Revista Judicial Brasileira

Ano 2 N.1 - Janeiro/Julho 2022

ENFAM

https://doi.org/10.54795/rejub.n.1.180

UTILIZAÇÃO DE DADOS PESSOAIS NO COMBATE AO CRIME ORGANIZADO: LIMITES E POSSIBILIDADES DE TÉCNICAS ESPECIAIS DE INVESTIGAÇÃO EM MEIO DIGITAL

PERSONAL DATA AGAINST ORGANIZED CRIME: LIMITS AND POSSIBILITIES OF SPECIAL INVESTIGATION TECHNIQUES IN DIGITAL MEDIA

ABHNER YOUSSIF MOTA ARABI

Juiz auxiliar da Presidência do Supremo Tribunal Federal – STF. Coordenador do Centro de Mediação e Conciliação do STF. Juiz de direito do Tribunal de Justiça do Estado de São Paulo – TJSP. Doutorando em Direito do Estado (subárea: Direito Constitucional) pela Universidade de São Paulo – USP. Mestre em Direito, Estado e Constituição (linha: Constituição e Democracia) pela Universidade de Brasília – UnB. Autor de livros, capítulos de livro e artigos jurídicos. Professor e palestrante.
https://orcid.org/0000-0002-8137-7760

RESUMO

A dinamicidade do mundo moderno aporta desafios adicionais à atividade estatal de persecução penal. Fenômenos como a globalização, a virtualização da economia e o surgimento contínuo de novas tecnologias representam a necessidade de atualização das técnicas de investigação na busca de uma tutela penal eficiente. Ao mesmo tempo, os limites formais e materiais da ordem constitucional que guiam a atuação penal do Estado são também continuamente atualizados, contexto em que a autonomia do direito fundamental à proteção dos dados pessoais surge como um novo limite a ser observado. Nesse cenário, o artigo expõe limites possíveis a essas

novas técnicas investigativas, à luz do direito fundamental à proteção dos dados e à preservação da cadeia de custódia de meios de prova digital, a partir do contexto brasileiro e internacional. Ainda, são abordados os desafios que se somam quando a descoberta de informações penalmente relevantes se dá por investigações jornalísticas.

Palavras-chave: proteção de dados; provas digitais; cadeia de custódia.

ABSTRACT

The dynamics of the modern world brings additional challenges to the state's criminal prosecution. Phenomena such as globalization, the virtualization of the economy and the continuous emergence of new technologies represent the need to update investigation techniques in the pursuit of efficient protection. At the same time, the formal and substantial limits that guide the criminal prosecution are also continuously updated, a context in which the fundamental right to the protection of personal data appears as a new limit to be observed. In this scenario, the article exposes possible limits to these new investigative techniques, considering the fundamental right to data protection and the preservation of the chain of custody of digital evidence, in the Brazilian and international perspectives. Also, it points to challenges that are added when the discovery of criminally relevant information takes place through non-official journalistic investigations.

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

Recebido: 7-3-2022
Aprovado: 28-4-2022

SUMÁRIO

1 INTRODUÇÃO

A persecução criminal estatal é tarefa que revela desafios intrínsecos em uma ordem constitucional acusatória. A tutela dos bens jurídicos protegidos e dos direitos fundamentais das vítimas impõem a realização eficiente dessa atividade. Ao mesmo tempo, na busca pela justificação da imposição legítima de uma sanção, exige-se fiel observância aos direitos e às garantias dos investigados, seja durante as investigações pré-processuais, seja no curso do processo penal propriamente dito.

O contínuo e dinâmico equilíbrio entre esses dois polos não é novidade no estudo do processo penal. Diz-se, inclusive, que seu grau de balanceamento indica o grau democrático ou autoritário de uma sociedade (GOLDSCHMIDT, 1935, p. 67), funcionando o processo penal como um "sismógrafo da Constituição do Estado" (ROXIN, 2000, p. 10, tradução nossa). Entretanto, no âmbito da persecução da macrocriminalidade, da criminalidade organizada e no combate a crimes de corrupção, lavagem de dinheiro e tráfico de pessoas, esses desafios ganham contornos dinâmicos e são ainda mais críticos, sobretudo quando assumem natureza transnacional, tendo em vista a limitação e a insuficiência dos meios investigativos e probatórios mais tradicionais.

Com efeito, fenômenos como a globalização e a virtualização da economia, a facilidade e a celeridade na coleta, tratamento e tráfego de dados cada vez mais volumosos, a dinamicidade do surgimento de novas tecnologias e seus elevados impactos sociais são circunstâncias que apresentam reflexos diretos na persecução penal (BASSIOUNI, 2015), inclusive quanto ao surgimento de novos bens jurídicos a serem tutelados. Essas peculiaridades, por consequência, veiculam a necessidade de aperfeiçoamento dos órgãos estatais e multilaterais,[1] bem como de seus métodos e instrumentos de ação, frente a novas técnicas de tipificação de crimes[2] e sanção penal; estímulos à prática de conformidade legal (*compliance*); novos meios de investigação e persecução penal, como a cooperação internacional, a adoção de soluções negociadas (ARAS, 2021); além de aspectos como a proteção e o incentivo aos denunciantes de boa-fé (*whistleblowers*) (ARAS, 2013).

De outro lado, essas inovações apenas podem se desenvolver legitimamente quando observados os direitos fundamentais dos investigados, inclusive aqueles que também nesse contexto surgem ou se atualizam. É o caso, por exemplo, do direito à proteção de dados, a atrair complexos elementos na sua tutela legal em sede de

[1] Nesse sentido, Shaw e Kemp (2015, p. 345-348) propõem a reestruturação do sistema multilateral de resposta ao crime organizado, em cinco etapas principais: a criação de um escritório das Nações Unidas para a Justiça, incrementando a liderança e não apenas a coordenação entre os países; o redirecionamento de algumas abordagens atuais que mesclam questões de saúde e justiça como uma coisa só; uma nova implementação da Convenção das Nações Unidas contra o Crime Organizado Transnacional; o investimento em performance analítica no combate ao crime organizado e sua vinculação com os Objetivos de Desenvolvimento Sustentável – ODS; além do aprimoramento do sistema global pelo fortalecimento dos sistemas regionais.

[2] É o que ocorre com a ascensão de modelos de tipificação de crimes de perigo abstrato e delitos de acumulação, por exemplo, decorrentes de uma sociedade do risco descrita por Beck (2002) com reflexos penais e processuais penais de relevo (BOTTINI, 2011, p. 119). Nesse contexto, o "perigo deixa o campo do subjetivo e passa a ostentar uma realidade objetiva, preenchida probabilidade fática da ocorrência da lesão ou do dano que se quer evitar" (BOTTINI, 2019, p. 23). Ainda, Hassemer (1999, p. 22) descreve algumas novidades do que chama de "moderno Direito Penal".

investigação criminal e sua inserção na cadeia de custódia, que deve ser documentada e preservada. Além das fronteiras decorrentes de novos direitos fundamentais, os limites legais e epistêmicos da atividade probatória (BADARÓ, 2018, p. 520) também se modificam, para uma valoração racional de provas íntegras e autênticas (FERRER-BELTRÁN, 2007, p. 42-47), que devem guiar "a convicção do juiz sobre a realidade de uma alegação fática" (GOLDSCHMIDT, 2015, p. 464, tradução nossa), que ultrapasse o mero caráter hipotético da acusação.

Quanto a esse ponto, outros aspectos importantes se revelaram em situações recentes em que elementos informativos surgiram a partir de meios não estatais de investigação, como denúncias anônimas e bem documentadas feitas a veículos internacionais de comunicação ou descobertas decorrentes de iniciativas conjuntas e transnacionais de jornalismo investigativo. É o exemplo dos casos conhecidos como Panama Papers e Swiss Leaks, por exemplo, que evidenciaram a publicação de uma enorme quantidade de dados e documentos que indicavam a possível prática de atos fraudulentos e criminosos por diversas pessoas, dentre as quais líderes políticos e celebridades. No ponto, também se envolve diretamente a liberdade de imprensa, outra garantia constitucional e internacionalmente protegida, a atrair desdobramentos particulares.

Configura-se, assim, o objeto do presente artigo: a partir da exposição de novas técnicas investigativas surgidas nesse contexto e dos limites que lhe têm sido atribuídos pela interpretação judicial em alguns casos nacionais e estrangeiros, propõe-se a contraposição entre a necessidade de seu desenvolvimento e a tutela de direitos fundamentais. Mais especificamente, quer-se apresentar o direito à proteção de dados como uma nova limitação autônoma às atividades de persecução penal pelo Estado, problematizando-o face a situações em que a descoberta de informações penalmente relevantes se dá

por meios extraoficiais, como os acima mencionados, protegidos pela liberdade de imprensa. Com efeito, esses são desafios que se revelam presente não apenas na América Latina e na Europa, como também em outros países do mundo, havendo casos em que é possível vislumbrar a aplicação prática dessas premissas, evidenciando a relevância e a necessidade da discussão.

