfico de pessoas, “sequestro relâmpago” (art. 158, §3º, CP[52]), extorsão mediante sequestro e tráfico de criança ou adolescente, a ponderação entre os direitos fundamentais envolvidos já foi feita pelo próprio legislador, que optou por excepcionar o direito à privacidade em favor dos interesses da persecução penal.

Diverge dessa posição Aras, para quem o acesso aos dados cadastrais pode ser concedido diretamente, sem prévia autorização judicial mediante requisição do Ministério Público ou da Polícia no curso de uma investigação criminal, impendentemente da natureza do delito apurado – posição com a qual não concordamos, porquanto desconectada do fundamento reitor de intervenções em direitos fundamentais, quais seja, a legalidade, cuja observância, pelo legislador, como visto acima, foi concretizada por meio de disposições que previram leis especiais para o acesso direto em vista da natureza das infrações penais apuradas[53].

Em síntese: a leitura sistemática e conforme a Constituição das normas que atualmente regram a matéria deixa claro que, quando o legislador quis excepcionar a cláusula de reserva de jurisdição para o afastamento do sigilo de dados cadastrais, o fez taxativamente, indicando os tipos penais em relação aos quais é prescindível ordem judicial para o acesso às informações que integram a privacidade do usuário.

1.3.4. Devido processo informacional e reflexos da LGPD no tratamento de dados para fins penais.

A Lei nº 13.709/18 estabeleceu regra expressa de exclusão de sua incidência para finalidades de segurança pública e repressão e prevenção a infrações penais (art. 4º, III, a) e d), que serão regidas por legislação específica até o momento não editada[54]. A

---

[52] BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 01 ago. 2024.

[53] ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo penal. Delictae - Revista de Estudos Interdisciplinares sobre o Direito, v. 8, p. 180-222, 2024.

[54] Está atualmente em tramitação no Congresso Nacional o Projeto de Lei nº 1515/22, que prevê regras de tratamento de dados pessoais para atividades de segurança do Estado, defesa social, segurança pública e repressão e investigação de infrações penais.

própria lei, porém, ressalva que o tratamento de dados pessoais em tais tipos de atividades seguirá, necessariamente, os princípios gerais de proteção de dados pessoais e os direitos do titular (parágrafo primeiro). Ao mesmo tempo, o art. 4º da LGPD dispensa o consentimento para o tratamento dados pela administração pública enquanto "conjunto de agentes, órgãos e pessoas jurídicas que tenham a incumbência de executar atividades administrativas". Além dos princípios da LGPD, que devem nortear todo e qualquer tratamento de dados pessoais, aqui, por ser o próprio ente público o responsável por conduzir esta atividade, deve ele se pautar também pelos princípios constitucionais que regem a atividade da administração pública, quais sejam: legalidade, impessoalidade, moralidade, publicidade e eficiência[55].

Além disso, a Agência Nacional de Proteção de Dados (ANPD) emitiu a Nota Técnica nº 175, reconhecendo expressamente a competência do órgão para emitir "*opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do art. 4º da Lei, e o dever de solicitar aos responsáveis o relatório de impacto à proteção de dados pessoais*", o que justifica a análise desses pontos – princípios de proteção, direitos do titular e atuação da ANPD em matéria de persecução penal – no presente trabalho[56].

O conceito de dado pessoal da LGPD é expansionista e opera com dois tipos de informação: (i) identificada: por atributos próprios identifica-se alguém, a exemplo do CPF, cuja sequência numérica se refere apenas a determinada pessoa; e (ii) identificável: lida com a atribuição por meio de potenciais combinações diante contexto em que o tratamento de dados é realizado.

Seguindo a lógica de clareza e transparência já adotada anos antes pelo Marco Civil da Internet, o art. 18 da LGPD reconheceu, os seguintes direitos do titular: à

---

[55] FRAJHOF, Isabella Z.; MANGETH, Ana Lara. As bases legais para o tratamento de dados pessoais. In: MULHOLLAND, Caitlin (org.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020, pp. 65 – 98.

[56] A nota técnica trata do acordo de Cooperação entre o MJSP e a CBF para compartilhamento de dados pessoais visando ao aprimoramento do Projeto Estádio Seguro, e a utilização de tecnologia para possibilitar a identificação de torcedores envolvidos em atos ilícitos. A ANPD enfatiza a observância aos princípios da necessidade e adequação do tratamento de dados, bem como o base legal aplicável e, diante da perspectiva de tratamento de dados pessoais sensíveis (biométricos), recomenda a elaboração de relatório de impacto na proteção de dados pessoais dos titulares afetados.

confirmação da existência do tratamento e o acesso aos dados (incisos I e II); à correção dos dados incompletos (inciso III); à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (inciso IV); à portabilidade (inciso V); à eliminação dos dados (inciso VI); bem como à informação das entidades públicas ou privadas com as quais o controlador realizou uso compartilhado de dados (inciso VII); possibilidade de não fornecer consentimento e consequências da negativa (inciso VIII). Além desses, o art. 20 previu o direito à explicação e à revisão de decisões automatizadas[57].

O primeiro direito expressamente reconhecido, de confirmação do tratamento de dados, é assegurado de forma livre e independentemente de recusa do responsável pelo tratamento. O fundamento por traz desse direito está na concepção de que a tutela dos dados pessoais decorre dos direitos de personalidade enquanto extensão ou dimensão do titular.

Os direitos de personalidade tutelam uma miríade de relações multilaterais, conjugando uma série de direitos individuais, como a inviolabilidade do domicílio; o controle sobre as informações de cunho pessoal; a liberdade de autodeterminação, incluindo as decisões sobre o próprio corpo, como o aborto e a eutanásia; assim como questões envolvendo privacidade e vigilância.

Por se tratar de direitos irrenunciáveis e intransmissíveis, não se admite a desvinculação dos dados do titular e, assim, que lhe seja reconhecida a capacidade de agenciamento sobre os próprios dados. Há dúvida se é necessário o requerimento prévio por parte do titular ou se a confirmação de tratamento deve ser comunicada automaticamente como forma de assegurar os demais direitos, pois o titular dos dados somente poderá verificar a conformidade das bases legais se tiver ciência de que seus dados foram objeto de tratamento pelo responsável[58].

Como decorrência do direito de confirmação, surge o direito de acesso do titular aos dados pessoais frente ao agente responsável pelo tratamento, de forma gratuita e

---

[57] BRASIL. Lei no 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados brasileira (LGPD). Disponível em: <http:// www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 04 dez. 2023.

[58] Essa é a posição defendida por Priscila Regina Silva. SILVA, Priscilla Regina. Os direitos dos titulares de dados. In: MULHOLLAND, Caitlin (org.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020, pp. 196.

em formato simplificado, mediante requerimento do titular. Além de indicar os dados tratados, o controlador tem a obrigação de informar a sua origem, forma de coleta e armazenamento, categorização dos dados, finalidade que motivou o tratamento bem como se houve o uso de decisões automatizadas – questão, aliás, de fundamental revelo ao tratarmos das ferramentas de extração forçado de dados pessoais de dispositivos móveis, como se verá adiante.

É preciso, contudo, assumir que os princípios de transparência e acesso aos dados tratados, pelo titular, embora decorram do princípio da proporcionalidade sob a perspectiva da necessidade de meio menos gravoso e tenham especial importância no regime geral de proteção de dados, sofrem inexoráveis mitigações no campo da persecução penal (assim como no da segurança pública), como reflexo da natureza dessas atividades. Por natural, em se tratando de métodos ocultos de investigação, como a intercepção telemática e a infiltração online, o acesso dos dados obtidos pela pessoa afetada somente se dará, em regra, finda a diligência ou a partir do momento em que não se vislumbre mais risco de comprometimento às investigações[59].

O direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade tem especial importância e demanda alguns esclarecimentos. O conceito de anonimização é dado pela própria LGPD enquanto “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”. Os dados anonimizados, por perderem a qualidade de dado pessoal, não estão sob a proteção da lei. E não devem ser confundidos com os dados pseudoanonimizados, cujas técnicas de encriptação são reversíveis e podem levar à ulterior identificação dos titulares. Conforme Silva, a anonimização busca dissociar dos dados a pessoa de origem, enquanto a eliminação dos

[59] Cf. GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penal e na segurança pública - 1ª Ed - Rio de Janeiro: Marcial Pons, 2021, p. 65. É importante apontar, ainda, a respeito do acesso aos elementos confidenciais ou decorrentes de medidas interventivas ocultas, que no Brasil há antiga construção jurisprudencial sumulada pelo Supremo Tribunal Federal na SV 14, que enuncia ser “direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa”, condicionando o acesso ao término das diligências, portanto.

dados objetiva a redução ao tratamento do mínimo de dados, sob o manto da finalidade e da necessidade[60].

No que diz respeito aos agentes responsáveis pelo tratamento de dados pessoais, a lei define como controlador aquele a quem compete a tomada de decisões referente ao tratamento de dados pessoais, ao passo que o operador realiza tal tratamento em nome do controlador, segundo suas diretrizes. No contexto de investigações criminais, o controlador será o órgão estatal responsável pela obtenção dos dados e condução das investigações, como a polícia judiciária (civil ou federal) e ministérios públicos estaduais ou federal.

A primeira constatação é de que a oponibilidade de direitos do titular ao controlador também se estende ao operador do tratamento de dados pessoais. Isso porque, embora o caput do art. 18 da LGPD mencione apenas o controlador, é de se presumir, conforme Priscila Regina Silva, tal extensão na medida em que ambos, controlador e operador, "são considerados pela lei como agentes de tratamento e, nessa condição, deverão garantir os direitos e responder solidariamente pelos danos advindos de violações ou tratamentos inadequados"[61].

A incidência do rol de direitos acima identificados - conquanto não infirme nem ratifique, neste momento, a legalidade e os requisitos a serem seguidos na extração forçada de dados pessoais de dispositivos apreendidos -, assegura, no mínimo, os seguintes direitos aos titulares de dados pessoais afetados por medida interventiva de tal natureza: confirmação da existência do tratamento e o acesso aos dados (art. 18, I e II); à correção dos dados incompletos (art. 18, III); à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (art. 18, IV); à portabilidade (art. 18, V); à eliminação dos dados (art. 18, VI); bem como à informação das entidades públicas ou privadas com as quais o controlador realizou uso compartilhado de dados (Art. 18, VII); possibilidade de não fornecer consentimento e consequências da negativa (VIII); por fim direito à explicação e à revisão de decisões automatizadas (art. 20).

---

[60] SILVA, Priscilla Regina. Os direitos dos titulares de dados. In: MULHOLLAND, Caitlin (org.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020, pp. 201 – 202.
[61] *Ibid.*, 195 – 215.

1.4. Síntese parcial

1. A inviolabilidade dos direitos fundamentais não implica impossibilidade de intervenção, mas exige justificação especial sob pena de violação.
2. A intervenção em direitos fundamentais sem reserva, isto é, restrição e parâmetros expressamente previstos constitucionalmente, é admissível desde que fundada em lei aliada a um juízo de proporcionalidade em face a outros valores de hierarquia constitucional.
3. A proteção de dados pessoais é direito fundamental que abrange não só os dados sob sigilo, mas quaisquer informações sobre pessoa natural identificada ou identificável, em que pese a regulamentação do acesso a tais tipos de dados esteja ligada a requisitos mais ou menos intensos previstos na legislação infraconstitucional.
4. A obtenção de dados para fins de persecução penal relaciona-se a atividades de elucidação de materialidade e autoria em face de pessoas suspeitas da prática de determinada infração penal.
5. A legislação infraconstitucional prevê requisitos específicos para o acesso a dados de comunicação privada, armazenados ou não (art. 2º, III, da Lei nº 9.296/96), registros de conexão à internet e registros de acesso em aplicações (arts. 13 e 15 do MCI) e dados cadastrais (art. 13-A do CPP, art. 17-B da Leo nº 9.613/98 e art. 15 da Lei nº 12.850/13). Não há previsão legal para acesso a outros tipos de dados sigilosos, como arquivos de áudio, vídeo ou texto salvos sistemas de armazenamento em nuvem, relação de buscas realizadas pelo usuário, histórico de exibição em plataformas de reprodução de vídeo ou áudio, relação de locais frequentados etc.
6. Conquanto a LGPD preveja a não incidência das disposições legais às atividades de tratamento de dados pessoais para fins de investigação e repressão de infrações penais, aplicam-se a principiologia e os direitos do titular.
7. O atendimento a princípios como, por exemplo, da finalidade, necessidade, qualidade dos dados, transparência, segurança, prevenção e prestação de contas dos agentes de tratamento envolvidos nas dinâmicas e rotinas de hacking são

preceitos que devem ser sedimentados com base no direito constitucional à proteção de dados pessoais.

8. Aos titulares de dados pessoais asseguram-se os direitos à confirmação da existência do tratamento e o acesso aos dados; à correção dos dados incompletos; à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD; à portabilidade; à eliminação dos dados; bem como à informação das entidades públicas ou privadas com as quais o controlador realizou uso compartilhado de dados; possibilidade de não fornecer consentimento e consequências da negativa; por fim direito à explicação e à revisão de decisões automatizadas (art. 20).
9. A ANPD é competente para emitir opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do art. 4º da Lei, e o dever de solicitar aos responsáveis o relatório de impacto à proteção de dados pessoais.

Traçados os fundamentos constitucionais e as bases infralegais do tratamento de dados pessoais, sigilosos ou não, aplicáveis ao processo penal, veremos no próximo capítulo o fenômeno político-institucional disseminado entre agências de inteligência, de segurança pública e de investigação criminal conhecido como hacking governamental. Em relação às agências de investigação, mais especificamente, tem-se compreendido que o uso de ferramentas para extração forçada de dados de dispositivos informáticos obtidos no decorrer da persecução penal constitui desdobramento natural e judicialmente convalidado da busca e apreensão, cujos limites legais e alcance permissivo do instituto - enquanto medida interventiva em direito fundamental tipicamente prevista e regulada em lei -, suscitam dúvidas quanto à legitimidade e conformidade dessa prática à luz do arcabouço protetivo de dados pessoais.

2. A busca e apreensão no contexto da extração forçada de dados

O acesso à internet se popularizou através de diversos dispositivos portáteis, transformando-os em verdadeiros "microcomputadores" que permitem a conexão imediata e instantânea à rede mundial de computadores. Os aparelhos celulares, antes utilizados principalmente para comunicação por voz, evoluíram para se tornarem multifuncionais, oferecendo uma ampla gama de funcionalidades aos usuários, como aplicações de mensageria instantânea, de e-mail, armazenamento e gerenciamento de arquivos, marcadores de saúde e sinais vitais, cartões de crédito, plataformas de compra etc[62].

Em operações de extração de dados de celular, identifica-se o fenômeno que tem sido chamado de *hacking* governamental[63], em que o Estado, na condição de controlador, contrata sistemas desenvolvidos por empresas privadas de obtenção

---

[62] A ampla capacidade de processamento de informações dos modernos aparelhos de celular foi descrita por Gloeckner e Eilberg: "O que deve ser imediatamente bem compreendido é que o aparelho celular configura-se, concomitantemente, como um objeto capaz de assegurar a portabilidade15 de registros e informações de conteúdo pessoal e receptáculo de tecnologias de informação (especialmente aplicativos), que faz o papel de conector entre o usuário e múltiplos veículos de informação e facilitadores. Dessa maneira, ao mesmo tempo que o celular integra aparatos tecnológicos – como câmeras digitais, agendas de contato, calculadoras, gravadores de voz e outros tantos instrumentais –, também acaba por servir como um verdadeiro computador, atuando, então, como uma 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". In GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. Revista Brasileira de Ciências Criminais. Vol 156/2019, p. 4.

[63] Conforme Pedro Amaral: "Para fins deste estudo, o que será considerado hacking diz respeito dois atributos: primeiro, do ponto de vista técnico, a exploração de uma vulnerabilidade, seja ela intencional ou não, conhecida ou não, pelo fabricante, que resulte no acesso não-autorizado a uma informação, seja comunicação ou dados em repouso ou em trânsito; em segundo lugar, do ponto de vista comportamental, essa exploração envolve intencionalidade, ou seja, o propósito de alcançar aquela informação por meio do desvio do que seria um sistema de segurança. Adicionalmente, optamos por usar a terminologia "governamental" por duas razões. Certos autores denominam o campo dessas atividades como "lawful hacking" ("hacking legal") ou mesmo "law enforcement hacking" ("hacking investigativo"). No entanto, uma vez que não delimitamos bases que confiram legalidade evidente à prática no Brasil e que, do ponto de vista político, ferramentas dessa natureza vêm sendo associadas à atividades de perseguição a dissidentes políticos, denominar a prática de "legal" demanda um amadurecimento legislativo muito mais avançado. Depois, como forma de ressoar boa parte da literatura internacional que opta por "government hacking", a adoção do termo também busca um alinhamento com o debate global para significar a agência de entidades pertencentes ao corpo estatal". In AMARAL, Pedro Mercadores da insegurança [livro eletrônico] : conjuntura e riscos do hacking governamental no Brasil / Pedro Amaral, Mariana Canto, Marcos César M. Pereira; coordenação André Ramiro. --1. ed. -- Recife, PE : IP.rec, 2022 (p. 6).

forçada de dados de dispositivos sob a custódia de agências penais[64], mediante a exploração de vulnerabilidades dos fabricantes, resultando em acessos não consentidos aos aparelhos.

À primeira vista, sofisticação dos crimes e a proteção das provas por sistemas de segurança robustos no mercado tecnológico poderiam motivar o uso de ferramentas mais avançadas para a segurança pública. No entanto, o investimento constante para superar essas barreiras cria uma cultura que busca e mantém vulnerabilidades em sistemas conectados, o que pode resultar no uso inadequado por agentes governamentais ou em incidentes de segurança que vazam informações para atores maliciosos.

De acordo com Pedro Amaral, existem duas categorias de *hacking* governamental[65]: i) o acesso a dados e comunicações a partir do controle físico do aparelho (por exemplo, um celular apreendido), possibilitando a extração em massa de dados do dispositivo. Esse cenário poderia envolver tanto a quebra de criptografia em aplicações e em discos de armazenamento, ou mesmo o desvio a outros sistemas de segurança, como senhas alfanuméricas, padrões ou autenticação mediante biometria para desbloqueio do dispositivo ou acesso a aplicações; e ii) o acesso remoto a dispositivos, normalmente a partir da exploração de uma vulnerabilidade ainda não conhecida pelo fabricante do sistema vulnerável e que permita o acesso total ou parcial ao aparelho. Para este último caso, também incluímos o uso de ferramentas para interceptação direta do tráfego de informações em redes móveis a partir de uma relativa proximidade do dispositivo alvo.

O presente estudo está limitado à primeira hipótese, em que as empresas provedoras de ditos sistemas extração forçada atuarão, em determinados contextos, como operadoras no tratamento de dados em nome dos órgãos de persecução estatais,

---

[64] "No campo das ferramentas de extração em massa de dados de celulares, também são registrados, de forma ainda mais marcante, altos níveis de escalabilidade que tornam cotidiano o uso de técnicas de hacking por forças policiais. Normalmente chamados de MDFTs (mobile device forensic tools), são conjuntos de hardware e software utilizados em dispositivos móveis em custódia das forças policiais para desbloqueá-los e extrair dados, através de conexão física, que alcançam serviços de e-mail, armazenamento em nuvem, dados de redes sociais, histórico de localização (GPS), comunicações privadas, fotos, vídeos e, basicamente, o que mais estiver armazenado e acessível em aparelhos de celular pessoais, incluindo dados deletados pelo usuário. Sobre o conjunto de dados coletados, não é incomum ver soluções de inteligência artificial aplicadas adicionalmente, como forma de identificar padrões. *Ibid.*, p. 9.

[65] *Ibid.*, p. 7

o que suscita a análise dos parâmetros de legalidade dessa prática – se é que o atual desenho normativo a comporta.

Atualmente, levantamentos apontam que a imensa maioria dos contratos entre empresas privadas desenvolvedoras de softwares de acesso remoto a sistemas de segurança e a dispositivos informáticos e agências da Administração Pública Federal ocorrem mediante dispensa de licitação[66]. As informações apontam que, além da dificuldade de obter dados claros sobre as cláusulas contratuais junto aos órgãos governamentais, muitas das empresas sofrem forte escrutínio social e político, por suposto envolvimento com prática de vigilância massiva de cidadãos no contexto de governos autoritários, bem como em episódios de vazamento de dados.

Estaria essa prática, desprovida de expressa previsão legal, amparada pela Convenção de Budapeste sobre Crimes Cibernéticos? Ou, ainda, poderia se utilizar do instituto da busca e apreensão, isto é, como consequência lógica da obtenção de dispositivos informáticos em posse dos investigados judicialmente autorizada, também estaria autorizada a respectiva extração forçada, mediante ferramentas tecnológicas de quebra de sistemas de segurança, dos dados pessoais – sigilosos ou não – armazenados

[66] Conforme noticiado pelo portal de notícias The Intercept Brasil em 12 de março de 2024, a despeito de a licitação ser a regra constitucional para a contratação de serviços pela administração pública, entre 2020 e 2023, diversos ministérios públicos estaduais e secretárias de segurança pública dos estados da federação adquiriram softwares de espionagem conhecido como Snap, ferramenta de análise de dados que permite o cruzamento de dados em redes sociais e fontes abertas, mediante procedimento de inexigibilidade de licitação, sob a justificativa de que se trata de que as especificidades do produto o tornam singular no mercado. A matéria também aponta que o Cellebrite, ferramenta de extração de dados desenvolvida em Israel e comercializada no Brasil por intermédio da Techbiz Forense Digital, já está amplamente disseminada entre as polícias civis e ministérios públicos no Brasil. Disponível em: https://www.intercept.com.br/2024/03/12/uso-de-ferramenta-que-cruza-conexoes-do-facebook-e-dados-da-policia-explode-no-pais/. Acesso (online) em: 17/05/2024. Além disso, tramita atualmente no STF a ADPF nº 1143, ajuizada pela Procuradoria-Geral da República em 13/12/2023, incialmente com ação declaratória de inconstitucionalidade por omissão, contra a ausência de atuação normativa do Congresso Nacional. Alega-se missão parcial na regulação do uso de programas de intrusão remota e monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal. A controvérsia reside no uso atual, secreto e abusivo de softwares e ferramentas de intrusão sem autorização judicial e sem limites e salvaguardas, contrariando garantias constitucionais, tendo a ação por objetivo sanar a omissão e estabelecer diretrizes provisórias para o uso de ferramentas de intrusão virtual no âmbito de serviços de inteligência e por órgãos de repressão, sob o pretexto de combater o terrorismo e o crime organizado. Em resposta a ofícios expedidos por determinação do Ministro Relato, Cristiano Zanin, o TCU indicou a existência de sete processos de aquisição de softwares. No âmbito dos estados, os TC de Santa Catarina, São Paulo, Paraná, Mato Grosso e Pará, confirmaram a aquisição de softwares de mais de uma empresa para esse propósito.

na memória dos aparelhos, bem como a recuperação de arquivos já deletados pelos usuários titulares dos dados pessoais objeto da operação de tratamento?

Em caso afirmativo, quais os requisitos específicos a decisão judicial porventura deverá preencher, direitos do titular assegurados e principiologia atinente ao tratamento e à proteção dos dados pessoais obtidos com a operação controlada pelos órgãos de persecução – e eventualmente operadas por entidades privadas detentoras dos meios tecnológicos - deverão ser seguidos?

Buscaremos responder a esses questionamentos nos tópicos que seguem.

2.1. Medidas probatórias na Convenção de Budapeste e internalização de tratados interventivos em direitos humanos

A Convenção de Budapeste sobre Cibercriminalidade entrou em vigor no Espaço Econômico Europeu em 1º de julho de 2004. No Brasil, o instrumento de direito público internacional foi aprovado pelo Decreto Legislativo nº 37/2021 e entrou em vigor internacional no país em 1º de março de 2023, uma vez concluído o processo de adesão. O texto possui 68 Partes e, com sua promulgação pelo Decreto nº 11.491/2023, ganhou vigência interna a partir de 13 de abril de 2023, data da publicação do tratado no Diário Oficial da União.

O art. 19 da Convenção de Budapeste regula medida de natureza que interessa ao presente estudo, qual seja, a busca e apreensão de computadores, dispositivos de armazenamento e sistemas informáticos e dos dados neles armazenados. Esse mecanismo em regra se implementa sem prévio aviso ao detentor dos dados, e o acesso aos dados de computador (quaisquer deles) pode ocorrer de maneira remota ou mediante apreensão física dos dispositivos de armazenamento.

O dispositivo é composto por cinco seções. A primeira dispõe que o Estado aderente à convenção deverá adotar medidas legislativas e conferir poderes às autoridades de persecução com atribuição para realizar buscas e apreensões, tendo por objeto “sistema de computador ou de parte dele e dos dados nele armazenados” (alínea a), assim como de “qualquer meio de armazenamento de dados de computador no qual possam estar armazenados os dados procurados em seu território”.

A segunda seção reforça a necessidade de produção legislativa para assegurar o acesso a dados de computador, sendo legítima a extensão da diligência para busca em outro sistema quando houver fundadas razões de que os dados procurados se encontram armazenados a partir de um sistema inicial ou disponíveis em tal sistema. Por sua vez, a terceira seção estabelece procedimentos mínimos de cadeia de custódia da prova, impondo a adoção de medidas legislativas que instituam o poder de "apreender ou proteger um sistema de computador ou parte dele ou um meio de armazenamento de dados" (a), obrigação de guardar uma cópia desses dados (b), manutenção da integridade dos dados relevantes (c), bem como "tornar inacessíveis esses dados no sistema de computador acessado ou dele removê-los".

A quinta seção, no que no interessa, remete à aplicação dos artigos 14 e 15 da Convenção para os fins de validade das medidas previstas no artigo 19. O artigo 14 trata do âmbito de aplicação dos dispositivos processuais. A segunda seção prevê que os poderes e procedimentos conferidos pela Convenção para fins de investigações ou processos criminais se aplicam aos crimes previstos na própria convenção[67] (a), bem como a outros crimes cometidos por meio de um sistema de computador (b) ou, ainda, para fins de coleta de provas eletrônicas da prática de um crime (c).

Já o artigo 15 é de absoluta relevante para a comprovação da hipótese ora desenvolvida – a reserva de lei como primeiro pressuposto para a intervenção na proteção de dados pessoais armazenados em aparelhos de celular apreendidos -, porquanto prevê, na primeira seção, a que a implementação e a aplicação dos poderes e procedimentos previstos na Convenção sujeitam-se às condições e garantias de sua própria legislação interna, respeitados os direitos humanos e a observância ao princípio da proporcionalidade. Além disso, a segunda seção contempla um mínimo de garantias a serem asseguradas, incluindo o controle judicial, fundamentação da aplicação, bem como limites no âmbito de aplicação e condições de duração dos mecanismos objeto da Convenção.

---

[67] A Convenção de Budapeste instituiu, nos Títulos I a IV da Seção I do Capítulo II, as infrações penais a fim de que as Partes signatárias adotem medidas legislativas para tipificar as condutas de acesso ilegal (artigo 2º, interceptação ilícita (artigo 3º), violação de dados (artigo 4º), interferência em sistema (artigo 5º), uso indevido de aparelhagem (artigo 6º), falsificação informática (artigo 7º), fraude informática (artigo 8º), pornografia infantil (artigo 9º) e violação de direitos autorias e de direitos correlatos (artigo 10).

Com base nessas disposições da Convenção sobre a necessidade de produção legislativa em âmbito interno que ampare os poderes e procedimentos outorgados às Partes signatárias, divergimos da posição de Aras – para quem as medidas cautelares probatórias da Convenção se aplicam imediatamente após a internalização[68] - e entendemos que, na ausência de disposição legal expressa que autorize a extração de dados de sistemas de computador – que incluem os sistemas operacionais utilizados na maioria dos aparelhos de telefone celular -, a utilização de ferramentas de *hacking* governamental capazes de extrair forçadamente os dados armazenados em dispositivos informáticos tem ocorrido de maneira clandestinas e à margem da legislação.

2.2. A busca e apreensão de dados e elementos informáticos

A presente pesquisa se limita à extração de dados não consentida de aparelho celular apreendido no âmbito de procedimento persecutório criminal – seja inquérito policial ou ação penal. Portanto, não tem por escopo perscrutar a tipicidade do acesso a dados a celulares apreendidas mediante autorização e fornecimento voluntário da senha pelo titular do aparelho - e dos respectivos dados armazenados -, tampouco o acesso remoto aos dados mediante o uso de ferramentas de espionagem, questões que remetemos o leitor a Rebellato[69].