2 A AUTONOMIA DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS: UM NOVO LIMITE À PERSECUÇÃO PENAL ESTATAL

A proteção constitucional da intimidade e da vida privada é noção que desde há muito se afirma. Com efeito, como reflexo inerente da dignidade da pessoa humana, há aspectos da vida de cada um que devem restar preservados do conhecimento público, ao menos enquanto assim recomendar sua própria autodeterminação. Ao mesmo tempo, também há muito se admite que o conflito com outros valores constitucionais ou direitos fundamentais pode representar a excepcional relativização dessa proteção, quando exista motivado interesse no conhecimento dessas informações pessoais, nos limites materiais e formais do que autorizado por lei.

Nesse sentido, por exemplo, é que a Constituição brasileira de 1988, desde sua redação original, expressamente afirma o direito fundamental de inviolabilidade da intimidade e da vida privada, além de cartas, correspondências, comunicações telemáticas, telefônicas e do domicílio físico dos indivíduos (art. 5º, X, XI, XII, da CRFB/1988), observadas as limitações ali mesmo indicadas ou remetidas à lei (BRASIL, 1988). No plano internacional, destaca-se a previsão da Convenção Americana sobre Direitos Humanos de 1969 (promulgada no Brasil pelo Decreto n. 678/1992) no sentido de que o art. 11, § 2° pontua que "ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação"

(COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS, 1969). Igualmente, no sistema europeu, a Convenção Europeia dos Direitos Humanos de 1950 (EUROPEAN COURT OF HUMAN RIGHTS, [2021], p. 11) estabelecia que "qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência" (art. 8°, § 1°).

Ao longo do tempo, porém, a regulamentação tradicional do direito à intimidade e à privacidade revelou-se insuficiente. A necessidade de contínua atualização e revisitação, de tempos em tempos, do conteúdo protetivo do direito à privacidade conforme as alterações sociais, econômicas e políticas de uma sociedade era descrita no século XIX por Warren e Brandeis (1890, p. 193).

Com efeito, na era da informação, "as leis existentes para proteção da privacidade da informação não responderam adequadamente ao surgimento dos dossiês digitais" (SOLOVE, 2004, p. 8), nem à desregulamentada utilização de dados pessoais, impondo a necessidade de que a própria proteção à privacidade fosse repensada. Eventos como o escândalo do Facebook e da Cambridge Analytica (KAISER, 2020), revelaram o amplo emprego de informações pessoais como itens valiosos, sem que seus titulares estivessem cientes ou pudessem participar desse processo (SOLOVE, 2004, p. 223). Isso não apenas para apropriações comerciais propriamente ditas, mas inclusive para campanhas eleitorais e definição de eleições,[3] mediante a utilização de técnicas algorítmicas de microdirecionamento (*microtargeting*) e veiculação de informações falsas.[4]

[3] Empoli (2020, p. 84) também indica como a irrupção de novas mídias e suas ferramentas de personalização contribuem para a construção de um caos político e social. O autor analisa o contexto de diferentes países europeus, como a Itália, no âmbito da qual cita o exemplo do Movimento 5 Estrelas (MoVimento 5 Stelle).

[4] No cenário brasileiro, um retrato exemplificativo da utilização dessas ferramentas, seus reflexos diretos no processo eleitoral e suas ameaças potenciais para a democracia pode ser encontrado em Mello (2020).

Nesse debate, por vezes, a tutela adequada de informações pessoais é colocada em confronto com a proteção da segurança da comunidade, especialmente em tempos de crise de segurança pública, quando são frequentes os argumentos de que direitos e liberdades pessoais devem ser sacrificados em prol de um interesse público nacional. Entretanto, considerando que esses valores não são necessariamente excludentes, essa dicotomia não é inexorável e pode se revelar falsa. Aliás, esse argumento pendular descrito por Solove (2011, p. 56) deveria se revelar em sentido contrário: em tempos de crise é que deveria ser mais incisiva a proteção à privacidade e às liberdades pessoais.

Nesse cenário, a proteção aos dados pessoais adquiriu, ao longo do tempo, uma necessária autonomia, como espécie de direito fundamental, tanto no plano doméstico (pela promulgação de atos legislativos destinados à tutela específica dos dados pessoais) quanto no plano multilateral e transnacional. A Carta de Direitos Fundamentais da União Europeia de 2000 o assegurava de forma própria em seu artigo 8º, § 1º, que dispõe que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" (UNIÃO EUROPEIA, 2000, p. 10). Ainda, nesse mesmo documento, garante-se no item 2° a necessidade de "[...] um tratamento leal [dos dados], para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei" (UNIÃO EUROPEIA, 2000, p. 10), garantido o direito de acesso e retificação às informações pessoais por seu titular.

Também no âmbito da interpretação e aplicação dessa previsão, o Tribunal de Justiça da União Europeia pronunciou-se de forma específica sobre a questão no conhecido caso Digital Rights Ireland (C-293/2012 e C-594/2012, apreciados em conjunto), em acórdão

datado de 8 de abril de 2014 (UNIÃO EUROPEIA, 2014).[5] Na ocasião, discutiu-se a Diretiva n. 2006/24/EC,[6] adotada pelo Conselho Europeu e pelo Parlamento Europeu na busca de uniformizar o tratamento da matéria dentre os países integrantes do bloco, que dispunha sobre o armazenamento de dados de telecomunicações por provedores de serviços de internet, para fins de utilização no combate a crimes graves cometidos na União Europeia. Na diretriz, não se alcançava o conteúdo das comunicações, mas especificamente:

> [...] os dados necessários para encontrar e identificar a fonte e o destino de uma comunicação, para determinar a data, a hora, a duração e o tipo de uma comunicação, o equipamento de comunicação dos utilizadores, bem como para localizar o equipamento de comunicação móvel, dados entre os quais figuram, designadamente, o nome e o endereço do assinante ou do utilizador registado, o número de telefone de origem e o número do destinatário e também um endereço IP para os serviços de internet. Estes dados permitem, designadamente, saber qual é a

[5] Cita-se com destaque a decisão do Tribunal Europeu por sua relevância internacional e pela consolidação que representa na afirmação do direito fundamental à proteção dos dados pessoais. Não se tratou, porém, da primeira vez que uma corte se dedicou ao tema. Pode-se citar, por exemplo, paradigmático caso julgado em 1983 pelo Tribunal Constitucional Federal Alemão, no qual se falava em uma "autodeterminação sobre a informação". O caso (BVerfGE 65, 1 – *Volkszählung*) dizia respeito à lei de 1982 que determinava a realização de recenseamento da população, a partir da coleta de dados como a profissão, o domicílio e o local de trabalho. Na ocasião, o tribunal assentou a constitucionalidade da lei, mas reconheceu a invalidade de alguns dispositivos, estabelecendo restrições sobre a comparação, a troca e a transmissão de dados em algumas situações. Ali, falava-se na necessidade de "uma proteção especialmente intensa" sobre o processamento de dados pessoais. Em suas razões, a corte assentou que "O livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais. [...] O direito fundamental garante o poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais." (MARTINS, 2005, p. 238).

[6] O ato normativo não foi o primeiro, no âmbito do Direito Comunitário europeu, a tratar do tema, colocando-se em uma sequência de outras disposições sobre a proteção de dados e informações pessoais nas ações de coleta, tratamento, tráfego e armazenamento, como as Diretivas n. 1995/46/CE e n. 2002/58/CE.

> pessoa com quem um assinante ou um utilizador registrado comunicou, e através de que meio, assim como determinar o tempo da comunicação e o local a partir do qual esta foi efetuada. Além disso, permitem saber com que frequência o assinante ou o utilizador registrado comunicam com certas pessoas, durante um determinado período. (UNIÃO EUROPEIA, 2014, § 26).

A partir de dois casos enviados pelas cortes máximas da Irlanda (High Court) e pela Áustria (*Verfassungsgerichtshof*), a questão chegou ao Tribunal Europeu. No primeiro, Digital Rights Ireland (uma organização da sociedade civil irlandesa para defesa dos direitos digitais) narrava que as medidas legislativas e administrativas de armazenamento de dados pessoais e informações eletrônicas seriam inválidas. No segundo, os proponentes também se queixavam de aspectos semelhantes. O próprio acórdão, em referência à manifestação da Corte Austríaca de remessa do caso ao Tribunal Europeu, destacava que:

> A conservação dos dados diz respeito quase exclusivamente a pessoas cujo comportamento não justifica sequer que os seus dados sejam conservados. Essas pessoas ficam expostas a um risco superior de que as autoridades investiguem os seus dados, tomem conhecimento do seu conteúdo, informem-se acerca da sua vida privada e utilizem esses dados com múltiplas finalidades, tendo designadamente em conta o número incomensurável de pessoas que têm acesso aos dados durante um período de, pelo menos, seis meses. Segundo o órgão jurisdicional de reenvio, há dúvidas, por um lado, quanto ao fato de esta diretiva poder alcançar os objetivos que prossegue e, por outro, quanto ao caráter proporcionado da ingerência nos direitos fundamentais em causa. (UNIÃO EUROPEIA, 2014, § 20).