Muito embora o acesso aos dados armazenados em aparelho celular, de um lado, tenha o potencial de devassa nas informações pessoais titularizadas pelo imputado sujeito à medida cautelar processual probatória, o artigo 19 da Convenção de Budapeste (conhecida como Convenção sobre o Crime Cibernético), de outro – que trata da busca

---

[68] O autor apresenta a possibilidade de aplicação imediata dos mecanismos de produção probatória previstos na Convenção de Budapeste, argumentando que “No âmbito do STF, há exemplos de pronta aplicação de normas decorrentes de tratados, em institutos como a extradição, a transferência de processos penais e a formalização de audiências de custódia, mesmo antes do Pacote Anticrime, dada a paridade normativa entre tratados e leis ordinárias: A eventual precedência dos tratados ou convenções internacionais sobre as regras infraconstitucionais de direito interno somente se justificará quando a situação de antinomia com o ordenamento doméstico impuser, para a solução do conflito, a aplicação alternativa do critério cronológico ("lex posterior derogatpriori ") ou, quando cabível, do critério da especialidade. ARAS, Vladimir. O congelamento de dados informáticos para fins de prova no processo penal. Delictae - Revista de Estudos Interdisciplinares sobre o Direito , v. 8, p. 180-222, 2024.

[69] REBELLATO, Luiz Fernando Bugiga. A análise constitucional do sigilo e da privacidade nas investigações criminais: o acesso a dados armazenados em aparelhos celulares. Dissertação (Mestrado – Programa de Pós-Graduação em Direito Processual) – Faculdade de Direito. Universidade de São Paulo, 2020.

e apreensão de dados de computador -, impõe aos países signatários o dever de produção legislativa que confira poderes às autoridades competentes para: (i) busca de "qualquer sistema de computador ou de parte dele e dos dados nele armazenados"; e (ii) de quaisquer dados de computador armazenados[70].

Em que pese o Brasil ter internalizado a normativa internacional por meio do Decreto nº 11.491/2023, desde então não houve avanços no quadro legislativo para regulamentar as disposições do artigo 19 e outras disposições relacionadas à obtenção de dados armazenados em sistemas de computadores, no que se incluem os modernos smartphones. Diante desse quadro de aparente anomia, tem-se recorrido à tradicional disciplina da busca e apreensão, prevista nos artigos 240 a 250 do Código de Processo Penal.

Sem pretensão de historiar o instituto da busca e apreensão no ordenamento jurídico nacional, cabe ao presente trabalho os seguintes apontamentos. A disciplina legal da busca e apreensão data de 1940, tendo sido pensada para outra realidade político-social, em que os elementos de informação úteis à formação da convicção "seriam tangíveis e efetivamente materiais, não estando plenamente adaptado à realidade virtual dos dados"[71]. Ainda que a medida cautelar possa ter por objeto um elemento corpóreo como um aparelho celular, os elementos que efetivamente interessam ao desenvolvimento da persecução penal são os dados digitais armazenados no dispositivo.

No Brasil, foi paradigmático o julgamento do HC 91.867/PA, em que o STF enfrentou o questionamento sobre a ilicitude do levantamento de dados de ligações registradas em aparelho celular apreendido[72]. Embora a situação fática subjacente consista em prisão em flagrante, a discussão do caso tocou em aspectos jurídicos relevantes para a esta pesquisa. Em especial, chamou a atenção o paralelo feito pelo Ministro Gilmar Mendes entre a apreensão de documentos físicos e digitais, partindo do exemplo de uma agenda de papel com contatos anotados localizado no interior de uma

---

[70] BRASIL. Decreto 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, concluída em Budapeste, em 23 de novembro de 2001 e objeto de adesão pelo Brasil em 30 de novembro de 2022. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2023- 2026/2023/decreto/D11491.htm>. Acesso em: 1 ago. 2024.

[71] Idem, p. 143.

[72] BRASIL. Supremo Tribunal Federal. HC 91867. Segunda Turma. Relator Gilmar Mendes. Julgado em 24/04/2012. Publicado em 20/09/2012.

residência, cuja equiparação aos registros de ligações efetuadas a partir de um aparelho telefônico seria razoável, sob pena de se conferir menor proteção ao domicílio.

Posteriormente, o STJ também apreciou caso emblemático, no HC 51.531/RO, o qual também trata da apreensão de smartphone no contexto de prisão em flagrante, e subsequente análise de conversas de WhatsApp incriminadoras do suspeito, sem autorização judicial prévia[73]. O Ministro relator Rogério Schietii declarou a ilicitude da prova, realizando *distinguishing* em relação ao precedente do STF, tomando por ratio decidendi o avanço tecnológico pelo qual passaram os aparelhos telefônicos nos últimos anos, àquela altura já dotados de ampla capacidade de processamento e armazenamento de dados, capazes de revelar informações pessoais por anos a fio, descortinando, ao fim e ao cabo, aspectos profundos e sensíveis da personalidade do indivíduo. Conforme Zilli, a decisão foi inspirada no caso Riley v. California, julgado pela suprema corte dos Estados Unidos, "em que se proclamou a indispensabilidade de ordem judicial para o acesso ao conteúdo de dados mantidos em aparelho celular em contexto de prisão em flagrante[74].

Portanto, a construção jurisprudencial que passou a reconhecer a necessidade de autorização judicial para o acesso aos dados armazenados em celulares decorre da assunção fática de que a inexistência de controles e limites às devassas de informações e dados pessoais implicaria violação excessiva à intimidade da pessoa afetada pelo interesse probatório estatal.

Para Rebellato, a normativa existente pode se amoldar à busca e apreensão digital, tomando por base os seguintes pressupostos. Primeiro, a apreensão de aparelho

---

[73] BRASIL. Superior Tribunal de Justiça. HC n. 674.185/MG. Sexta Turma. Relator Ministro Sebastião Reis Júnior, julgado em 17/08/2021, publicado em 20/08/2021.

[74] O caso, relata o autor, "envolveu a prisão de Riley ocorrida após uma abordagem de trânsito. Uma vez constatada a suspensão da habilitação, os policiais realizaram os procedimentos de rotina, o que incluía a busca no interior do veículo. Foi quando encontraram armas de fogo, fato que justificou a prisão em flagrante. Nas buscas pessoais, encontraram em poder de Riley um aparelho celular o qual foi prontamente manuseado. Os policiais identificaram, então, referências constantes a uma abreviatura ("CK"), usualmente associada a gangues de rua (*Crip Killers*). Riley foi conduzido ao distrito onde um investigador fez uma pesquisa mais detalhada de seu aparelho celular. Após visualizar alguns vídeos e fotos, o investigador destacou uma imagem na qual Riley aparecia ao lado de um carro. Era o automóvel utilizado durante uma troca de tiros entre gangues, ocorrida semanas antes. Com base nesses elementos, Riley foi acusado por vários crimes, dentre os quais o envolvimento em organização criminosa". Cf. ZILLI, Marcos. A prisão em flagrante e o acesso a dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade. Em: Direitos fundamentais e processo penal na era digital / Dennys Antonialli, Jacqueline de Souza Abreu [editores]. -- São Paulo : InternetLab, 2018. -- (Doutrina e prática em debate ; v. 1).

celular é mero meio de passagem para o acesso aos dados nele armazenados, não havendo, em regra, interesse probatório na apreensão do dispositivo per se[75].

Em segundo lugar, na forma do artigo 240, § 1º, do Código de Processo Penal, a busca e apreensão de dados pessoais extraídos de dispositivos informáticos é cabível para se apreender documentos digitais obtidos por meios criminosos (alínea *b*), descobrir dados digitais necessários à prova da infração ou à defesa do réu (alínea *e*), bem como colher qualquer dado digital a ser considerado elemento de convicção (alínea *h*).

Terceiro, a decisão judicial deve demonstrar o *fumus comissi delicit* consubstanciado em indícios de autoria e prova de materialidade do delito em apuração, ao que se agrega o juízo de probabilidade de encontro de elementos relacionados ao fato criminoso; assim como o perigo de perecimento ou ocultação indevida da pessoa ou coisa de interesse para a prova de infração penal.

Em quarto, embora a decisão deva, na medida do possível, especificar e delimitar quais dados pessoais estão sujeitos à apreensão, não se trata de requisito obrigatório, dada a impossibilidade de o magistrado prever de antemão todas as informações potencialmente úteis à investigação criminal armazenadas no aparelho celular.

Como quinto argumento, com apoio no artigo 19.3 da Convenção de Budapeste, alega-se que a "apreensão de dados digitais poderá ser otimizada a partir da realização de cópia dos dados contidos no dispositivo móvel, mediante aparato técnico suficiente e com o auxílio de profissionais capacitados para a medida".

Teceremos a seguir considerações críticas a cada uma das condicionantes elencadas acima e, ao final, tomaremos posição.

2.2.1. Os limites da busca e apreensão

Conquanto o instituto da busca e apreensão esteja tratado no capítulo destinado aos meios de prova no Código de Processo Penal, é consenso que consiste, em realidade, em meio de obtenção de prova, na medida em que a busca e eventual apreensão de pessoa não reproduzem, por si só, situação de fato que se preste como prova. A busca consiste na procura por determinado elemento de prova, como um diário, uma correspondência ou mesmo um dispositivo informático. E, partir da localização da

---

[75] Rebellato, *op. cit.*, p. 147.

coisa ou pessoa de interesse à persecução criminal, será ultimada a apreensão. Portanto, em regra, a apreensão sucede a busca, havendo uma relação de meio e fim que justificou a disciplina conjunta pelo legislador.

Em algumas situações, no entanto, poderá a busca e a apreensão ocorrer de maneira independente. Caso o suspeito entregue voluntariamente o aparelho celular para que seja periciado, lavrar-se-á apenas o auto de arrecadação, dispensando-se, logicamente, a busca pelo smartphone.

O art. 240, § 1.º, do CPP prevê os casos em que é cabível a busca domiciliar: Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para: (i) prender criminosos; (ii) apreender coisas achadas ou obtidas por meios criminosos; (iii) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos; (iv) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso; (v) descobrir objetos necessários à prova de infração ou à defesa do réu; (vi) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato; (vii) apreender pessoas vítimas de crimes; (viii) colher qualquer elemento de convicção[76].

Não nos interessa, nos limites do presente estudo, historiar o instituto da busca e apreensão, muito menos analisar uma a uma das hipóteses de cabimento, as distinções da busca pessoal para a busca domiciliar, e o detalhamento procedimental do CPP, tarefa já exaustivamente executada a contento pela doutrina especializada. Mas sim apontar que o instituto da busca e apreensão são categorias jurídicas que, na atualidade, já não se mostram suficientes diante da complexidade dos direitos fundamentais afetados e suas correlatas garantias.

Essa constatação, conforme Gloeckner e Eilberg, decorre da própria adstrição da medida cautelar de busca ao devido processo legal, o que exige seguir diretrizes normativas estanques (requisitos do mandado, horário de cumprimento, limites da autorização), sob pena obtenção de prova ilícita; assim como a apreensão, contingente

---

[76] BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 1 ago. 2024.

em relação à busca, também rege-se por prescrições legais a respeito do auto circunstanciado dos objetos apreendidos[77].

Os autores ainda veiculam a ideia de que toda medida cuja finalidade seja a obtenção de prova caracteriza uma busca, independentemente do nome adotado pelo legislador, como seria o caso da busca por material genético como uma hipótese de identificação criminal. Nesse sentido, alertam para a necessidade de que novas modalidades de meio de obtenção de prova sejam tratadas como busca diante do avanço da tecnologia, por exemplo: (i) busca genética; (ii) busca de dados eletrônicos; (iii) buscas para a obtenção de metadados (incluindo números de celular, uso de cartão de crédito, envio de mensagens); (iv) buscas para localização via GPS, entre outros[78].

Resta-nos responder: à luz da dogmática constitucional que alicerça a proteção de dados pessoais, está autorizada o vasculhamento (busca) e extração (apreensão) de dados de celulares?

Para responder a esse questionamento, partimos de três premissas:

(i) Da possibilidade de o aparelho celular - assim como qualquer outro dispositivo informático, se obtido por meio criminoso (por exemplo, celular receptado) ou utilizado para fins criminosos (para a combinar a entrega de determinada quantia de drogas por membros de uma associação para o tráfico) - ser passível de apreensão não decorre uma autorização implícita para acesso aos dados nele contidos;

(ii) A ordem judicial que decreta a busca e apreensão, seja domiciliar ou pessoal, desde que devidamente fundamentada, contém uma autorização implícita de vulneração ao direito à intimidade das pessoas afetadas pela medida interventiva. Afinal, o suspeito que tiver a casa invadida por agentes policiais para remexer seus pertences e o seu próprio corpo, inexoravelmente estará diante de uma situação de restrição provisória de seu espaço privado.

(iii) A obtenção e a utilização de dados pessoais para fins de persecução penal é admitida pela legislação. Nesse sentido, retomemos as autorizações legais para acesso aos dados de comunicações privadas em fluxo (art. 2º da Lei nº

[77] Gloeckner, *op. cit.*, p. 2.
[78] *Ibid.*, p. 4.

9.296/96) ou armazenadas (art. 7º, III, do Marco Civil da Internet), dados cadastrais (art. 10, § 3º), registros de conexão e de acesso a aplicações de internet, bem como, em casos excepcionalíssimos, dados de localização de usuários de serviços de internet (art. 13-B do CPP).

Em relação à primeira premissa, retomamos concepção de que regras de competência não implicam autorizações e que a reserva legal no processo penal exige que as intervenções em direitos fundamentais devem ser expressamente previstas, não se admitindo autorizações implícitas, sob pena de violações desmedidas e desproporcionais sempre que a autoridade envolvida na persecução penal justificar, com mero de jogo de palavras, uma suposta decorrência lógica entre uma intervenção expressa anterior e uma intervenção implícita posterior. Além disso, Gloeckner e Eilberg demonstram que a, antes da revolução digital, não havia a possibilidade de alguém trazer consigo número equivalente de informações, dados pessoais e documentos, que o armazenamento em celular atualmente permite[79]:

> Sem dúvidas, o paralelo com os documentos físicos (objeto da decisão no caso Olmstead e que serviu durante largo tempo para a Suprema Corte americana balizar as suas decisões) é absolutamente inapropriado, pois o conteúdo apreendido em um dispositivo celular seria o equivalente a alguém ter apreendido milhares de fotos, um computador, uma câmera digital, cartão e conta bancária, enfim, uma gama enorme de informações que jamais seriam apreendidos em um único momento estando na posse de um sujeito.

A segunda premissa relaciona-se com o requisito da delimitação, pelo magistrado que autorizar a medida interventiva, sobre quais dados poderão ser acessados, em qual espaço de tempo e para qual finalidade. Em outras palavras, a autorização judicial por si só não basta, devendo o magistrado realizar juízo de prognose à luz do fato penal objeto de apuração pelo órgão investigativo, com o intuito de mitigar a exposição da intimidade do indivíduo.