Em síntese, argumentava-se nos dois casos que a diretiva e as respectivas leis nacionais estariam servindo como fundamento para a implementação de sistemas de vigilância em massa, em violação aos direitos fundamentais de privacidade e de proteção dos dados pessoais.

Analisada a questão, o Tribunal de Justiça da União Europeia assentou que a diretiva representava indevida ingerência no direito fundamental à proteção dos dados pessoais. Nesse sentido, a corte assentou que a diretiva não previa limitações como a aplicação a pessoas em relação às quais houvesse prévios indícios de participação em determinada atividade criminosa grave, não excepcionava situações de comunicações acobertadas por sigilo profissional, não restringia de forma adequada o período temporal ou determinada região geográfica a partir de qual se desse o armazenamento de dados, nem se sujeitava a um controle judicial prévio. Assim, apesar de atender a um objetivo efetivo de interesse geral — a "prevenção das infrações e na luta contra a criminalidade, designadamente a criminalidade organizada" (UNIÃO EUROPEIA, 2014, § 43) —, a medida não se revelava proporcional, tendo em vista que permitia "uma ingerência nos direitos fundamentais de quase toda a população europeia" (UNIÃO EUROPEIA, 2014, §56).

O caso permite identificar, portanto, que a afirmação da autonomia do direito fundamental à proteção de dados aporta novos limites materiais e procedimentais à atuação dos órgãos de persecução penal. Com efeito, a própria Diretiva n. 2006/24/EC cita conclusões de 19 de dezembro de 2002 do Conselho Justiça e Assuntos Internos, constituído pelos ministros da Justiça e de Assuntos Internos dos Estados-Membros da União Europeia, no sentido de que:

> [...] devido a um notável crescimento das possibilidades oferecidas pelas comunicações eletrônicas, os dados gerados pela utilização deste tipo de comunicações

> constituem um instrumento extremamente importante e útil na prevenção, investigação, detecção e de repressão de infrações penais, em especial contra a criminalidade organizada. (UNIÃO EUROPEIA, 2006, § 7°).

O texto – aprovado depois dos atentados de Londres de julho de 2005, em que se intensificou no Conselho Europeu a compreensão pela necessidade de estabelecer medidas comuns entre os países quanto à conservação de dados de telecomunicações – volta, mais à frente, a confessar sua motivação penal, no sentido de possibilitar novos meios de prevenção e repressão de delitos, especialmente os praticados por organizações criminosas:

> Visto que a conservação de dados se tem revelado um instrumento de investigação necessário e eficaz de repressão penal em vários estados-membros, nomeadamente em matérias tão graves como o crime organizado e o terrorismo, é necessário assegurar que as autoridades responsáveis pela aplicação da lei possam dispor dos dados conservados por um período determinado, nas condições previstas na presente diretiva. (UNIÃO EUROPEIA, 2006, § 9°).

No Brasil, há desde 1988 previsão constitucional da inviolabilidade do sigilo de dados (art. 5º, XII, da CRFB/1988), revelando-se possível falar em sua proteção não apenas como um desdobramento do direito à intimidade e à vida privada, mas como um direito fundamental autônomo, que reclama atuações estatais específicas – negativas e positivas – para sua tutela adequada (BRASIL, 1988; MENDES, 2018, p. 188). Ainda, a autodeterminação informativa é medida que ganha força normativa progressiva no país, sobretudo a partir da edição da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados), ato normativo que

representou a criação de um sistema protetivo aos dados pessoais e seu tratamento (BRASIL, 2018a).[7]

No âmbito do Supremo Tribunal Federal – STF, por exemplo, a autonomia do direito fundamental à proteção dos dados pessoais foi assentada por alguns ministros durante o julgamento da Ação Direta de Inconstitucionalidade n. 6.387 (BRASIL, 2020e), julgada em 7 de maio de 2020, em que se impugnava a Medida Provisória n. 954/2020, que dispunha sobre a coleta, a conservação e o compartilhamento de dados pessoais por empresas de telecomunicações com o órgão estatal de estatística, para fins de enfrentamento da pandemia de Covid-19. Na ocasião, o ato normativo não ultrapassou o juízo de proporcionalidade realizado pela corte, tendo sido considerado incompatível com a ordem constitucional brasileira.

Em reforço a essa autonomia, houve reconhecimento explícito do direito fundamental à proteção dos dados pessoais, inclusive nos meios digitais, pela superveniência da Emenda Constitucional n. 115, promulgada em 10 de fevereiro de 2022. A partir de sua edição, acrescentou-se nova disposição ao catálogo dos direitos fundamentais afirmados pelo art. 5º da Constituição brasileira (BRASIL, 1988), (inciso LXXIX), assegurando de forma expressa "nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais", assegurando à União a competência para "organizar e fiscalizar a proteção e o tratamento de dados pessoais" (art. 21, XXVI), bem como para legislar privativamente sobre a matéria (art. 22, XXX).

[7] Na legislação brasileira, também se destaca o Marco Civil da Internet, Lei n. 12.965/2014, que estabelece a internet como ambiente essencial ao exercício da cidadania, garantindo a seus usuários a "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação"; "a inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei"; e "a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial" (art. 7º, I, II e III) (BRASIL, 2014a).

Dessa forma, ao mesmo tempo em que surge um interesse cada vez maior sobre as informações pessoais digitais para execução do *ius puniendi* estatal, o direito fundamental à proteção dos dados pessoais implica que as medidas legislativas que disciplinam seu acesso, bem como as empreitadas investigativas sobre seu conteúdo devem se revelar proporcionais, isto é, adequadas e necessárias ao atendimento dos objetivos que justificam a relativização de sua inviolabilidade, sem que se vislumbre a alternatividade de outra medida menos gravosa. Assim, interesses como a persecução penal eficiente à criminalidade organizada são objetivos adequados à limitação da proteção dos dados pessoais, mas devem ser perquiridos com fundamento em lei e de forma limitada, pontual e justificada, sem que se promova uma devassa sobre os dados de pessoas indeterminadas.

3 TÉCNICAS ESPECIAIS DE INVESTIGAÇÃO EM MEIO DIGITAL: UTILIZANDO DADOS PESSOAIS NO PROCESSO PENAL

A partir das premissas do tópico anterior, chega-se à dinâmica relação entre o surgimento de novos direitos fundamentais limitadores da persecução penal e a necessidade de desenvolvimento de novas técnicas investigativas que, em um mundo cada vez mais digital e globalizado, permitam um eficiente combate ao crime organizado. Essa relação não revela contradição inerente, podendo sua justa medida de equilíbrio ser encontrada a partir dos mencionados critérios de proporcionalidade, cuja delimitação mais específica pode ser apreendida a partir da análise de alguns casos concretos. É o que se propõe a fazer na presente seção, a partir da identificação de alguns casos julgados no Brasil pelo Superior Tribunal de Justiça – STJ, sobre o tema de meios digitais de provas e seu possível confronto com o sigilo e a inviolabilidade dos dados pessoais, mediante aportes advindos do enfrentamento de temas similares também em outros países. A maioria dos casos se relaciona, em alguma medida, ao enfrentamento do crime organizado e mesmo os que não se vinculam de forma direta a essa

finalidade permitem solidificar premissas teóricas importantes para a sua persecução.

De início, surge relevante a requisição judicial de dados digitais armazenados por provedores de aplicação na internet relativamente a um conjunto indeterminado de pessoas. O tema foi apreciado pela Terceira Seção do STJ em um conjunto de casos[8] relacionados à investigação do homicídio da vereadora fluminense Marielle Franco e de seu motorista Anderson Gomes.

Nesses julgados, debatia-se sobre a validade de decisões do juízo de primeira instância que determinavam que alguns provedores fornecessem a identificação dos usuários de aplicativos que estivessem em uma região específica da cidade do Rio de Janeiro, dentro de um intervalo temporal também determinado (no caso, os limites eram de 15 minutos em um certo polígono de coordenadas em que um veículo relacionado ao crime havia sido visto), bem como a identificação dos IPs (Internet Prococols) de usuários do Google que, nos dias anteriores à prática do crime, tivessem realizado certas buscas nessa plataforma, a partir da delimitação de alguns parâmetros de pesquisa. Quanto ao ponto, destaca-se que a autorização judicial se dava em intervalo delimitado de tempo (de 10 de março 2018 a 14 de março de 2018, data do crime), a partir de algumas palavras-chave também delimitadas, relacionadas à investigação.[9]

As decisões de origem eram impugnadas pelo próprio Google, que argumentava que as circunstâncias do caso não justificavam a quebra do sigilo desses dados, nem se revelariam proporcionais, sobretudo por não recaírem sobre investigados específicos, mas

[8] RMS 60.698 (BRASIL, 2020a), RMS 61.302 (BRASIL, 2020b) e RMS 62.143 (BRASIL, 2020c), todos de relatoria do Ministro Rogerio Schietti, julgados pela Terceira Seção do STJ em 26 de agosto de 2020.

[9] Os parâmetros adotados foram os seguintes: "Marielle Franco", "Vereadora Marielle", "Agenda Vereadora Marielle", "Casa das Pretas", "Rua dos Inválidos, 122" ou "Rua dos Inválidos".

sobre um conjunto não identificado de pessoas. Em outros países, a empresa havia recebido ordens judiciais semelhantes, quando cumpriu a requisição de identificação de protocolos de internet a partir de parâmetros de pesquisa para identificação de suspeitos.[10]

Esses argumentos não foram acolhidos pelo STJ, que confirmou a validade das determinações judiciais, tendo em vista que havia um concreto interesse público relevante, reconhecido previamente por decisão fundamentada da autoridade judicial competente para supervisão das investigações, possibilitando uma limitação à inviolabilidade de dados estáticos de registro armazenados, não alcançando o conteúdo em si do fluxo de comunicações de dados.[11] Ademais, a decisão judicial apresentava elementos que restringiam a incidência da medida, a partir de critérios justificados e correlacionados de forma específica à investigação (circunstâncias de tempo, de lugar e de modo delimitadas), ainda que não houvesse – por absoluta impossibilidade e pela ineficácia, quanto ao ponto, dos outros meios investigativos previamente utilizados – a identificação individualizada das pessoas alcançadas, visto que esse era justamente o objetivo da diligência investigativa. Não se tratava, assim, de uma devassa geral e irrestrita de dados pessoais.[12]

[10] Cita-se o caso de Robert Kelly e Michael Williams, este último identificado como suspeito pela possível prática de um incêndio criminoso a um carro, a partir de protocolos de internet utilizados para buscas do endereço da vítima no dia do crime e na véspera (ARAS, 2020a).

[11] Com efeito, o Direito brasileiro comporta diferentes níveis protetivos conforme a maior ou menor intromissão nos dados pessoais, relativamente ao próprio conteúdo da comunicação em si, seus dados de armazenamento ou mesmo dados cadastrais propriamente ditos (MOURA; BARBOSA, 2020, p. 478). Nesse sentido, destaca-se recente decisão do STJ de que o mero requerimento, para que a guarda dos registros de acesso a aplicações de internet ou registros de conexão se dê por prazo superior ao legal, pode ser feito diretamente pela autoridade policial ou pelo Ministério Público, sem autorização judicial prévia, visto que a medida não traduz acesso aos dados armazenados (BRASIL, 2022).

[12] Vladimir Aras lembra o caso de Nicky Verstappen, garoto holandês de 11 anos morto em 1988 durante um acampamento de verão (ARAS, 2020b). A solução do caso só foi possível em 2008, após a realização de mais de 16 mil testes de DNA dentre os homens da região, que atenderam voluntariamente ao chamado da polícia. A busca permitiu restringir, mediante os traços genéticos que indicavam parentesco, o foco da investigação, até que se encontrasse, mediante busca e apreensão judicialmente autorizada na casa de um investigado, uma amostra 100% compatível com o material genético que havia sido encontrado nas roupas da vítima.

Assim, a corte considerou que, no caso, estavam atendidos os critérios de proporcionalidade da quebra de sigilo dos dados requisitados, tendo em vista que era adequada ao fim buscado e necessária ante à ineficácia de outros métodos de investigação.[13] Ainda, persistiria o dever de sigilo sobre os dados obtidos e não conexos à investigação criminal, de modo que a medida não levaria à exposição pública de pessoas não vinculadas ao fato criminoso.

Em outra situação, a ausência de critérios específicos de delimitação temporal levou o STJ a considerar inválida a quebra de sigilo de comunicações por *e-mail* em intervalo desproporcional de tempo. No Habeas Corpus n. 315.220/RS (BRASIL, 2015), investigava-se a prática dos crimes de corrupção, peculato e falsidade ideológica, tendo a autoridade judicial determinado a quebra de sigilo de *e-mails* dos investigados em um período superior a dez anos, sem que fossem apresentadas razões suficientes que concretamente indicassem a necessidade de que a diligência recaísse sobre tão largo tempo. Entendendo se tratar, assim, de medida desproporcional, declarou-se a nulidade das provas resultantes dessa diligência.

Em relação à determinação de identificação dos usuários de aplicações de internet que estivessem em uma dada região dentro de um intervalo temporal determinado, trata-se de técnica conhecida como *geofencing* (cercamento geográfico), que no Brasil encontra

[13] Nesse ponto, destaca-se trecho do voto proferido pelo ministro relator: "Quanto à proporcionalidade da quebra de dados informáticos, ela é adequada, na medida em que serve como mais um instrumento que pode auxiliar na elucidação dos delitos, cuja investigação se arrasta por mais de dois anos, sem que haja uma conclusão definitiva; é necessária, diante da complexidade do caso e da não evidência de outros meios não gravosos para se alcançarem os legítimos fins investigativos; e, por fim, é proporcional em sentido estrito, porque a restrição a direitos fundamentais que dela redundam – tendo como finalidade a apuração de crimes dolosos contra a vida, de repercussão internacional – não enseja gravame às pessoas eventualmente afetadas, as quais não terão seu sigilo de dados registrais publicizados, os quais, se não constatada sua conexão com o fato investigado, serão descartados." (BRASIL, 2020c).

respaldo legal no artigo 22 do Marco Civil da Internet (BRASIL, 2014a).[14] A partir da autorização judicial de acesso a dados digitais, permite-se identificar as pessoas que estavam em um espaço geográfico em determinado período, afunilando as investigações sobre possíveis suspeitos.

Nos Estados Unidos, discute-se sobre a validade jurídica dos "mandados de geocercamento" ("*geofence warrants*") ou "mandados de localização reversa" ("*reverse location warrant*"), sobretudo à luz da limitação de buscas e apreensões irrazoáveis, afirmada pela Quarta Emenda à Constituição daquele país. Apesar de seu texto afirmar a inviolabilidade sobre "pessoas, casas, papéis e pertences", também os dados pessoais são alcançados pelo dispositivo constitucional (GEOFENCE..., 2021, p. 2513). Assim é que:

> [...] a expansão dos métodos ocultos de investigação, com seu potencial de eliminação das barreiras à privacidade, provoca reativamente a configuração de defesas jurídicas de proteção do âmbito essencial da configuração da vida privada que se constituem a partir de uma dimensão de dependência recíproca entre legalidade e reserva de jurisdição. (PRADO, 2021, p. 179).

Em termos próximos, destaca-se que desde 2016 o Código de Processo Penal – CPP brasileiro (art. 13-A) autoriza que, no caso de alguns crimes específicos,[15] o Ministério Público ou a polícia requisite, de órgãos públicos ou de entidades privadas, dados e informações cadastrais da vítima ou de suspeitos, independentemente de autorização judicial prévia (BRASIL, 1941). Ateriormente havia previsões

[14] Sobre o ponto, destacam-se os arts. 22 e 23 da Lei n. 12.965/2014.

[15] Os crimes indicados pelo art. 13-A do Código de Processo Penal são: sequestro e cárcere privado; redução à condição análoga à de escravo; tráfico de pessoas; extorsão mediante restrição de liberdade da vítima; extorsão mediante sequestro e tráfico internacional de crianças.

similares nas leis que tratam do crime de lavagem de capitais (art. 17-B da Lei n. 9.613/1998) e das organizações criminosas (art. 15 da Lei n. 12.850/2013).

Ainda, no caso de investigação relacionada ao tráfico de pessoas, o CPP (art. 13-B) dispõe que essa requisição pode alcançar também informações de telecomunicações e telemática que permitam identificar a localização da vítima ou de suspeitos, mediante a triangulação de posicionamento de estações rádio base – ERB, por exemplo (BRASIL, 1941). Nesse caso, apesar de haver certa contradição na redação do dispositivo (LIMA, 2017, p. 139-141), exige-se prévia autorização judicial, havendo limites temporais e circunstanciais estabelecidos pela lei.