Para Rebellato, a impossibilidade de o julgador antever todos os dados existentes no aparelho celular apreendido não impede a decretação da medida interventiva, senão isenta-o da obrigação de descrever pormenorizadamente, pois não se pode exigir que julgador realize um exercício de futurologia probatória, que lhe possibilite identificar e

---

[79] *Ibid*., p. 5.

delimitar com precisão todos os elementos que possam guardar relação com os fatos que se deseja provar[80].

Ainda que se possa concordar com a dificuldade de o magistrado exercer um de juízo prévio de delimitação da medida intrusiva, esse é um ônus que deve ser suportado pelo Estado, afinal

> o fato de que não há legislação específica sobre o acesso ao conteúdo do celular é diverso da afirmação de que se trata de um conteúdo de acesso "livre" às autoridades públicas. Interpretando-se rigorosamente todos os impactos trazidos pelas tecnologias móveis, a justaposição de inúmeros aplicativos em apenas um dispositivo não apenas reclama a reserva jurisdicional. O acesso aos distintos aplicativos reclama autorizações judiciais precisas: acesso a mensagens trocadas pelo WhatsApp, acesso a dados bancários, acesso a contas de e-mail, tudo isso reclama da autoridade judicial que Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos examine as distintas formas de afastamento da privacidade. Assim, a rigor, para que a polícia examine dados bancários, telefônicos, contas de e-mail, o aplicativo WhatsApp, tudo deve ser detalhadamente requerido e examinado pelo juízo, sob pena de se estabelecer indevidas quebras não autorizadas a sigilos protegidos pela lei e pela Constituição da República. Aliás, o acesso ao telefone celular, mediante uma autorização genérica, poderia consistir em um "atalho" que facilitaria, mediante apenas um pedido e uma decisão, acesso a múltiplas dimensões da privacidade, considerando que o aparelho celular, como já referido, é, ao mesmo tempo, um facilitador e um mecanismo de armazenamento de informações[81].

Ademais, como aponta Sousa Mendes, é admissível que os agentes de persecução utilizem técnicas forenses que permitam restringir a pesquisa e apreensão somente aos arquivos que contenham palavras-chave específicas relacionadas aos crimes investigados sob o mandado judicial.

Aliás, ainda que tal método não possa ser imposto judicialmente, ele será naturalmente preferível a todos os envolvidos nos casos em que a investigação dispuser de informações que conformem maior exatidão ("smoking gun evidence") sobre o arquivo ou informação buscada. Nesse sentido, a utilização de palavras-chave será preferível pelas autoridades de investigação pois evitam a obtenção de material irrelevante e que reduziria a eficiência da apuração; igualmente, será preferível pelos titulares de dados sujeitos à medida interventiva, na medida em que a devassa à privacidade seria

---

[80] Rebellato, *op. cit.*, p. 147.
[81] Gloeckner, *op. cit.*, p. 6.

restringida, atendendo-se os postulados de necessidade e adequação decorrentes do princípio da proporcionalidade.

Em relação à terceira premissa, as disposições são dirigidas às empresas provedoras de conexão e de aplicações de internet, operacionalizando verdadeira extração remota de dados, isto é, sem a necessidade de um dispositivo físico no qual as informações estejam gravadas na memória, inexistindo previsão legal expressa para que sejam aplicadas, por analogia – *in malam partem* -, em relação aos indivíduos que tiverem seus smartphones apreendidos. E, se nem mesmo essa analogia parece possível à luz do princípio da legalidade, a extração de dados pessoais outros, como arquivos de fotos, vídeos, agenda etc., mostra-se ainda mais grave, eis que inexistente paralelo na legislação em relação às extrações remotas de dados, tornando ilimitadas e impassíveis de controle as práticas atualmente em curso pelas Polícias Judiciárias.

Em suma, todas essas premissas não infirmam o déficit de legalidade que permeia o desatualizado instituto da busca e apreensão, na medida em que inexistente autorização expressa para que, ultrapassada a primeira barreira da intimidade física, tangível, possam os atores da persecução mover um espaço além, intangível, da personalidade desenvolvida no plano digital, aprofundando-se no âmago dos dados pessoais - potencialmente - armazenados por anos a fio.

2.2.1.1. O conceito de domicílio: (im)possibilidade de equiparação ao smartphone

O conceito de domicílio é tradicionalmente ligado a um espaço físico delimitado, que pode ser tanto individual, como uma residência, no interior da qual o indivíduo tem a legítima expectativa de desenvolver livremente a sua personalidade e manter laços afetivos protegido, bem como coletivo, como uma empresa ou estabelecimento religioso, nos quais atividades profissionais visando o lucro ou a adoração da fé e da espiritualidade podem ser praticados sem o que o Estado possa, em princípio, intervir.

Porém, para os propósitos desse capítulo, em que discutimos a abrangência e os limites do instituto da busca e apreensão no processo penal e a sua relação com medidas intrusivas de acesso a dados armazenados em smartphone, é pertinente abordar a posição de Madeira Dezem. Segundo ele, o conceito de domicílio precisa ser reinterpretado à luz dos avanços tecnológicos e das novas possibilidades de interação

com o mundo proporcionadas por aparelhos de celular que não mais se limitam a fazer e receber ligações. Por se tratar de dispositivo com capacidade operacional equivalente a de um computador, o smartphone se tornou o espaço em que o indivíduo atualmente desenvolve a sua vida privada, já que nele armazena fotos e conversas íntimas, registros bancários, documentos profissionais entre outras funcionalidades que dizem respeito apenas ao proprietário do dispositivo, a quem cabe decidir o que tornar público ou não[82].

Sob essas premissas, conquanto não se trate de um espaço físico, o smartphone contempla as características que justificaram a proteção jurídica diferenciada do domicílio físico, razão pela qual propõe a expansão do conceito de domicílio para qualquer espaço, físico ou digital (intangível), em que o indivíduo possa manter dados e informações relativas à vida privada, e receber o mesmo tratamento dispensado a uma residência ou sede de uma empresa, no que toca aos requisitos de uma busca e apreensão para fins de prova de fatos constitutivos de crime[83]. Em outras palavras, mediante prévia autorização judicial e observados os requisitos do subsequente mandado, entende ser legítima e legalmente amparada a busca – ou coleta, na acepção da LGPD – de dados armazenados em um smartphone apreendido.

Com fundamento no art. 6º do MCI, o autor ainda argumenta que a intepretação dos dispositivos de tal lei – que em nada se relacionam com o fornecimento de dados armazenados em dispositivos informáticos, mas sim ao acesso de dados cadastrais e registros de acesso dirigidos aos provedores de conexão e de aplicação de internet (vide 1.3.2) – seria aplicáveis à proteção domiciliar na internet, que é utilizada como local de exercício da vida íntima e privada, mas que também não se confunde com a totalidade de informações registradas em um smartphone[84].

Essa tese não passa ilesa de críticas. Para Zilli, não é possível desconectar a ideia de “cara” enquanto espaço físico demarcado e estável de proteção do indivíduo e da

---

[82] 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).
[83] *Ibid.*, p. 473.
[84] *Ibid.*, p. 474.

família, razão pela qual a transposição para o ambiente digital e a própria portabilidade do smartphone se apresentam como uma “metáfora exagerada”. Isso 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[85].

Em nosso entendimento, Rebellato acertadamente refuta a proposta de reinterpretação do conceito de domicílio que extrapola os limites do espaço físico, ao abordar o tema o sob a ótica do direito civil. Com fundamento no art. 70 do CC, aponta que o domicílio implica na fixação de residência de forma definitiva, ideia inexoravelmente ligada à existência de um espaço físico, e que gera implicações em outras esferas do direito, razão pela qual seria temerária a ressignificação do conceito ainda para fins estritamente processuais penais[86].

Por fim, é digna de nota a alusão feita por Felipe de Castro quanto ao aparelho celular ter características de uma prótese corporal com capacidade de potencializar as habilidades e os sentidos dos seres humanos, como a comunicação e a memória, com a nota distintiva de que o dispositivo se mantém funcional mesmo separado do corpo. A ideia de prótese, conquanto possa soar estranha em um primeiro momento, faz sentido, segundo o autor, partindo da premissa de que materiais orgânicos podem ser livremente descartados uma vez fora do corpo, diante da perde de função, mas o aparelho celular continua operante no campo digital mesmo fisicamente separado do proprietário[87]. Por esse motivo, um celular não é equivalente a material biológico encontrado no local do

---

[85] Zilli, *op. cit*, p. 88-89.

[86] Alguns exemplos: o domicílio do réu é critério de fixação de competência no direito civil (artigo 46 do Código de Processo Civil). Igualmente, o domicílio tributário do Código Tributário Nacional pressupõe um local de residência habitual (artigo 127, inciso I, da Lei n.º 5.172/1966). Rebellato, *op. cit.*, p. 159.

[87] FELIPE DE CASTRO, Matheus. Um celular na cena do crime: o STF e a proteção de dados estáticos. Consultor Jurídico. São Paulo, 20 set. 2024. Disponível em: <https://www.conjur.com.br/2024-set-20/um-celular-na-cena-do-crime-o-stf-e-a-protecao-dos-dados-estaticos/>. Acesso em: 24 set. 2024.

crime e, entendemos, tampouco pode ser equiparado ao conceito de domicílio para fins probatórios no processo penal.

2.3. Encontro fortuito de provas na busca e apreensão virtual de dados pessoais e a doutrina da visibilidade imediata

Para a sustentação dos argumentos acima apresentados, cabe testá-lo mediante o acréscimo de mais uma problemática, no que se refere à descoberta inesperada de dados pessoais aptos a comprovar infração penal não inicialmente vislumbrada e apontada como justificativa para a realização da medida interventiva nos direitos fundamentais do titular afetado.

Suponha-se que numa investigação de tráfico de entorpecentes, os agentes policiais obtenham um mandado judicial que autorize a extração de dados de celular apreendidos do suspeito e, analisando os ficheiros, deparam-se com material compatível como pornografia infantil. Em vez de solicitarem uma autorização complementar para o aprofundamento das buscas de outros elementos desse crime que não compunha os objetivos iniciais da diligência – elucidar a autoria de mercancia ilícita de drogas -, os agentes policiais empreenderam pesquisas para localizar material de exploração sexual infantil, justificando, posteriormente, que assim o fizeram pois estavam diante de uma causa provável de aquilatar mais arquivos de imagem no material obtido com a extração de dados[88].

Nos Estados Unidos, as consequências jurídicas desse tipo de busca exploratória foram bem desenvolvidas por meio da doutrina jurisprudencial da visibilidade imediata

[88] O exemplo é inspirado no caso Estados Unidos vs. Carey (1999), cujas investigações inicialmente tinham por foco apurar tráfico de drogas, e no curso da qual houve apreensão e busca em um computador pertencente a Patrick J. Carey. Os agentes encontraram acidentalmente arquivos de pornografia infantil. A defesa do imputado argumentou que a descoberta dos arquivos de pornografia infantil excedeu o escopo do mandado de busca original e, portanto, violava a Quarta Emenda (proteção contra buscas e apreensões não razoáveis). O caso foi submetido ao Tribunal de Apelação do Décimo Circuito dos Estados Unidos da América, onde se decidiu que a descoberta fortuita de pornografia infantil não era admissível porque os agentes não tinham permissão para buscar esse tipo de evidência sem um mandado específico. A singularidade do caso decorre do fato de que o mandado judicial autorizara pesquisas no computador de Carey por meio de palavras-chave, razão pela qual os arquivos de imagem eram inacessíveis a priori. Porém, os investigadores transferiram o material para outros dispositivos informáticos, o que lhes permitiu abrir os arquivos de imagem e identificar o conteúdo infringente, levando o Tribunal de Apelação a julgar inaplicável da doutrina da visibilidade imediata, que será abordada neste tópico.Cf. SOUSA MENDES, PAULO DE, 2020: «A privacidade digital posta à prova no processo penal», in Quaestio facti, 2: 225-250. Madrid: Marcial Pons Ediciones Jurídicas y Sociales. DOI: http://dx.doi.org/10.33115/udg_bib/qf.i2.22487.

(*plain view doctrine*). Trata-se de uma exceção ao requisito constitucional de obtenção de mandado judicial para a realização de buscas e apreensões. De acordo com essa doutrina, qualquer objeto apreendido por um agente da autoridade que esteja atuando sem um mandado judicial ou além do escopo de um mandado pode ser utilizado como prova de um crime, desde que sejam cumpridas três condições: (i) a evidência deve estar visível de imediato; (ii) o agente deve ter uma justificativa prévia para estar no local de onde avistou a evidência; (iii) a evidência, por si só ou juntamente com outros fatos conhecidos pelo agente no momento da apreensão, deve fornecer uma probabilidade razoável de que haja uma conexão entre a evidência e alguma atividade criminosa. Conforme Sousa Mendes:

> A doutrina jurisprudencial da visibilidade imediata baseia-se na experiência empírica da percepção visual no mundo físico. No mundo cibernético, porém, não há, em princípio, analogia com a visão no mundo físico. Um objeto pode ser imediatamente avistado no mundo físico, ao passo que um ficheiro informático só pode ser visto se for aberto. Aquilo que se vê imediatamente é apenas o nome do ficheiro, que pode nem ser revelador do respetivo conteúdo. Esta dificuldade tem dado azo a uma rica casuística no direito jurisprudencial norte-americano[89].

Poder-se-ia cogitar que tal possibilidade restaria amparada pelo tema 280, em que o STF fixou a tese segundo a qual a entrada forçada em domicílio, em razão de flagrante delito, deve ser justificada concretamente a posteriori, expandindo-se o conceito de domicílio, em que manifestada a intimidade de maneira tangente, o computador pessoal[90].

Entendemos que essa interpretação e a adoção da teoria de maneira geral é incompatível com o ordenamento jurídico brasileiro, porquanto abre margem para a execução de medidas interventivas mais gravosas que a própria busca e apreensão, para além dos limites da autorização judicial ou mesma na inexistência de mandado, o que

---

[89] Sousa Mendes, *op. cit.*, p. 242.