Em todo caso, renova-se a afirmação quanto à incidência dos vetores limitativos da adequação e necessidade dessas medidas investigatórias, bem como a estrita observância ao sigilo no tratamento dos dados coletados, inclusive com o descarte daqueles que não apresentem relevância para a atividade investigativa. Ainda, em qualquer dessas circunstâncias, os dados coletados deverão ter uma fiel documentação de sua cadeia de custódia, a fim de que se garantam a autenticidade e a integridade dos elementos informativos colhidos.

Com efeito, a inevitável digitalização da investigação criminal apresenta desafios adicionais ao registro da cadeia de custódia, sobretudo na documentação de sua cronologia e na garantia de não interferência dos agentes envolvidos. Aliás, a própria produção de elementos informativos digitais revela aspectos de difícil controle, especialmente nos chamados "meios ocultos de investigação" (MOURA; BARBOSA, 2020, p. 484), o que "reclama adequada compreensão quanto ao cabimento – forma e conteúdo – da cadeia de custódia das provas nesse cenário" (PRADO, 2021, p. 179).

Veja-se, nesse sentido, questão enfrentada pelo STJ relativamente à utilização do espelhamento de aplicativo de mensagens de celular

em computador (WhatsApp Web) para fins de investigação criminal. No caso RHC n.99.735/SC (BRASIL, 2018b), houve autorização judicial para que se apreendesse o celular de um investigado e, mediante a coleta de dados do WhatsApp e a leitura de um QR Code, a autoridade policial procedeu ao espelhamento de seu conteúdo em computador, a fim de que tivesse acesso ao histórico de mensagens recebidas e enviadas pelo investigado, bem como àquelas que ainda seriam enviadas, depois de a ele restituído o bem apreendido. A técnica investigativa que, inicialmente, parece promissora por permitir o conhecimento interno de detalhes de uma organização criminosa ou do planejamento de um crime, por exemplo, apresenta peculiaridades reconhecidas no mencionado julgamento.

Diferentemente de uma interceptação telefônica ou do acesso a trocas de *e-mails*, em que se registra o conteúdo das comunicações realizadas sem qualquer possibilidade de interferências pelos investigadores, o acesso espelhado ao aplicativo de mensagens permite que, em tese, as pessoas envolvidas possam interferir na troca de informações entre os investigados. A partir do emparelhamento entre celular e computador, é possível que por esse último meio, envie-se mensagens ou apague conteúdo presente ou passado, enviado ou recebido, em atualizações simultâneas entre as plataformas, sem possibilidade de posterior recuperação ou desfazimento.

Assim, a própria funcionalidade utilizada indica a possibilidade de que haja, por parte da investigação, interferência direta na comunicação, além de viabilizar o acesso a todo o histórico de conversas do investigado, alcançando conteúdo passado, quando ainda inexistia autorização judicial que permitisse a quebra de seu sigilo. Não se podendo garantir, portanto, a autenticidade e a mesmidade (PRADO, 2014, p. 17) dos elementos a serem aportados como prova em um processo penal, a corte assentou a nulidade da decisão judicial que havia autorizado o espelhamento do aplicativo, bem como das provas que resultaram dessa diligência. Para o futuro, porém, imagina-se se não seria possível desenvolver um *software* que permitisse registrar

e/ou limitar as atividades dos investigadores no computador, a fim de permitir a utilização válida desse meio de investigação.

Nota-se, assim, que o direito fundamental à inviolabilidade e à proteção dos dados pessoais aporta novas limitações às técnicas investigativas que constantemente surgem, impondo requisitos que devem ser observados pelos órgãos estatais de persecução penal. Em outras situações, porém, as informações colhidas podem advir de meios não oficiais de investigação, como quando derivam de descobertas jornalísticas ou vazamento de dados, refletindo novas preocupações no processo penal.

4 COMPARTILHAMENTO INTERNACIONAL DE DADOS EM INVESTIGAÇÕES JORNALÍSTICAS: CADEIA DE CUSTÓDIA E VERDADE PROCESSUAL

As circunstâncias afirmadas nos tópicos anteriores ganham relevo adicional quando se considera a dimensão internacional do enfrentamento à criminalidade organizada, não apenas como consequência de tratados entabulados entre os países,[16] mas também como inevitável desdobramento prático de sua investigação. Com

[16] Podem ser citados, nesse sentido, a Convenção de Palermo (Convenção das Nações Unidas contra o Crime Organizado Transnacional), como principal documento internacional destinado ao tema, promulgado internamente no Brasil pelo Decreto n. 5.015/2004. Seus protocolos adicionais versam sobre o Combate ao Tráfico de Migrantes por Via Terrestre, Marítima e Aérea; a Prevenção, Repressão e Punição do Tráfico de Pessoas, em Especial Mulheres e Crianças; e a Fabricação e o Tráfico Ilícito de Armas de Fogo, suas Peças, Componentes e Munições; os quais foram também promulgados no Brasil (Decretos n. 5.016/2004, 5.017/2004 e 5.941/2006, respectivamente). Ainda, surgem como documentos internacionais relevantes sobre o tema a Convenção de Viena de 1988 (Convenção contra o Tráfico Ilícito de Entorpecentes e Substâncias Psicotrópicas), promulgada pelo Decreto n. 154/1991 e a Convenção de Mérida (Convenção das Nações Unidas contra a Corrupção), promulgada pelo Decreto n. 5.687/2006. Por fim, a Convenção de Budapeste (Convenção sobre o Crime Cibernético), cuja adesão pelo Brasil se deu em dezembro de 2021, pelo Decreto Legislativo n. 37 daquele ano.

efeito, cada vez mais, impõe-se o enfrentamento internacional do crime organizado, cenário em que assumem relevância instrumentos como a cooperação internacional, não apenas entre os estados, mas também em abrangência dos organismos internacionais.

Ainda, acordos bilaterais de cooperação jurídica ostentam relevância crescente, como instrumentos de troca de informações entre países para investigações criminais, bem como para obtenção de dados pessoais de investigados. É o caso, por exemplo, do Mutual Legal Assistance Treaty – MLAT (Tratado de Assistência Jurídica Mútua em Matéria Penal), firmado entre Estados Unidos e Brasil em 1997, promulgado internamente pelo Decreto n. 3.810/2001 (BRASIL, 2001). Esse ato normativo tem, inclusive, seu alcance discutido perante o STF na Ação Declaratória de Constitucionalidade n. 51 (BRASIL, 2020d), especialmente no que diz respeito à (im)possibilidade de requisição direta de dados pessoais de comunicação em poder de provedores de aplicação que possuem sua sede no exterior.[17]

Não bastassem essas complexidades, casos recentes de relevantes investigações jornalísticas aportam desafios práticos adicionais ao compartilhamento internacional de informações e seu aproveitamento

[17] ADC n. 51, rel. Min. Gilmar Mendes. Na ação, requer-se a confirmação da constitucionalidade do Decreto n. 3.810/2001, além do artigo 237, II, do Código de Processo Civil, e dos arts. 780 e 783 do Código de Processo Penal (que versam sobre o cumprimento de cartas rogatórias e a cooperação jurídica internacional). Discute-se, na ação, se a mencionada requisição direta de dados de comunicação contrariaria esses dispositivos. A entidade autora (Federação das Associações das Empresas de Tecnologia da Informação) argumenta que apenas por meio da expedição de carta rogatória ou pelo cumprimento estrito dos instrumentos previstos pelo MLAT (solicitação pelo Ministério da Justiça brasileiro ao Department of Justice – DOJ norte-americano) é que esses dados poderiam ser acessados por autoridades judiciais brasileiras. A discussão ainda envolve reflexos da legislação interna estadunidense (Stored Communications Act e Cloud Act), relativamente à necessidade ou não de prévia decisão judicial interna para o envio dos dados pessoais solicitados. A corte realizou audiência pública para discussão do tema em 10 de fevereiro de 2020 e o julgamento do caso está agendado para 11 de maio de 2022.

na esfera penal. Exemplos como os conhecidos Panama Papers[18] e Swiss Leaks[19] revelam situações de vazamento de um elevado número de dados pessoais, nas quais o descobrimento de elementos de informação relativos ao possível cometimento de crimes diversos, inclusive no contexto transnacional, derivam de meios não estatais de investigação, como denúncias anônimas e bem documentadas feitas a veículos internacionais de comunicação ou descobertas decorrentes de iniciativas conjuntas de jornalismo investigativo. Nesses casos, as iniciativas são acobertadas pela liberdade constitucional de imprensa, mas sua inserção no processo penal pode representar peculiaridades relevantes.

Dentro de uma concepção democrática, a liberdade de imprensa, como reflexo de uma das liberdades públicas, possui proteção destacada e até mesmo preferencial nas ordens constitucionais. Isso porque, para além das inerentes finalidades que justificam a proteção dessas liberdades, elas também assumem importância instrumental para a garantia e implementação de outros direitos fundamentais. Como consequência, a regra é que prevaleça sua ampla liberdade, exigindo-se um significativo ônus argumentativo para as decisões que determinem sua restrição ou seu afastamento (ARABI, 2019, p. 127-128).