[90] No julgamento do RE 603616, em que se analisou à luz do art. 5º, XI, LV e LVI, da Constituição Federal, a legalidade, ou não, das provas obtidas mediante invasão de domicílio por autoridades policiais sem o devido mandado judicial de busca e apreensão, o STF fixou a tese de que entrada forçada em domicílio sem mandado judicial só é lícita, mesmo em período noturno, quando amparada em fundadas razões, devidamente justificadas a posteriori, que indiquem que dentro da casa ocorre situação de flagrante delito, sob pena de responsabilidade disciplinar, civil e penal do agente ou da autoridade, e de nulidade dos atos praticados. Conforme veiculado em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=3774503&numeroProcesso=603616&classeProcesso=RE&numeroTema=280>. Acesso em: 22 ago. 2024.

potencialmente gera concentração de poderes excepcionais aos órgãos de persecução penal.

2.4. O poder geral de cautela e os meios atípicos de produção de prova no processo penal

Estabelecidos os marcos normativos que disciplinam a intervenção em direitos fundamentos relativos ao tratamento de dados pessoais no processo penal, a ausência de previsão legal da extração forçada de dados pessoais e refutados os argumentos sobre a compatibilidade entre tal meio (atípico) de obtenção de prova com o instituto da busca e apreensão, cabe analisar, à luz do art. 3º do CPP, o cabimento da medida interventiva com base no poder geral de cautela do juiz.

O moderno processo penal, ao refutar a busca da verdade a qualquer custo, persegue o equilíbrio entre o exercício do *ius puniendi* e a preservação dos direitos fundamentais. A necessidade de restringir direitos fundamentais em prol da eficiência da persecução faz que todo o processo penal submeta-se ao princípio da legalidade estrita. Conforme leciona Antonio Magalhães Gomes Filho[91]:

As medidas cautelares penais têm o condão de assegurar o objeto do provimento final almejado no processo penal, caracterizando-se pela instrumentalidade, pela acessoriedade, pela preventividade, pela sumariedade e pela provisoriedade[92]. Ao contrário da jurisdição cível, na qual há verdadeiro "processo" cautelar, no processo penal a tutela cautelar se operacionaliza pela formação de incidentes processuais visando a assegurar algum objetivo pertinente ao processo penal, durante o tempo necessário para o seu desenvolvimento.

---

[91] Conforme leciona Antonio Magalhães Gomes Filho: "o princípio da legalidade dos delitos e das penas não diz respeito apenas ao momento da cominação, mas à legalidade da inteira repressão, que põe em jogo a pessoa desde os momentos iniciais do processo até a execução da pena imposta.(...) a lei processual deve tipificar tanto as condições de aplicação, como o conteúdo das intromissões dos poderes públicos no âmbito dos direitos fundamentais dos cidadãos". In Medidas cautelares e princípios constitucionais: comentários ao art. 282 do CPP, na redação da Lei 12.403/2011. In: GOMES FILHO, Antonio Magalhães et al. (FERNANDES, Og, coord.), Medidas cautelares no processo penal: prisões e suas alternativas: comentários à Lei 12.403, de 04.05.2011, São Paulo, Revista dos Tribunais, 2011, p.18.

[92] Gustavo Henrique Badaró leciona que "as medidas cautelares surgem como um instrumento que assegura o provimento final. No entanto, como normalmente, a instrução ainda não está concluída, não se pode decidir com base em um juízo fundado em cognição profunda e exauriente. (...) A tutela cautelar é preventiva, isto é, sua finalidade é prevenir a ocorrência de um dano irreparável ou de difícil reparação, durante o tempo necessário para que se desenvolva o devido processo legal (...). A tutela cautelar tem duração limitada àquele período de tempo que deverá transcorrer entre a instauração do procedimento

No processo penal, não prevalece a lógica de que aquilo que não está proibido é permitido. As restrições a direitos dependem de prévia cominação legal. Não por outro motivo, tanto a doutrina processual penal[93] quanto a jurisprudência refutam a existência de um poder geral de cautela dos juízes criminais para restringir direitos. As cautelares penais das cautelares civis em razão da tipicidade das primeiras, que são taxativamente previstas em lei. Em matéria penal, a legalidade estrita rege tanto o direito material quando o processo, sendo vedado aos juízos criminais inovar e aplicar medidas não previstas em lei de antemão[94]. O fato de o legislador ter definido um rol de medidas cautelares penais é garantia ao acusado de que não poderá ter seus direitos restritos antes do trânsito em julgado de sentença condenatória (artigo 5º, LVII, da Constituição da República), a não ser nas hipóteses claramente inscritas em lei.

Também se diferenciam as cautelares penais das cautelares civis em razão da tipicidade das primeiras, que são taxativamente previstas em lei. Em matéria penal, a legalidade estrita rege tanto o direito material quando o processo, sendo vedado aos juízos criminais inovar e aplicar medidas não previstas em lei de antemão. O juiz da jurisdição penal não possui autoridade para empregar medidas atípicas ou não previstas na lei. No processo penal, não existem medidas cautelares inominadas. Sempre que o juiz recorre a esse controverso poder geral de cautela, ele está, na verdade, infringindo o princípio da legalidade. No processo penal, a forma é uma garantia. O juiz só está

---

cautelar e a promulgação do procedimento definitivo.". BADARÓ, Gustavo Righy Ivahy. *Processo penal*. 2ª ed. Rio de Janeiro: Elsevier, 2014, p. 705.

[93] BADARÓ, Gustavo Henrique Righy Ivahy. *Processo penal,* 2ª ed.. Rio de Janeiro: Elsevier, 2014, p. 710.

[94] Conforme Badaró "O princípio da legalidade também se aplica às medidas cautelares. No processo penal, mormente em tema de prisão processual, não existem medidas cautelares atípicas. Não há, como no processo civil, a previsão de um poder geral de cautela do juiz que o autorize a decretar medidas cautelares não previstas em lei". BADARÓ, Gustavo Righy Ivahy. *Processo penal*. 2ª ed. Rio de Janeiro: Elsevier, 2014, p. 705. No mesmo sentido, Luiz Flávio Gomes: "O juiz da jurisdição penal não tem poderes para lançar mão de medidas atípicas ou não previstas em lei. Não existem medidas cautelares inominadas no processo penal. Todas as vezes que o juiz lança mão desse famigerado poder geral de cautela, na verdade, ele está violando o princípio da legalidade. No processo penal, forma e garantia. O juiz só está autorizado a praticar os atos que contam com forma legal. Se o juiz se distancia da forma legal, resulta patente a violação à legalidade". Cf. GOMES, Luiz Flávio e MARQUES, Ivan Luís. Prisão e Medidas Cautelares – Comentários à Lei 12.403, de 4 de maio de 2011: São Paulo: Editora Revista dos Tribunais, 2011, p. 150.

autorizado a realizar atos que estão legalmente previstos. Qualquer afastamento das formas legais por parte do juiz resulta em uma clara violação da legalidade[95].

Trata-se de verdadeira inovação em tema de medidas cautelares penais para restringir a intimidade e a proteção de dados pessoais, do que decorre sua manifesta ilegalidade.

2.5. Síntese parcial

1. A apreensão de aparelhos celulares é de interesse para os propósitos de uma investigação criminal – demonstrar a ocorrência de um fato típico penal e identificar o autor desse fato – na medida em que existem, atualmente, ferramentas tecnológicas de extração forçada dos dados armazenados nesses dispositivos móveis, prática cunha como *hacking* governamental.
2. Não existe legislação específica que regulamente, para fins de persecução penal, a utilização de ferramentas de tal natureza, o que já demonstra o não atendimento ao primeiro pressuposto da dogmática constitucional em matéria de proteção de dados pessoais nos meios digitais, qual seja, a reserva de lei.
3. A Convenção de Budapeste, conquanto tenha instituído poderes e mecanismos de acesso a dados em sistemas de computador ou dados nele armazenados - no que se inclui o acesso a dados de celular -, relegou às Partes signatárias a obrigação de regular, por meio da legislação interna, as condições, garantias e hipóteses em que tais procedimentos e medidas interventivas poderão ser utilizados na persecução penal.
4. Por rigor científico, demonstramos que os contornos dogmáticos do instituto da busca e apreensão não podem ser esticados a ponto de permitir que, para além da apreensão do próprio aparelho celular de interesse à prova de determinada infração penal, os dados armazenados no dispositivo sejam extraídas como consectário lógico da execução da medida interventiva. De um lado, se é verdade

[95] Também comungam dessa posição Luiz Flávio Gomes e Ivan Luís Marques. GOMES, Luiz Flávio e MARQUES, Ivan Luís. Prisão e Medidas Cautelares – Comentários à Lei 12.403, de 4 de maio de 2011: São Paulo: Editora Revista dos Tribunais, 2011, p. 150

que é impossível, ao julgador, antever e delimitar quais dados poderão ser extraídos e tratados do celular apreendido, de outro, é igualmente certo que o universo de dados atualmente armazenados em dispositivos com funcionalidades de microcomputadores, é muito superior que a quantidade de informações, em substrato físico, que um indivíduo usualmente costuma manter em sua residência ou local de trabalho – o que escancara o absoluto descompasso entre a proteção de dados pessoais, alicerçada pela proporcionalidade e a finalidade, em relação aos danos colaterais da busca e apreensão de dados.

5. A validade do encontro fortuito de informações e dados pessoais armazenados em aparelhos celulares apreendidos, com base na teoria jurisprudencial norte-americana da visibilidade imediata esbarra, uma vez mais, no problema da reserva legal. É dizer: não havendo autorização para a intervenção inaugural, de acesso aos dados do dispositivo para outra finalidade, a intervenção secundária também esbarrará na falta de permisso legal.
6. No processo penal, não é admissível a invocação de um poder geral de cautela para a inovação em matéria de medidas cautelares que causem intervenção em direitos fundamentais, ainda que a pretexto de proteger interesses estatais, como a melhor eficiência da persecução penal. O princípio da tipicidade, já amplamente enraizada entre os penalistas, também dá concretude ao princípio da legalidade no processo penal, ao exigir forma e procedimento específico para cada intervenção em direito fundamental provocada no decorrer da apuração de crimes, desde prisões provisórias até acessos não consentidos de dados pessoais privados armazenados.

3. Pressupostos de lege ferenda para o acesso a dados armazenados em smartphones apreendidos

Há um aparente antagonismo entre as visões que defendem o tratamento de dados para uma melhor e mais eficiente prestação de serviços públicos, incluindo o processamento de infrações penais, de um lado, e a proteção da privacidade e dos dados pessoais, de outro, como se o pêndulo para um dos lados, coibisse a importância do outro[96]. A superação dessa dicotomia passa por reconciliar e equilibrar mecanismos protetivos do cidadão em relação ao uso abusivo de seus dados, enquanto projeção da personalidade humana – contra ações de vigilância massiva, recriminação de grupos políticos dissidentes, persecução de integrantes de classes socialmente vulneráveis - com a necessidade de execução de atividades econômicas e estatais. A criação de regras claras quanto às possibilidades de tratamento legítimo para fins de persecução penal dos dados obtidos de aparelhos de telefonia móvel é o desafiam a edição de ato normativo que contemple, no mínimo, os requisitos abaixo desenvolvidos.

3.1. Edição de lei prévia

As proposições da dogmática constitucional em matéria de proteção de dados pessoais desenvolvidas nesse trabalho confirmam a máxima da proibição com reserva de permissão, admitindo-se apenas as medidas interventivas para fins de produção de prova em investigações e processos criminais que estejam expressas em lei em sentido estrito, o que adjetiva o tipo de norma idônea a tal propósito. Trata-se de indelével reflexo da vontade popular de cada Estado soberano no que toca às formas de compatibilizar interesses persecutórios e a necessidade de reprimir delitos complexos – o que inexoravelmente passa pelo tratamento de dados contidos em sistemas informáticos – com a adequada proteção aos direitos fundamentais. Faremos, a seguir, um estudo

[96] WIMMER, Miriam. Cidadania, Tecnologia e Governo Digital: Proteção de Dados Pessoais no Estado Movido a Dados. In: Alexandre F. Barbosa. (Org.). TIC Governo Eletrônico 2019. Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. 1ed.São Paulo: Comitê Gestor da Internet no Brasil, 2020, v. 1, p. 27-36.

prospectivo das condições e garantias mínimas a serem contempladas por eventual lei que venha a regular a matéria[97].

3.1.1. Hipóteses de cabimento à luz do princípio da proporcionalidade

Como referido em 2.1, o direito à privacidade, à proteção dos dados pessoais nos meios digitais ao sigilo de dados telemáticos não são absolutos. No entanto, como toda intervenção na esfera de direitos fundamentais, o afastamento desses sigilos e a intromissão na esfera privada dos cidadãos, além de legalmente autorizadas, devem ocorrer por necessidade, de forma adequada e na justa medida[98].

As principais manifestações da proporcionalidade em sentido estrito [99] no ordenamento jurídico brasileiro, em matéria de intervenção em direitos fundamentais, encontram-se nas LC nº 105/2001 e da Lei nº 9.296/1996 artigo 2º, III, da Lei Federal nº 9.296/96 não autoriza as interceptações – assim como as quebras de sigilo armazenado, como exposto acima –, quando (i) não houver indícios razoáveis de autoria ou participação em infração penal (inciso I); (ii) a prova puder ser feita por outros meios

---

[97] Weiblen bem esclarece a cronologia de problemas concretamente enfrentados pelos poderes do Estado na regulamentação de novas tecnologias no processo penal: “as bases de autorização existentes no processo penal devem ser constantemente analisadas a respeito de sua adequação às medidas investigativas. O ideal é que isso seja feito pelos Poderes Executivo e Legislativo, porém, na prática, o Judiciário acaba por ser a instância na qual há a primeira análise dessa adequação. De fato, a experiência mundial demonstra que a construção de disciplina adequada de meios investigativos inovadores passa, em geral, pelas seguintes fases: prática policial sem regulamentação; primeiros problemas jurídicos; previsão legal com regulamentação insuficiente; nova experimentação prática; novos problemas jurídicos; e, por fim, regulamentação adequada, em uma "tipificação processual progressiva". Parece evidente que há. um descompasso entre o progresso tecnológico e a utilização dessas ferramentas pela criminalidade (notadamente aquela organizada e mais grave), em comparação com o ritmo do legislador na elaboração de normas legais que possibilitem expressamente o uso de novas tecnologias . WEIBLEN, Fabrício Pinto. O uso de software espião na investigação criminal: interpretação aberta à tecnologia, (in)admissibilidade e tratamento jurídico adequado. Londrina, PR: Thoth, 2024, p. 39.

[98] TOLEDO DE BARROS, Susana, O princípio da proporcionalidade e o controle de constitucionalidade das leis restritivas de direitos fundamentais. 2. ed. Brasília, Brasília Jurídica, 2000, p. 91.