[18] O escândalo deriva do vazamento de milhões de documentos do escritório Mossak Fonseca (sediado no Panamá), enviados anonimamente a um jornal alemão e compartilhados com o Consórcio Internacional de Jornalistas Investigativos – Icij. Os arquivos relevavam um amplo esquema organizado de remessa oculta de valores bilionários a empresas de fachada sediadas em paraísos fiscais e relacionadas a diversos políticos de relevo e celebridades internacionais. A divulgação, iniciada em abril de 2016, despertou interesse em autoridades investigativas de diversos países, que passaram a buscar acesso a esses documentos.

[19] De forma semelhante, o caso deriva de investigações jornalísticas que partiram do vazamento de dados apropriados por um ex-funcionário de um relevante banco europeu, os quais revelariam um organizado esquema de evasão fiscal e alocação de recursos financeiros no exterior. O caso eclodiu em fevereiro de 2015, provocando também amplo interesse penal em sua investigação.

Há que se garantir, portanto, a livre e independente possibilidade de investigação jornalística, cujo grau de autonomia revela, inclusive, perfis mais ou menos democráticos de uma nação.[20] Seus reflexos penais, porém, despertam preocupações adicionais.

De início, há que se destacar que a busca da verdade jornalística e a busca da verdade processual penal apresentam escopos distintos (VIEIRA, 2012, p. 131). Para além das próprias limitações epistemológicas da apropriação de qualquer verdade, no processo penal, obedecidas as limitações materiais e procedimentais que são condições de validade de sua própria existência (GOMES FILHO, 1997, p. 54), a verdade probatória coloca-se como a "maior aproximação possível" (TARUFFO, 1992, p. 158) dos fatos, empreitada que não leva a certezas, mas a probabilidades daquilo que se investiga. Nesse sentido, a verdade processual "é apenas um pressuposto para se poder adequadamente decidir qual é a hipótese legal aplicável ao caso concreto" (BADARÓ, 2018, p. 518), revelando-se como uma verdade aproximativa (FERRAJOLI, 2014, p. 53).

Nessa perspectiva, o valor jornalístico de um elemento de informação não necessariamente coincidirá com seu valor probatório no processo penal, à luz das limitações materiais e formais distintas a que uma e outra forma de investigação estão sujeitas. A inviolabilidade de dados pessoais e das comunicações privadas, o devido processo legal e a ampla defesa são algumas das garantias cuja observância estrita pode não interessar à atividade jornalística investigativa. Trata-se, de outro lado, de requisitos de legitimidade da atuação dos órgãos estatais de persecução penal.

[20] Nesse sentido, cite-se a conhecida Classificação Mundial da Liberdade de Imprensa, promovida pela organização Repórteres Sem Fronteiras. No *ranking* de 2022, o Brasil ocupa a 110ª posição, dentre os 180 países integrantes do estudo (REPÓRTERES SEM FRONTEIRAS, 2022).

Em relação aos dados pessoais, cuja proteção consubstancia direito fundamental autônomo, é possível que informações obtidas sem prévia e justa autorização judicial e/ou legal sirvam, no âmbito da liberdade de imprensa, à busca da verdade jornalística. Entretanto, sua utilização no processo penal como meio de prova na persecução da verdade processual deve se cercar de cuidados adicionais, tanto nos momentos de sua admissão quanto naqueles de sua valoração e da decisão a partir dos fatos provados, conforme diferentes padrões de racionalidade que cada etapa exige (FERRER-BELTRÁN, 2007, p. 67-68).

Além dos aspectos materiais e procedimentais que limitam a atuação penal estatal, também a ausência de registro de sua cadeia de custódia pode ser elemento que influencie na admissão e valoração desses materiais como meios de prova. Com efeito, "a necessidade de documentação da cadeia de custódia é fundamental para assegurar o potencial epistêmico das fontes de provas reais" (BADARÓ, 2021, p. 8), o que se revela em relação a qualquer meio de prova. Sua regulamentação no Direito brasileiro, porém, é recente e ainda se guia pelos meios de prova físicos ou materiais (arts. 158-A a 158-F do Código de Processo Penal, incluídos pela Lei n. 13.964/2019).

Há que se considerar que em situações como as mencionadas acima, não há supervisão judicial ou contraditório sobre a formação dos elementos de informação, que por vezes derivam de vazamento de documentos – que inclusive podem representar, em si, atividade criminosa (como no caso de invasão a dispositivo informático). Assim, o mero acesso pelos órgãos estatais de persecução penal a esses documentos, via cooperação internacional, não necessariamente valida a sua utilização como meio de prova no processo penal. Nesse sentido, é ainda mais dificultosa a garantia de que os meios de prova sejam autênticos e íntegros, à luz dos vetores da mesmidade e da desconfiança (PRADO, 2014, p. 17).

Por sua própria natureza, há uma dificuldade intrínseca em "preservar a integridade do elemento probatório digital e de verificar sua autenticidade, além de determinar o cuidado extremado que se deve ter, haja vista os riscos concretos de manipulação e alteração de dados" (PRADO, 2021, p. 194). Nesse sentido, há de destacar que, por vezes, uma alteração propositada ou imprudente empreendida em um meio de prova digital pode se dar sem qualquer possibilidade de identificação ou rastreio posterior, visto que se trata de "fonte de prova que pode ser facilmente contaminada, sendo sua gestão muito delicada, por apresentar um alto grau de vulnerabilidade a erros" (BADARÓ, 2021, p. 8).

Jurisprudencialmente, o tema foi enfrentado em alguns casos julgados no Basil. Relativamente à interceptação telefônica e telemática, autorizada por decisão judicial prévia, válida e bem fundamentada, o STJ considerou, por exemplo, que o acesso integral ao conteúdo derivado de sua realização deve ser disponibilizado, tal qual captado, aos investigados e sua defesa, necessidade que não se supre pelo acesso aos autos do processo em si.

No Habeas Corpus n. 160.662/RJ (BRASIL, 2014b), em que se investigava a prática dos crimes de associação criminosa, descaminho e lavagem de capitais por organizado grupo de empresas reais e de fachada no Brasil e no exterior, houve, ainda durante a fase policial, extravio de parte do conteúdo captado, havendo, no material disponibilizado à defesa dos acusados, partes omissas e descontínuas nos áudios e *e-mails* capturados, em razão da formatação do computador utilizado durante as investigações, sem possibilidade de recuperação. Enfrentando a questão, o STJ afirmou que a preservação da integralidade dos elementos de informação colhidos na investigação é dado essencial à efetivação das garantias do contraditório e da ampla defesa, de modo que a falha na cadeia de custódia da prova

representaria um cerceamento ao direito de defesa. Dessa forma, ante à não preservação da integralidade do material probatório, foi reconhecida a nulidade das provas resultantes das interceptações telefônica e telemática.

Aspectos semelhantes também foram considerados no enfrentamento da matéria pelo STF. No caso Rcl n. 32.722/MT (BRASIL, 2019), relativo à investigação de uma organização criminosa de tráfico internacional de entorpecentes, houve o reconhecimento de dúvidas sobre a confiabilidade do resultado de interceptação telefônica e telemática. Discutia-se, assim, independentemente da validade e da legitimidade da realização da interceptação, se era adequado o acesso pela defesa aos dados interceptados em sua forma autêntica, integral e original.

Mais especificamente, havia suspeitas de que a autoridade policial teria alterado os arquivos que retratavam a transcrição de mensagens trocadas entre os investigados, substituindo os números de identificação originalmente indicados pelos nomes dos supostos emissores e destinatários das mensagens. A corte reconheceu, assim, a existência de uma dúvida concreta sobre a fidedignidade dos dados apresentados pela polícia, reafirmando à defesa, em razão da necessidade de registro e preservação adequada da cadeia de custódia, o acesso integral ao material informativo, tal qual originalmente colhido.[21]

[21] Registra-se que, na ocasião, o Ministro Edson Fachin proferiu voto divergente no sentido de que a possível alteração mencionada não representaria impactos à confiabilidade ou à autenticidade dos meios de prova, tendo em vista que todo o seu conteúdo havia sido disponibilizado à defesa dos investigados tal como colhidos na interceptação. Segundo a distinção que ali se fez, se havia dúvidas quanto à transcrição realizada, inexistiam suspeitas sobre o conteúdo propriamente dito.

Nota-se, assim, uma contínua preocupação legislativa, doutrinária e jurisprudencial com a correta preservação da cadeia de custódia, como elemento necessário à concreta efetivação do devido processo legal. Em relação aos dados digitais, essas disposições são ainda mais significativas, tendo em vista a inexistência de regulamentação legal específica e mesmo de consenso sobre as práticas e formas corretas de sua preservação.

Em relação aos elementos informativos resultantes de investigações jornalísticas realizadas no exercício legítimo da liberdade de imprensa, seu aproveitamento no processo penal deve cercar-se de cuidados adicionais, visto que não atendem, a princípio, características próprias da investigação criminal (supervisão judicial, reserva de jurisdição, contraditório, registro da cadeia de custódia). Essas peculiaridades devem, portanto, guiar os *standards* racionais e argumentativos de decisão nos momentos de admissão e valoração dos dados e das informações colhidas como meios de prova em um processo penal. A liberdade de imprensa deve mesmo ser ampla, mas a internalização de seus documentos e de sua produção informativa no processo penal deve se guiar por critérios que garantam a identidade, a integridade e a autenticidade daquilo que se admitir como meio de prova.

5 CONCLUSÃO

Em um processo penal democrático, a busca da verdade processual não pode se dar a qualquer custo, sob pena de invalidação de seus próprios resultados (CONDE, 2003, p. 112). Os limites formais e materiais que se colocam derivam da necessidade de que a eficiência da tutela penal estatal se alinhe à observância dos direitos fundamentais. Esses variados aspectos são dinâmicos e acompanham as mudanças sociais que se enfrentam. Assim é que os meios de investigação criminal

e os direitos fundamentais que o limitam atualizam-se constantemente, influenciando-se reciprocamente.

A essas constatações, somam-se ainda as limitações epistemológicas que a produção probatória intrinsecamente assume, contexto em que a busca da verdade processual é sempre aproximativa, levando a distintos graus de probabilidade dos fatos investigados, esclarecidos em procedimento dialético que permita o contraditório efetivo na verificabilidade das hipóteses acusatórias e defensivas. Assim, a busca de um procedimento válido é um dos elementos que confere justiça à própria decisão, ao permitir a "apuração confiável dos fatos relevantes do caso" (TARUFFO, 1997, p. 319-320, tradução nossa).

Nesse contexto, a utilização de dados pessoais no processo penal é medida necessária, mas que deve se cercar de cuidados peculiares. A promoção de uma persecução penal estatal eficiente é objetivo adequado à limitação da proteção dos dados pessoais, desde que obedecidos os critérios constitucionais e legais, que indicam a necessidade de uma intervenção limitada, pontual e justificada.

Em relação aos dados digitais, em atendimento a dificuldades inerentes que sua preservação apresenta, também a documentação de sua cadeia de custódia deve guiar a atuação dos órgãos de persecução penal, a fim de que se garanta a integralidade e a autenticidade dos documentos e elementos de informação colhidos. Adicionalmente, quando derivem de dados compartilhados a partir de investigações jornalísticas, a admissão e a utilização dessas informações como meios de prova no processo penal aportam a necessidade de cumprimento de um mais elevado ônus argumentativo, tendo em vista que sua produção ocorre sem contraditório ou supervisão judicial, por meios não oficiais de investigação.

Sem descuidar da necessidade de que essas investigações jornalísticas sejam protegidas no âmbito da liberdade de imprensa, sua utilização no processo penal deve considerar as peculiaridades que envolvem, a partir de distintos *standards* racionais e argumentativos de decisão nos momentos de admissão e valoração dos dados e das informações colhidas. A garantia de identidade, integridade e autenticidade dos meios de prova admitidos é medida essencial à consecução de um procedimento válido que busque uma decisão justa.

Ainda que esses valores pareçam contraditórios, deve-se buscar um equilíbrio que promova a tutela penal eficiente e a proteção dos direitos fundamentais dos investigados. Essa é a empreitada contínua a que se dedica o processo penal democrático, que cotidianamente se modifica e deve se atualizar.

REFERÊNCIAS

ARABI, Abhner Youssif Mota. As liberdades públicas e o Supremo: 30 anos de uma nova história constitucional. *In*: ARABI, Abhner Youssif Mota; MALUF, Fernando; MACHADO NETO, Marcello Lavènere (coord.). **Constituição da República 30 anos depois**: uma análise prática da eficiência dos direitos fundamentais – estudos em homenagem ao Ministro Luiz Fux. Belo Horizonte: Editora Fórum, 2019. p. 127-143.

ARAS, Vladimir. Acesso a dados do Google para investigações criminais. **Blog do Vlad**, [*S. l.*], 31 out. 2020a. Disponível em: https://vladimiraras.blog/2020/10/31/acesso-a-dados-do-google-para-investigacoes-criminais/. Acesso em: 10 fev. 2022.

ARAS, Vladimir. Acordos penais no Brasil: uma análise à luz do direito comparado. *In*: CUNHA, Rogério Sanches; BARROS, Francisco Dirceu; SOUZA; Renee do Ó; CABRAL, Rodrigo Leite Ferreira (org.). **Acordos de não persecução penal e cível**. Salvador: JusPodivm, 2021. p. 57-128.

ARAS, Vladimir. O Google e a vereadora assassinada no Rio. **Blog do Vlad**, [*S. l.*], 5 out. 2020b. Disponível em: https://vladimiraras.blog/2020/10/05/o-google-e-a-vereadora-assassinada-no-rio. Acesso em: 10 fev. 2022.

ARAS, Vladimir. Whistleblowers, informantes e delatores anônimos. *In*: ZANELLATO, Vilvana Damiani (org.). **A jurisprudência do Supremo Tribunal Federal**: Temas Relevantes. Porto Alegre: Verbo Jurídico, 2013. p. 359-406.

BADARÓ, Gustavo. A cadeia de custódia e sua relevância para a prova penal. *In*: SIDI, Ricardo; LOPES, Anderson Bezerra (org.). **Temas atuais da investigação preliminar no processo penal**. Belo Horizonte: D'Plácido, 2018. p. 517-538.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim do Instituto**

Brasileiro de Ciências Criminais, São Paulo, ano 29, n. 343, p. 7-9, jun. 2021.

BASSIOUNI, M. Cherif (ed.). **Globalization and its impact on the future of human rights and international criminal justice**. Portland: Intersentia, 2015.

BECK, Ulrich. **La sociedad del riesgo**: hacia una nueva modernidad. Barcelona: Paidós, 2002.

BOTTINI, Pierpaolo Cruz. **Crimes de perigo abstrato**: uma análise das novas técnicas de tipificação no contexto da sociedade de risco. 4. ed. rev. atual. São Paulo: Revista dos Tribunais, 2019.

BOTTINI, Pierpaolo Cruz. O paradoxo do risco e a política criminal contemporânea. *In*: MENDES, Gilmar Ferreira; BOTTINI, Pierpaolo Cruz; PACELLI, Eugênio. **Direito Penal contemporâneo**: questões controvertidas. São Paulo: Saraiva, 2011. p. 109-134.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. **Decreto n. 3.810, de 2 de maio de 2001**. Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997, corrigido em sua versão em português, por troca de Notas, em 15 de fevereiro de 2001. Brasília, DF: Presidência da República, 2001. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2001/d3810.htm. Acesso em: 17 maio 2022.

BRASIL. **Decreto-Lei n. 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro: Presidência da República, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 17 maio 2022.

BRASIL. **Lei n. 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras –COAF, e dá outras

providências. Brasília, DF: Presidência da República, 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9613.htm. Acesso em: 17 maio 2022.

BRASIL. **Lei n. 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei n. 9.034, de 3 de maio de 1995; e dá outras providências. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 17 maio 2022.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 8 fev. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais – LGPD. Brasília, DF: Presidência da República, 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 8 fev. 2022.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus n. 315.220/RS**. Relatora: Min. Maria Thereza de Assis Moura, 20 de outubro de 2015. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumetipoPes&termo=001975798201530000000&totalRegistrosPorPagina=40&aplicacap=processos. Acesso em: 17 maio 2022.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus n. 160.662/RJ**. Penal e processual penal. Habeas corpus substitutivo de recurso ordinário. Utilização do remédio constitucional como sucedâneo de recurso. Relatora: Min. Assusete Magalhães, 18 de fevereiro de 2014b. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1297583&num_registro=201000153608&data=20140317&formato=PDF. Acesso em: 17 maio 2022.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus n. 626.983/PR**. Relator: Min. Olindo Menezes, 8 de fevereiro de 2022. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2031001&num_registro=202003003135&data=20220222&formato=PDF. Acesso em: 17 maio 2022.

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus n. 99.735/ SC**. Recurso ordinário em habeas corpus. Penal e processo penal. Tráfico de drogas e associação ao tráfico. Autorização judicial de espelhamento, via
WhatsApp web, das conversas realizadas pelo investigado com terceiros. Relatora: Min. Laurita Vaz, 27 de novembro de 2018b. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1777437&num_registro=201801533498&data=20181212&formato=PDF. Acesso em: 17 maio 2022.