[99]Conforme leciona Luiz Roberto Barroso, a proporcionalidade consiste em critério para aferir a legitimidade das restrições a direitos fundamentais: “Referida como prinípio, máxima ou postulado, ela se tornou um mecanismo de controle dividido em três etapas, nas quais se vai verificar: (i) a *adequação* de uma medida para produzir determinado resultado (idoneidade do meio para o fim visado); (ii) a *necessidade* da providência, sendo vedado o excesso (se houver meio menos gravoso para se atingir o o mesmo fim, é ilegítimo o emprego do meio mais gravoso) e (iii) a *proporcionalidade em sentido estrito*, pela qual se afere se o fim justifica o meio, vale dizer, se o que se ganha é mais valioso do que aquilo que se sacrifica”. BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo - 8. ed. - São Paulo: Saraiva, 2019.

menos gravosos disponíveis (inciso II) e (iii) o fato investigado constituir crime apenado, no máximo, com detenção (inciso III).

Ao vedar o afastamento do sigilo sobre comunicações privadas para a investigação e instrução processual penal dos crimes apenados com detenção, estabeleceu-se, no próprio texto legal, critério de proporcionalidade em sentido estrito a ser observado pelo Poder Judiciário no exame de cada pedido de quebra. A gravidade abstrata dos delitos norteia a distinção entre os crimes apenados com reclusão e detenção, conforme observa Luiz Regis Prado[100]. Ao vedar as quebras de sigilo de comunicações telemáticas para crimes apenados com detenção, o artigo 2º, III, da Lei Federal nº 9.296/96 claramente estabelece que apenas as infrações penais objetivamente reputadas mais graves poderão dar ensejo a tão extrema vulneração da intimidade.

3.1.2. Responsabilidades dos agentes responsáveis pelo tratamento de dados

A definição legal, para fins de persecução penal, desses agentes de tratamento de dados, seja mediante a aprovação do PL 1515/22, seja mediante a edição de lei própria que regule a extração e demais atividades de dados obtidos de aparelhos de telefonia móvel, é providência necessária para fixar e distribuir responsabilidades pelas operações.

3.1.2.1. O controlador e o operador de dados

A LGPD criou três figuras relacionadas ao tratamento de dados pessoais, reproduzidas no Anteprojeto da LGPD Penal[101]. Como brevemente referido no item 2.3.4, ao controlador de dados é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”. Cabe ao controlador definir a finalidade e os motivos para o tratamento de dados pessoais[102]. Em

---

[100] PRADO, Luiz Régis. Curso de direito penal brasileiro, vol. I – Parte Geral, 15ª ed., São Paulo, Revista dos Tribunais, 2017, p.351.

[101] Embora sem adotar os conceitos dados pela LGPD, o Anteprojeto menciona as aborda as figuras do controlador, do operador e do encarregado de dados no Capítulo V. Disponível em: https://imagem.camara.gov.br/Imagem/d/pdf/DCD0020220622001010000.PDF#page=593. Acesso (online) em 13/08/2024.

[102] De LIMA, Cíntia Rosa Pereira. Agentes de tratamento de dados pessoais (controlador, operador e encarregado pelo tratamento de dados pessoais). In Comentários à lei geral de proteção de dados: Lei n.

atividades de investigação criminal, parece intuitivo que os órgãos de Polícia Judiciária e dos ministérios públicos, diretamente interessados na obtenção de dados pessoais para fins de prova do fato penal pretérito que se busca reconstruir e da respectiva autoria, sejam legitimados na posição de controladores. Porém, essa possibilidade não é única.

Por sua vez, o operador, que também pode ser pessoa natural ou jurídica, de direito público ou privado, realiza o tratamento de dados pessoais em nome do controlador. Na prática atualmente em curso no país em relação às ferramentas de extração forçada de dados de smarphones apreendidos no contexto de uma investigação criminal, não se sabe se os programas comumente utilizados pelas agências são totalmente operados pelos próprios servidores públicos ou se há a intervenção e a realização de alguma operação a cargo das empresas que comercializaram ao Poder Público os softwares utilizados – o que dificulta a atribuição de responsabilidades por violações à proteção de dados pessoais e à operações e compartilhamentos clandestinos.

A propósito, o Capítulo V da LGPD, que regulamenta as atividades dos agentes de tratamento de dados pessoais, cria uma série de obrigações e procedimentos relevantes à hipótese que tratamos no presente estudo, como: (i) o dever de manter registro das operações de tratamento de dados pessoais (art. 37); (ii) o dever de produzir relatório de impacto à proteção de dados pessoais quando requisitado pela autoridade nacional (art. 38), contendo a descrição dos tipos de dados coletados, a metrologia utilizada na coleta, mecanismos de segurança da informação e mitigação dos riscos adotados; (iii) a obrigação de o operador realizar o tratamento de dados seguindo as instruções passadas pelo controlador (art. 39); e (iv) responsabilidade e dever ressarcimento de danos de ordem patrimonial, moral, individual ou coletivo, por violação à legislação de proteção de dados pessoais (art. 42), prevendo (iv.1) a responsabilidade solidária do operador quando violar a lei ou descumprir as instruções do controlador; v(dever de notificação sobre a ocorrência de incidente de segurança que coloque em risco ou cause dano relevante aos titulares de dados pessoais (art. 48). Também instituí

13.709/2018, com alteração da lei n. 13.853/2019 / coordenadora Cíntia Rosa Pereira de Lima – São Paulo: Almedina, 2020, p. 290.

garantias de que os agentes de tratamento não serão responsabilizados quando (i) não realizarem o tratamento de dados pessoais que lhes é atribuído (art. 43, I); (ii) não tiverem descumprimento a legislação ou, ainda, (iii) quando o dano decorrer de culpa exclusiva do titular ou de terceiro.

A legislação atual, que não se aplica às atividades de persecução penal, ainda obriga os agentes a adotarem medidas técnicas e administrativas de segurança e de sigilo dos dados, com o fito de impedir acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou outras formas de tratamento inadequado de dados. O detalhamento dessas medidas e os padrões técnicos a serem observados é de responsabilidade da autoridade nacional.

A criação de regras para definir corretamente as agências – e eventuais entes privados – que exerçam os papéis de controlador e operador de dados é medida inexorável à concretização da garantia fundamental à proteção de dados pessoais. A ausência de disciplinar legal sobre o órgão legitimado a definir a finalidade do tratamento de dados pessoais produto de uma extração forçada em smartphone, implica, do ponto de vista prático nas investigações criminais em curso, em verdadeira carta branca.

3.1.2.2. O encarregado de dados e a figura do *Data Privacy Officer*

O encarregado é a pessoa natural ou jurídica indicada pelo controlador para atuar como “canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados” (art. 5º, VIII). As atribuições do encarregado consistem em (i) “aceitar reclamações dos titulares, prestar esclarecimentos e adotar providências” (art. 41, §2º, I); (ii) “receber comunicações da autoridade nacional e adotar providências” (art. 41, § 2º, II); e (iii) “orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais” (art. 41, § 2º, III). Portanto, de acordo com a disciplina da LGPD, o encarregado não ostenta atribuições, características e responsabilidades equivalentes à figura do Data Privacy Officer previstas no GDPR europeu. Consoante o art. 27 do GDPR, a principal função do “representante seria a comunicação entre controlador e o operador e entre os titulares dos dados pessoais e as autoridades de proteção de dados”, exatamente como art. 41 da LGPD disciplina a figura do encarregado.

O “Data Privacy Officer” no GDPR é disciplinado nos artigos 37 a 39 do regulamento europeu sobre proteção de dados pessoais, que estabelece três hipóteses em que o DPO é obrigatório, quais sejam: (i) tratamento efetuado por uma autoridade ou um organismo público, exceto os tribunais no exercício da sua função jurisdicional; (ii) atividades principais do responsável pelo tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controle regular e sistemático dos titulares dos dados em grande escala ou (iii) atividades principais do responsável pelo tratamento consistam em operações de tratamento em grande escala.

Além disso, o GDPR estabelece diretrizes sobre quem seria o DPO, ou seja, a autoridade ou um organismo público pode designar um único DPO para várias dessas autoridades ou organismos, tendo em conta a respectiva estrutura organizacional e dimensão, sendo que o DPO é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados. O DPO pode ser um elemento do pessoal da entidade responsável pelo tratamento, por exemplo, um funcionário do controlador, ou exercer as suas funções com base em um contrato de prestação de serviços, isto é, o controlador contrata uma empresa especializada em proteção de dados para dar esse suporte[103].

Além disso, as atribuições do DPO vão além de atividades de comunicação entre os titulares, a ANPD e o controlador, como dispõe a LGPD brasileira, contemplando: (i) agir em nome das associações e de outros organismos que representem os responsáveis pelo tratamento ou os subcontratantes; (ii) informar e aconselhar o responsável sobre as melhores práticas em proteção de dados pessoais; (iii) controlar a conformidade do tratamento com o GDPR e legislação selecionada; (iv) prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização; (v) cooperar com a OPA; e (vi) ser um contato para que os titulares possam resolver as questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos.

Seguindo as balizas do GDPR, entendemos que a previsão legal de um DPO a ser nomeado pelo órgão de persecução controlador dos dados pessoais tratados a partir

---

[103] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). Disponível em: <https://gdprinfo.eu/pt-pt>. Acesso em: 24 set. 2024.

de uma extração de dispositivo celular, é medida que traria segurança na interação entre a agência penal e os titulares dos dados pessoais objeto de tratamento, bem como centralizaria as demandas da autoridade nacional para fins de prevenção e atuação em caso de incidentes de segurança, produção de relatório de impactos etc.

3.1.3. Direitos do titular de dados pessoais afetado

Em primeiro lugar, observamos que uma série de direitos positivados no artigo 18 da LGPD, em realidade, já eram reconhecidos pelo ordenamento jurídico brasileiro. O pouco utilizado instrumento do *habeas data* já servia para confirmar a existência de tratamento, acesso e retificação de dados constitucionais, contando com lei regulamentadora própria (Lei nº 9.507/1997), além de previsão constitucional (art. 5º, LXIX). exemplo da confirmação de existência de tratamento. Igualmente, a Lei de Acesso à Informações criou mecanismos de igual efeito prático[104]. O MCI, por sua vez, como visto em 1.3.2, instituiu regras sobre o consentimento para o tratamento de dados. Também o direito de oposição a tratamento de dados em desconformidade com a lei já poderia ser exercido devido ao direito constitucional de petição aos poderes públicos, em defesa de direitos ou contra ilegalidade ou abuso de poder. Não por acaso, a LGPD remete explicitamente a essas normas, esclarecendo que os prazos e procedimentos para exercício dos direitos do titular perante o poder público observarão o disposto em legislação especifica”[105].

---

[104] O art. 7º assegura os direitos de obter: I - orientação sobre os procedimentos para a consecução de acesso, bem como sobre o local onde poderá ser encontrada ou obtida a informação almejada; II - informação contida em registros ou documentos, produzidos ou acumulados por seus órgãos ou entidades, recolhidos ou não a arquivos públicos; III - informação produzida ou custodiada por pessoa física ou entidade privada decorrente de qualquer vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha cessado; IV - informação primária, íntegra, autêntica e atualizada; V - informação sobre atividades exercidas pelos órgãos e entidades, inclusive as relativas à sua política, organização e serviços; VI - informação pertinente à administração do patrimônio público, utilização de recursos públicos, licitação, contratos administrativos; e VII - informação relativa: a) à implementação, acompanhamento e resultados dos programas, projetos e ações dos órgãos e entidades públicas, bem como metas e indicadores propostos; b) ao resultado de inspeções, auditorias, prestações e tomadas de contas realizadas pelos órgãos de controle interno e externo, incluindo prestações de contas relativas a exercícios anteriores.

[105] WIMMER, Miriam. Cidadania, Tecnologia e Governo Digital: Proteção de Dados Pessoais no Estado Movido a Dados. In: Alexandre F. Barbosa. (Org.). TIC Governo Eletrônico 2019. Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. 1ed.São Paulo: Comitê Gestor da Internet no Brasil, 2020, v. 1, p. 27-36

3.1.4. Regras de anonimização e pseudoanonimização de dados pessoais

Imaginemos a seguinte situação: após a coleta de dados pessoais, tais como o próprio número telefônico, as fotografias da face do titular encontradas no álbum e as coordenadas geográficas mantidas em histórico de localização de smartphones apreendidos em uma investigação de roubos ocorridos em determinada região urbana, a agência penal responsável pela apuração do delito, resolve, com base em uma lei hipotética, manter os registros de tais informações em um banco de dados – excluindo-se o nome do titular -, com o objetivo de consulta para futuras investigações criminais de delitos patrimoniais no local dos fatos. A referido banco de dados têm acesso todos os policiais do órgão, não apenas daquela agência específica que apurou o roubo. Acrescentemos a seguinte variável: ao consultar a base de dados, e a partir do número de celular do aparelho apreendido, outra agência requisita a identificação do titular em redes sociais, obtendo além de seu nome, as informações de postagens e rede de contatos, cruzando tais informações a fim de traçar um perfil de suspeito para determinado fato em apuração.

É legítimo que as informações que compõe o banco de dados hipotético acima se encontrem absolutamente abertas, sem qualquer camada de mascaramento, ou a aplicação de técnicas de anonimização é necessária para mitigar operações de tratamento desvinculadas da que legitimou a coleta originalmente, em havendo base legal para as operações sucessivas?

3.1.5. Regras de compartilhamento e eliminação dos dados

A obtenção de dados pessoais de celulares apreendidos no contexto de uma investigação criminal é capaz de produzir quantidades significativas de informações, que, não raro, serão de interesse para outros procedimentos investigativos, inclusive não penais, bem como para a execução de atividades alheias à persecução penal, como a segurança pública.

Atualmente, não se tem clareza sobre quais operações de tratamento de dados pessoais são realizadas sucessivamente à coleta, ao processamento e à utilização das

informações em um procedimento determinado. Em outras palavras, a difusão, a comunicação e a transferência[106], por exemplo, de dados pessoais de uma agência penal, que os controle, a outra, não é objeto de regulação, na ausência de uma LGPD Penal.

Igualmente, não há regras sobre a eliminação de dados pessoais, enquanto procedimento para a exclusão de dado ou de conjunto de dados armazenados em banco de dados, o que desafia a lógica do ciclo de vida do tratamento de dados pessoais, segundo a qual toda operação envolvendo dados pessoais, em algum momento, exaurida a finalidade da operação e não existindo mais base legal para a continuidade do tratamento, impõe ao controlador o dever de eliminação.