BRASIL. Superior Tribunal de Justiça (Terceira Seção). **Recurso em Mandado de Segurança n. 60698/RJ**. Relator: Min. Rogerio Schietti Cruz, 26 ago. 2020a. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumetipoPes&termo=007296896201881900000&totalRegistrosPorPagina=40&aplicacap=processos.ea. Acesso em: 17 maio 2022.

BRASIL. Superior Tribunal de Justiça (Terceira Seção). **Recurso em Mandado de Segurança n. 61302/RJ**. Relator: Min. Rogerio Schietti Cruz, 26 ago. 2020b. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroUnico&termo=00166393020198190000&totalRegistrosPorPagina=40&aplicacao=processos. Acesso em: 17 maio 2022.

BRASIL. Superior Tribunal de Justiça (Terceira Seção). **Recurso em Mandado de Segurança RMS n. 62143/RJ**. Relator: Min. Rogerio Schietti Cruz, 26 ago. 2020c. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/922867091/recurso-ordinario-em-mandado-de-seguranca-rms-62143-rj-2019-0318252-3. Acesso em: 17 maio 2022.

BRASIL. Supremo Tribunal Federal. **Ação Declaratória de Constitucionalidade n. 51/DF**. Requerente: Federação das Associações das Empresas Brasileiras de Tecnologia da Informação – ASSESPRO Nacional. Intimando: Presidente da República. Relator: Min. Gilmar

Mendes, 9 de dezembro de 2020d. Disponível em: https://stf.jusbrasil.com.br/jurisprudencia/1143005379/acao-declaratoria-de-constitucionalidade-adc-51-df-0014496-5220171000000/inteiro-teor-1143005402. Acesso em: 17 maio 2022.

BRASIL. Supremo Tribunal Federal. **Reclamação n. 32.722/MT**. Reclamante: Ricardo Cosme Silva dos Santos. Reclamado: Juízo da 1ª Vara da Subseção Judiciária de Cáceres. Relator: Min. Gilmar Mendes, 7 de maio de 2019. Disponível em: https://stf.jusbrasil.com.br/jurisprudencia/861522996/reclamacao-rcl-32722-mt-mato-grosso-0083429-4320181000000/inteiro-teor-861523000. Acesso em: 17 maio 2022.

BRASIL. Supremo Tribunal Federal. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade n. 6.387/DF**. Medida cautelar em ação direta de inconstitucionalidade. Referendo. Medida Provisória n. 954/2020. Emergência de saúde pública de importância internacional decorrente do novo Coronavírus (Covid-19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o Instituto Brasileiro de Geografia e Estatística [...]. Relatora: Min. Rosa Weber, 7 de maio de 2020e. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 17 maio 2022.

CONDE, Francisco Muñoz. **La búsqueda de la verdad en el proceso penal**. 2. ed. Buenos Aires: Hamurabi, 2003.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Convenção Americana Sobre Direitos Humanos**. San José, Costa Rica: CIDH, 22 nov. 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em:8 fev. 2022.

CRUZ, Rogerio Schietti. **Prisão cautelar**: dramas, princípios e alternativas. 6. ed. rev. atual. e ampl. Salvador: Juspodivm, 2021.

DIAS, Jorge de Figueiredo. **Direito Processual Penal**. Coimbra: Coimbra Editora, 1984.

EMPOLI, Giuliano da. **Os engenheiros do caos**. São Paulo: Vestígio, 2020.

EUROPEAN COURT OF HUMAN RIGHTS. Council of Europe. **Convenção Europeia dos Direitos do Homem**. France: ECHR, [2021]. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf. Acesso em: 8 fev. 2022.

FERRAJOLI, Luigi. **Direito e razão**: teoria do garantismo penal. 4. ed. rev. São Paulo: Revista dos Tribunais, 2014.

FERRER-BELTRÁN, Jordi. **La valoración racional de la prueba**. Madrid:Marcial Pons, 2007.

GEOFENCE warrants and the fourth amendment. **Harvard Law Review**, Cambridge, v. 134, n. 7, May 2021. Disponível em: https://harvardlawreview.org/wp-content/uploads/2021/05/134-Harv.-L.-Rev.-2508-2.pdf. Acesso em: 14 fev. 2022.

GOLDSCHMIDT, James. **Derecho, derecho penal y proceso**. Tomo III - El proceso como situación jurídica: una crítica al pensamiento procesal. Madrid: Marcial Pons, 2015.

GOLDSCHMIDT, James. **Problemas juridicos y politicos del proceso penal**: conferencias dadas en la Universidad de Madrid en los meses de diciembre de 1934 de enero, febrero y marzo de 1935. Barcelona: Bosch, 1935.

GOMES FILHO, Antonio Magalhães. **Direito à prova no processo penal**. São Paulo: Revista dos Tribunais, 1997.

HASSEMER, Winfried. **Persona, mundo y responsabilidad**: bases para una teoría de la imputación en derecho penal. Santa Fé de Bogotá: Temis, 1999.

KAISER, Brittany. **Manipulados**: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque. Rio de Janeiro: Harper Collins, 2020.

LIMA, Renato Brasileiro de. **Manual de Processo Penal**. 5. ed. rev. atual. Salvador: Juspodivm, 2017.

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

MELLO, Patrícia Campos. **A máquina do ódio**: notas de uma repórter sobre *fake news* e violência digital. São Paulo: Companhia das Letras, 2020.

MENDES, Laura Schertel Ferreira. *Habeas* data e autodeterminação informativa: os dois lados da mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 185-216, jul./dez. 2018.

MOURA, Maria Thereza Rocha de Assis; BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. *In*: LUCON, Paulo Henrique dos Santos *et al.* (coord.). **Direito, processo e tecnologia**. São Paulo: Revista dos Tribunais, 2020. p. 477-502.

PRADO, Geraldo. Ainda sobre a "quebra da cadeia de custódia das provas". **Boletim IBCCrim**, São Paulo, v. 22, n. 262, p. 16-17, set. 2014.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. 2. ed. Madrid: Marcial Pons, 2021.

REPÓRTERES SEM FRONTEIRAS. **Análises 2022**. [*S. l.*]: RSF, 2022. Disponível em: https://rsf.org/pt-br/ranking. Acesso em: 17 maio 2022.

ROXIN, Claus. **Derecho procesal penal**. Traducción de la 25ª edición alemana. Buenos Aires: Editores del Puerto, 2000.

SHAW, Mark; KEMP, Walter. Rethinking Multilateral Responses to Organized Crime. *In*: BASSIOUNI, M. Cherif (ed.). **Globalization and its impact on the future of human rights and international criminal justice**. Portland: Intersentia, 2015. p. 327-348.

SOLOVE, Daniel J. **Nothing to hide**: the false tradeoff between privacy and security. New Haven, London: Yale University Press, 2011.

SOLOVE, Daniel J. **The digital person**: technology and privacy in the information age. New York: New York University Press, 2004.

TARUFFO, Michele. Idee per una teoria della decisione giusta. **Rivista Trimestrale di Diritto e Procedura Civile**, v. 51, n. 2, p. 315-328, 1997.

TARUFFO, Michele. **La prova dei fatti giuridici**. Milano: Giuffre, 1992.

UNIÃO EUROPEIA. Parlamento Europeu. Carta dos direitos fundamentais da União Europeia. Elaborado em: Nice, França, 7 dez. 2000. **Jornal Oficial das Comunidades Europeias**: [Europa], n. C 304/1, 18 dez. 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 8 fev. 2022.

UNIÃO EUROPEIA. Parlamento Europeu. Conselho da União Europeia. Directiva n. 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006. Relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE. **Jornal Oficial da União Europeia**: [Europa], n. L 105/54, 14 abr. 2006. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32006L0024&from=PT#d1e39-54-1. Acesso em: 8 fev. 2022.

UNIÃO EUROPEIA. Tribunal de Justiça. **Acórdão do Tribunal de Justiça, de 8 de abril de 2014**. Comunicações eletrônicas, Diretiva 2006/24/CE, serviços de comunicações eletrônicas publicamente disponíveis ou de redes públicas de comunicações, conservação de dados gerados ou tratados no contexto da oferta desses serviços, validade, artigos 78° e 11° da Carta dos Direitos Fundamentais da União Europeia.[Europa]: InfoCuria Jurisprudência, 2014. Disponível em: https://curia.europa.eu/juris/document/document.jsf?%20text=&docid=150642&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=586%203500. Acesso em: 8 fev. 2022.

VIEIRA, Ana Lúcia Menezes. **O sigilo da fonte de informação jornalística como limite à prova no processo penal**. 2012. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, Cambridge, v. 4, n. 5, p. 193-220, 15 Dec. 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents. Acesso em: 9 fev. 2022.