Há duas ideias subjacentes à eliminação de dados ao final do ciclo de tratamento que devem ser contempladas pelas regras sobre o tema: (i) no que tange aos agentes de tratamento, a imposição de obrigações de gestão e de mecanismos técnicos capazes de proceder com a eliminação gerando o menor risco possível para a continuidade do tratamento de dados pessoais obsoletos ou em desconformidade; e (ii) o balanceamento entre a legítima expectativa dos titulares de dados pessoais de que seus direitos possam ser plenamente exercidos com a realização de atividades de interesse público[107], como a persecução de delitos[108].

---

[106] Operações de tratamento objeto do art. 5º, X, da LGPD, que se encaixam em atividades de compartilhamento, latu sensu, dos dados pessoais controlados por uma determinada agência penal.

[107] De acordo com Sérgio Garcia Alves, a eliminação de dados ao final do ciclo de tratamento rompeu com a lógica existente de "colete agora, pergunte depois", que, em um ambiente desprovido de regulamentação, tolera práticas de coleta de informações de maneira errática ou experimental, com ausência de controle ou planejamento. Esse fenômeno, segundo, foi uma consequência natural, mas não mais compatível, com o processo expansivo de tratamento de dados proporcionado pelas novas tecnologias: "A digitalização da economia, a alta capacidade computacional e a redução de custos de processamento tornaram possível a coleta massiva de dados das mais diversas fontes com objetivos de inteligência, vigilância, controle, eficiência, prestação de serviços, antecipação de tendências e ganho econômico. Os incentivos para essa coleta massiva em ambientes pouco regulados foram bem documentados, e regramentos como a LGPD buscam alterar esse balanço impondo obrigações para empresas e governos". ALVES, Sérgio Garcia. Fechando um ciclo: do término do tratamento de dados pessoais (arts. 15 e 16 da LGPD). In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ivo Wolfgang e RODRIGUES JR., Otávio Luiz (coord.). Tratado de proteção de dados pessoais – 2ª ed. – Rio de Janeiro: Forense, 2023, p. 230.

[108] Pode-se imaginar, também, a perda do referencial da necessidade como critério substancialmente fundado de eliminação de dados ainda no decorrer de uma investigação criminal não concluída. Seria o caso de uma medida cautelar real de indisponibilidade de bens do investigado subjacente ao inquérito policial, em que levantados os bens imóveis atrelados ao CPF do imputado e realizadas as averbações pertinentes nas respectivas matrículas, os documentos referentes a tais bens do patrimônio deveriam ser

A título de ilustração, o art. 7º do PL 1515/22, que trata da LGPD Penal, confere base legal para o tratamento de dados pessoais para fins de persecução penal mediante previsão legal específica, a qual se consubstancia, de acordo com o parágrafo único, nas competências legais dos órgãos incumbidos de tais atividades. Logo, uma determinada delegacia de polícia federal teria competência legal para tratar dados pessoais no contexto de uma investigação de crimes federais. Como regra, a conclusão do inquérito policial encerraria a atribuição da autoridade policial presidente na consecução das atividade de polícia judiciária de elucidação de crime, esvaecendo, também, a finalidade que justificou o tratamento de determinado dado pessoal para os propósitos da investigação – a rigor, comprovar materialmente a ocorrência do crime e apontar o provável autor do fato -, devendo ser eliminado.

No entanto, o PL também prevê três exceções à regra da eliminação ao final do tratamento de dados pessoais, quais sejam, o cumprimento de obrigação legal ou regulatória pelo controlador, estudo por órgão de pesquisa, garantida sempre a anonimização dos dados pessoais ou, ainda, para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (art. 22). Portanto, na redação atual, fica autorizada a transferência de dados pessoais entre entidades de persecução penal, segurança pública e de inteligência, mediante a observância das regras previstas no art. 11.

Ainda que o modelo acima, ainda não vigente, possa ser alvo de críticas por conferir ampla margem para a manutenção de bancos de dados e compartilhamento sob pretextos genéricos entre órgãos com atribuições distintas, é inequívoco que a edição de regras dessa natureza tem por objetivo impedir que, no cotidiano dos órgãos controladores, o compartilhamento seja ilimitado e a eliminação de dados pessoais uma mera faculdade do controlador.

No atual quadro de déficit de legalidade sobre a matéria, entendemos, com base nas considerações acima, não ser legítimo que uma determinada agência penal responsável por elucidar inúmeros roubos em determinada região do município, após coletar dados pessoais (sigilosos ou não) de diversos suspeitos que tiveram seus

---

suprimidos (eliminados), pois não subsiste necessidade de mantê-los nos autos indefinidamente, em investigações, que não raro, demoram anos a serem concluídas.

smartphones apreendidos, possa mantê-los sob custódia indeterminadamente. Menos que a secretaria de segurança pública da unidade federativa a que pertence tal município, possa solicitar o compartilhamento desses dados, a fim de compreender a dinâmica dos crimes, horários de maior incidência, perfil (inclusive socioeconômico e racial) das vítimas e dos suspeitos, para fins de implementação de políticas públicas voltadas à redução desse tipo de delito na localidade.

Aliás, a criação de regras de compartilhamento e eliminação de dados visa justamente definir se e quando um intercâmbio de informações como o pretendido na hipótese acima poderia ocorrer. A lei deve prever com clareza que tipos de dados pessoais oriundos de operação de coleta forçada de smartphone apreendido para fins de investigação criminal poderiam ser mantidos pela agência penal e por quanto tempo, e se o compartilhamento com órgãos de segurança pública para fins de prevenção de crimes patrimoniais com violência, que nos parece proporcional, também seria possível fossem infrações de menor gravidade que o Estado desejasse prevenir, como dano ao patrimônio público.

3.1.6. Cadeia de custódia da prova digital decorrente de dados extraídos de aparelhos de celular

A cadeia de custódia é um mecanismo que assegura a autenticidade dos elementos que se transformarão em prova no curso da instrução processual, por meio do qual se permite identificar e registrar todo o seu percurso desde as investigações, o que garante segurança, rastreabilidade e confiança. A importância desse protocolo probatório decorre da possibilidade de manipulações indevidas ou manuseios que, acidentalmente ou não, contaminem os elementos de prova, minando a confiabilidade necessária para que possam ser valorados pelo Poder Judiciário. Afinal, a existência de dúvidas razoáveis sobre a idoneidade da prova impossibilita a identificação de possível vínculo entre provas aparentemente lícitas e outra, ilícita, bem como inviabiliza o exercício do contraditório e o controle sobre as alegações lastreadas por tais elementos.

A cadeia de custódia deve ser compreendida como “documentação da cadeia de custódia”, isto é, o registro do conjunto de pessoas e o momento específico em que cada

uma delas teve contato com a evidência. Como dito, a finalidade do instituto é garantir a autenticidade e a integridade da fonte de prova. De acordo com Gustavo Badaró

> a autenticidade significa que a fonte de prova é genuína e autêntica quanto à sua origem" - é dizer que a fonte examinada em juízo é aquela que foi colhida no início da investigação. Já a integridade "é a condição da fonte de prova que se apresenta íntegra ou inteira, não tendo sido adulterada, sofrendo diminuição ou alteração de suas características, que se mantêm as mesmas desde a sua colheita[109].

A Lei nº 13.964/19 introduziu no CPP os artigos 158-A a 158-F, por meio dos quais se instituiu um microssistema de regulação da cadeia de custódia no processo penal. A despeito da importância do tema e da recente alteração legislativa, a simples leitura dos dispositivos legais indica que o legislador voltou os olhos à colheita e à integridade da prova física, que deixa vestígios no mundo independentemente de qualquer dispositivo informático.

Ainda que se considere que o regime normativo instituído pelo CPP para a cadeia de custódia seria voltado, em um primeiro exame, aos vestígios físicos, as discussões em torno desse mecanismo de integridade da prova e a necessidade de cumprir protocolos legais com esse intuito não é nova. Antes da edição da Lei nº 13.965/19, o CPP já previa, no art. 6º, I e II, por exemplo, o dever dirigido à autoridade policial para preservação do local do crime até a chegada dos peritos, bem como a apreensão dos objetos após o exame.

Além disso, o art. 158, cuja redação se manteve intacta desde a edição do CPP em 1941, torna mandatória a realização de exame de corpo de delito para qualquer infração penal que deixe vestígios, sendo a cadeia de custódia condição de procedibilidade do referido exame, pois não seria possível valorar a conduta de A pela morte de B, se o laudo necroscópico descreve a causa da morte do cadáver de C, examinado no lugar daquele.

O dispositivo revela, também, a opção do legislador pela prova pericial como regra em nosso sistema probatório, o que não implica dizer que a cadeia de custódia

---

[109] BADARÓ, Gustavo. Processo penal [livro eletrônico] -- 9. ed. -- São Paulo : Thomson Reuters Brasil, 2023.6 Mb ; ePub 9. ed. em e-book baseada na 11. ed. Impressa.

deverá ser seguida apenas nas hipóteses de realização de perícia técnica. Em outras palavras, por mais que a cadeia de custódia esteja normalmente ligada à prova científica, sua aplicação deverá ser seguida em relação a qualquer fonte de prova, tanto real, como armas e documentos identificados na cena do crime, quanto imaterial, como elementos registrados eletronicamente, sejam e-mails, vídeos, arquivos de áudio, coordenadas geográficas de um usuário fornecidas por determinado provedor de aplicação de internet etc.

A legislação processual penal não regulamentou expressamente a cadeia de custódia de elementos imateriais, como o são os dados eletrônicos - enquanto combinações alfanuméricas dependentes de interpretação e leitura por sistemas de computação - que resultarão na prova digital. A informação digital está disponível em diversas fontes, em suportes físicos ou, igualmente, digitais: (i) dispositivos eletrônicos aparelhos celulares (*smartphones*), computadores, HDs externos, pen-drives e mídias de armazenamento; (ii) redes sociais e páginas da rede mundial de computadores; (iii) armazenados em provedores de aplicação de internet, como provedores de e-mail, aplicativos de instituições financeiras, de gestão de arquivos em nuvem.

A inexistência ou a insuficiência de documentação da cadeia de custódia permitirá que se questione a autenticidade e a integridade da fonte de prova, e consequentemente, dos elementos de prova dela extraídos. Havendo dúvidas sobre (i) as pessoas que tiveram contato com a fonte em relação aos atos de coleta, acondicionamento, transporte, recebimento, processamento, armazenamento e descarte, bem como (ii) quanto aos métodos e técnicas empregados em cada etapa desse processo, deve-se desconfiar da origem e de possíveis adulterações da prova, a depender do grau de informação existente.

No entanto, o legislador processual penal não previu expressamente as consequências da não documentação da cadeia de custódia, seja no que diz respeito à admissibilidade da prova no procedimento criminal, seja quanto à valoração do meio de prova.

De acordo com Badaró, a doutrina identifica, a princípio, duas possibilidades diante da violação da cadeia de custódia: a primeira, considerar a prova ilícita, nos termos do art. 5º, LVI, da CF, e do art. 157 do CPP, e, como tal, inadmissível no processo,

devendo ser desentranhada, se o caso. O direito à prova não implica num direito à admissão de todas as provas, sendo legítimo que a lei estabeleça hipóteses de exclusão probatória. Em outras palavras, pode o legislador definir sob quais pressupostos um determinado elemento de prova pode ser considerado apto e utilizado como fundamento para a reconstrução dos fatos[110].

Assim, para essa corrente, a manutenção da cadeia de custódia da prova seria condição de validade da própria fonte de prova que se pretende introduzir ao processo; ao revés, a ausência de documentação adequada ou comprovação de integridade dos elementos, sobretudo aqueles obtidos por métodos ocultos, como a interceptação telefônica e telemática, tornaria a prova ilícita e contaminaria aquelas derivadas.

A segunda possibilidade desloca o problema para o campo da valoração da prova e propõe que seja dado menor valor ao meio de prova produzido a partir de fontes cuja cadeia de custódia tenha sido violada. Para os autores que defendem esse efeito, é central a ideia de “mesmidade”, segundo a qual a finalidade da cadeia de custódia é assegurar a autenticidade e a integridade da fonte de prova, e não demonstrar que determinada alegação sobre determinado fato com base em determinada prova é verdadeira. Assim, a valoração judicial de uma determinada fonte de prova que apresente irregularidades na documentação da cadeia de custódia dependerá de um esforço de justificação, cujos contornos ainda devem ser melhor definidos.

O Superior Tribunal de Justiça, porém, oscila entre as duas posições acima. No HC 653.515/RJ, decidiu-se que as irregularidades constatadas na documentação da cadeia de custódia devem ser avaliadas no confronto com os demais elementos produzidos na instrução processual, aferindo-se, assim, o grau de confiabilidade. No caso, questionou-se a confiabilidade da droga apreendida, armazenada em saco de pão e posteriormente submetida à perícia, sem lacre[111].

---

[110] BADARÓ, Gustavo. Processo penal [livro eletrônico] -- 9. ed. -- São Paulo : Thomson Reuters Brasil, 2023.6 Mb ; ePub 9. ed. em e-book baseada na 11. ed. Impressa.

[111] Conforme declinado no acórdão, “A integralidade do lacre não é uma medida meramente protocolar; é, antes, a segurança de que o material não foi manipulado, adulterado ou substituído, tanto que somente o perito poderá realizar seu rompimento para análise, ou outra pessoa autorizada, quando houver motivos”. Ainda assim, a condenação foi mantida com base em outros elementos. BRASIL, Superior Tribunal de Justiça, AgRg no RHC n. 143.169/RJ, Quinta Turma, Relator Ministro Messod Azulay Neto, Relator para acórdão Ministro Ribeiro Dantas, julgado em 07/02/2023, publicado em 02/03/2023.

Já no RCH 143.169/RJ, o STJ anulou prova pericial por ausência de demonstração da cadeia de custódia por parte do perito judicial. De acordo com o acórdão, a polícia não documentou nenhum dos atos por ela praticados na arrecadação, armazenamento e análise dos computadores apreendidos durante o inquérito, nem se preocupou em apresentar garantias de que seu conteúdo permaneceu íntegro enquanto esteve sob a custódia policial. Como consequência, não há como assegurar que os dados informáticos periciados são íntegros e idênticos aos que existiam nos computadores do réu. Em última análise, decidiu o STJ que não há uma presunção de autenticidade na atividade probatória desenvolvida pelos agentes estatais.

Essas decisões sugerem que a aparente lacuna legislativa não necessariamente implica em impedimento para que a atividade persecutória continue se desenvolvendo, mormente no que toca à documentação da cadeia de custódia da prova digital. Recorre-se à categoria do "bônus de transição", já bem trabalhada pela jurisprudência alemã e segundo a qual enquanto não há lei, a jurisprudência deve desenvolver alguns parâmetros provisórios, de modo a não interromper importantes tarefas persecutórias[112].

3.2. Síntese parcial

A edição de lei que tipifique, processualmente, a extração de dados pessoais de dispositivos apreendidos no âmbito de investigações criminais e ações penais, para fins de produção de prova, e regulamente os requisitos, garantias e procedimentos, deve conter, no mínimo:

1. Critério positivado de proporcionalidade em sentido estrito das hipóteses de infrações penais que admitem a extração de dados de smartphones, seja por meio de rol taxativo ou patamar mínimo de pena cominada em abstrato;
2. Atribuição de responsabilidades e órgãos ou pessoas naturais legitimadas a ocupar as posições de controlador e operador de dados, e de Data Privacy Officer.
3. Regras de privacidade desde a concepção a serem observadas pelos desenvolvedores das ferramentas tecnológicas utilizadas para as operações de

[112] Greco, *op. cit.*, p. 167.

tratamento de dados pessoais para fins de investigação criminal, sejam entes estatais ou privados, incluindo mecanismos de segurança que minimizem os riscos de incidentes e vazamentos de dados, bem como o compartilhamento indevido e a correta eliminação, ao final do processo de tratamento, esgotada a finalidade.

Conclusão

REFERÊNCIAS

ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. Revista de Investigações Constitucionais, Curitiba, vol. 11, n. 1, e256, jan./abr. 2024. DOI: 10.5380/rinc.v11i1.89280

ABREU, Jaqueline de Souza. Proteção da privacidade e cooperação jurídica internacional. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 156-169.

ABREU, Jaqueline. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel Ferreira; RODRIGUES JUNIOR, Otavio Luiz; BIONI, Bruno (org.). Tratado de proteção de dados pessoais. Rio de Janeiro, RJ: Editora Forense, 2021. p. 583–603.

ABREU, Jacqueline de Souza, ANTONIALLI, Dennys. *Vigilância Sobre as Comunicações no Brasil*. INTERNETLAB, São Paulo, 2017.

ALVES, Sérgio Garcia. Fechando um ciclo: do término do tratamento de dados pessoais (arts. 15 e 16 da LGPD). In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ivo Wolfgang e RODRIGUES JR., Otávio Luiz (coord.). Tratado de proteção de dados pessoais – 2ª ed. – Rio de Janeiro: Forense, 2023.

ARAS, V. . O congelamento de dados informáticos para fins de prova no processo penal. Delictae - Revista de Estudos Interdisciplinares sobre o Direito , v. 8, p. 180-222, 2024.

AZEVEDO, Y. (2017). A importância da cadeia de custódia das provas para o devido processo legal. In Prado, G.; & Malan, D. (orgs.). Ensaios sobre a cadeia de custódia das provas no processo penal brasileiro, p. 106. Empório do Direito.

BADARÓ, Gustavo. Processo penal [livro eletrônico] -- 9. ed. -- São Paulo : Thomson Reuters Brasil, 2023.6 Mb ; ePub 9. ed. em e-book baseada na 11. ed. Impressa.

BADARÓ, Gustavo. O debate constitucional sobre privacidade, intimidade e proteção de dados no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 51-69.

BARROSO, Luís Roberto. Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo - 8. ed. - São Paulo: Saraiva, 2019.

BRASIL. Constituição da República Federativa do Brasil. Promulgada em 5 de outubro de 1988. Disponível em:

<https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 01 ago. 2024.

BRASIL. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 24 set. 2024.

BRASIL. Decreto 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, concluída em Budapeste, em 23 de novembro de 2001 e objeto de adesão pelo Brasil em 30 de novembro de 2022. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2023- 2026/2023/decreto/D11491.htm. Acesso em: 01 ago. 2024.

BRASIL. Decreto-lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 01 ago. 2024.

BRASIL. Decreto nº 8771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 24 set. 2024.

BRASIL. Lei no 9.296 de 24 de julho de 1996. Lei de Interceptações Telefônicas e Telemáticas. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 04 dez. 2023.

BRASIL. Lei 12.527, de 18 de novembro de 2011. Lei de Acesso à Informação. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 22 ago. 2024.

BRASIL. Lei 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2013/lei/l12850.htm>. Acesso em: 13 ago. 2023.

BRASIL. Lei 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011- 2014/2014/lei/l12965.htm>. Acesso em: 13 out. 2023.

BRASIL. Lei no 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados brasileira (LGPD). Disponível em: <http:// www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 04 dez. 2023.

BRASIL. Superior Tribunal de Justiça. HC n. 674.185/MG. Sexta Turma. Relator Ministro Sebastião Reis Júnior, julgado em 17/08/2021, publicado em 20/08/2021.

BRASIL, Superior Tribunal de Justiça, AgRg no RHC n. 143.169/RJ, Quinta Turma, Relator Ministro Messod Azulay Neto, Relator para acórdão Ministro Ribeiro Dantas, julgado em 07/02/2023, publicado em 02/03/2023.

BRASIL, Supremo Tribunal Federal. MS 21729, Tribunal Pleno, Relator Ministro Marco Aurélio, julgado em 05/10/1995, publicado em 19/10/2001.

BRASIL. Supremo Tribunal Federal. RE 418416, Tribunal Pleno, Relator Ministro Sepulveda Pertence, julgado em 10/05/2006, publicado em 19/12/2006.

BRASIL. Supremo Tribunal Federal. HC 91867. Segunda Turma. Relator Gilmar Mendes. Julgado em 24/04/2012. Publicado em 20/09/2012.

BRASIL. Supremo Tribunal Federal. ADI 5642. Tribunal Pleno. Relator Edson Fachin. Julgado em 18/04/2024. Publicado em 22/08/2024.

CORRÊA DA LUZ, Yuri. Bancos de dados públicos e o compartilhamento com agencias penais. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 170-181.

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).

DIETER, Maurício. Big data e devido processo: poder penal preditivo. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 83-95.

ESTELLITA, Heloisa. O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF. Direito Público, *[S. l.]*, v. 18, n. 100, 2022. DOI: 10.11117/rdp.v18i100.5991. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5991. Acesso em: 12 set. 2023.

ESTELLITA, Heloisa. O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (Ed.). Direitos fundamentais e processo penal na era digital: doutrina e prática em dabate [livro eletrônico]. São Paulo: InternetLab, 2022, p. 98-141.

FELIPE DE CASTRO, Matheus. Um celular na cena do crime: o STF e a proteção de dados estáticos. Consultor Jurídico. São Paulo, 20 set. 2024. Disponível em: < https://www.conjur.com.br/2024-set-20/um-celular-na-cena-do-crime-o-stf-e-a-protecao-dos-dados-estaticos/>. Acesso em: 24 set. 2024.

FERRAZ JUNIOR, Tércio Sampaio. O alcance da proteção do sigilo das comunicações no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 97-105.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. O direito de proteção de dados no processo penale na segurança pública - 1ª ed. - Rio de Janeiro: Marcial Pons, 2021.

GLEIZER, Orlandino. A dogmática dos métodos ocultos de investigação no processo penal. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 119-129.

GOMES, Luiz Flávio e MARQUES, Ivan Luís. Prisão e Medidas Cautelares – Comentários à Lei 12.403, de 4 de maio de 2011: São Paulo: Editora Revista dos Tribunais, 2011, p. 150.

LUZ, Yuri. Bancos de dados públicos e o compartilhamento com agências penais. In: CRUZ, Francisco Brito; SIMÃO, Bárbara (Ed.). Direitos fundamentais e processo penal na era digital [livro eletrônico]. São Paulo: InternetLab, 2021, p. 170-181.

GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. Revista Brasileira de Ciências Criminais. Vol 156/2019, p. 353-393.

MACHADO, Eloísa. O debate constitucional sobre privacidade, intimidade e proteção de dados no Brasil. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 38-49.

MAGALHÃES, Antonio Gomes et al. (FERNANDES, Og, coord.), Medidas cautelares no processo penal: prisões e suas alternativas: comentários à Lei 12.403, de 04.05.2011, São Paulo, Revista dos Tribunais, 2011, p.18.

MAGALHÃES, Assusete. Quebra de sigilo de dados e das comunicações telefônicas: o dever estatal de preservação da fonte da prova. 2015. Disponível em: https://bit.ly/2PSIUoh. Acesso em: 23 jul. 2023.

MALAN, Diogo. Métodos ocultos, devido processo e o enfrentamento à criminalidade organizada. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 107-117.

MENDES, Carlos Hélder Carvalho Furtado. Tecnoinvestigação criminal: entre a proteção de dados e a infiltração por software. Salvador: Editora Jus Podivm, 2020.

MUDROVITSCH, Rodrigo. Compartilhamento de dados entre o privado e o público no âmbito da segurança pública. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (Ed.). Direitos fundamentais e processo penal na era digital: doutrina e prática em dabate [livro eletrônico]. São Paulo: InternetLab, 2022, p. 162-176.

OSÓRIO, Anamara. Direitos fundamentais e a extensão de ordens judiciais de acesso a dados de pessoas indefinidas. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (Ed.). Direitos fundamentais e processo penal na era digital: doutrina e prática em dabate [livro eletrônico]. São Paulo: InternetLab, 2022, p. 180-191.

PEGORARO DE ARAUJO, C. V. (2022). Os Aspectos Gerais Dos Tratados Internacionais e a Convenção de Budapeste Sobre Crimes Cibernéticos. *Revista Da Faculdade De Direito Da Universidade Federal De Uberlândia*, *50*(1), 145–165. https://doi.org/10.14393/RFADIR-50.1.2022.65259.145-165

PÉREZ Estrada, M. J. (2019). La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. *Revista Brasileira De Direito Processual Penal*, *5*(3), 1297-1330. https://doi.org/10.22197/rbdpp.v5i3.253

PRADO, Geraldo. Breves notas sobre o fundamento constitucional da cadeia de custódia da prova digital. Disponível (on-line) em: https://geraldoprado.com.br/artigos/breves-notas-sobre-o-fundamento-constitucional-da-cadeia-de-custodia-da-prova-digital/. Acesso em: 24 set. 2023. Texto correspondente à palestra proferida intitulada “A interface entre o Direito Digital e o Processo Penal”, no Ciclo Permanente de Palestras com o tema “Consequências do Uso da Inteligência Artificial no Processo Penal”, oferecido pelo Núcleo de Estudo Luso-Brasileiro da Faculdade de Direito da Universidade de Lisboa (NELB), em 20 de janeiro de 2021, às 13 horas (horário de Brasília), transmitida pelo aplicativo *Zoom*.

PRADO, Luiz Régis. Curso de direito penal brasileiro, vol. I – Parte Geral, 15ª ed., São Paulo, Revista dos Tribunais, 2017, p.351.

QUEIROZ, Rafael Mafei Rabelo. PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fscalizadora do Estado: o

que permanece e o que deve ser reconsiderado. *In: Internet e sociedade*. N. 1. V. 1. Fevereiro de 2020, pp. 64-90.

QUITO, Carina. Acesso a comunicações eletrônica armazenadas na prática judiciária. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (Ed.). Direitos fundamentais e processo penal na era digital: doutrina e prática em dabate [livro eletrônico]. São Paulo: InternetLab, 2022, p. 100-107.

REBELLATO, Luiz Fernando Bugiga. Caso COAF: critérios de classificação e transparência. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (Ed.). Direitos fundamentais e processo penal na era digital: doutrina e prática em dabate [livro eletrônico]. São Paulo: InternetLab, 2022, p. 142-161.

RICARDO, Carolina. Sistemas de vigilância em massa e proteção de dados: cenário na segurança pública. In: BRITO CRUZ, Francisco; SIMÃO, Bárbara (eds.). Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. IV. São Paulo. InternetLab, 2021, p. 71-81.

RUIZ, Evandro Eduardo Seron. In: PEREIRA DE LIMA, Cíntia Rosa (coord.). Anonimização, Pseudoanonimização e desanonimização de dados pessoais. Comentário à lei geral de proteção de dados – São Paulo: Almedina, 2020, p. 101-122.

SANTORO, A. E. R.; Tavares, N. L. F.; & Gomes, J. C. (mai./ago. 2017). O protagonismo dos sistemas de tecnologia da informação na interceptação telefônica: a importância da cadeia de custódia. Revista Brasileira de Direito Processual Penal, 3(2), pp. 605-632. https://bit.ly/2TSnOIV.

SIDI, Ricardo. *A Interceptação das Comunicações Telemáticas no Processo Penal.* Belo Horizonte, 2016, Editora D'Plácido.

SOUSA MENDES, PAULO DE, 2020: «A privacidade digital posta à prova no processo penal», in Quaestio facti, 2: 225-250. Madrid: Marcial Pons Ediciones Jurídicas y Sociales. DOI: http://dx.doi.org/10.33115/udg_bib/qf.i2.22487

SOUZA, Lia Andrade de; VASCONCELOS, Vinicius Gomes de. A cadeia de custódia da prova obtida por meio de interceptações telefônicas e telemáticas: meios de proteção e consequências da violação. Revista da Faculdade de Direito UFPR, Curitiba, v. 65, n. 2, p. 31-48, ago. 2020. Disponível (on-line) em: <https://revistas.ufpr.br/direito/article/view/68577>. Acesso em: 08 set. 2023.

TOLEDO DE BARROS, Susana, O princípio da proporcionalidade e o controle de constitucionalidade das leis restritivas de direitos fundamentais. 2. ed. Brasília, Brasília Jurídica, 2000, p. 91.

WEIBLEN, Fabrício Pinto. O uso de software espião na investigação criminal: interpretação aberta à tecnologia, (in)admissibilidade e tratamento jurídico adequado. Londrina, PR: Thoth, 2024

WIMMER, Miriam. Cidadania, Tecnologia e Governo Digital: Proteção de Dados Pessoais no Estado Movido a Dados. In: Alexandre F. Barbosa. (Org.). TIC Governo Eletrônico 2019. Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. 1ed.São Paulo: Comitê Gestor da Internet no Brasil, 2020, v. 1, p. 27-36.

WOLTER, Jürgen. O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal: organização e tradução Luís Greco; tradução Alaor Leite, Eduardo Viana - 1ª ed. - São Paulo: Marcial Pons, 2018.

ZILLI, Marcos. A prisão em flagrante e o acesso a dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade. Em: Direitos fundamentais e processo penal na era digital / Dennys Antonialli, Jacqueline de Souza Abreu [editores]. -- São Paulo : InternetLab, 2018. -- (Doutrina e prática em debate ; v. 1).