EXCELENTÍSSIMA SENHORA MINISTRA ROSA WEBER DO SUPREMO TRIBUNAL FEDERAL, RELATORA DO RECURSO EXTRAORDINÁRIO EM MANDADO DE SEGURANÇA N. 1.301.250

O **Instituto Brasileiro de Ciências Criminais** (**IBCCrim**), regularmente habilitado como *AMICUS CURIAE*, vem perante V. Exa., por meio de seus procuradores signatários, apresentar seu parecer, com o objetivo de fornecer subsídios a essa Corte para o aprimoramento da prestação jurisdicional no âmbito do recurso acima identificado.

I. PRELIMINARMENTE: QUEM MANDOU MATAR MARIELLE FRANCO E ANDERSON GOMES?

A morte violenta de Marielle escancara as diversas dimensões da gravidade da situação da segurança pública no Brasil. Marielle Franco era mulher, negra, moradora da periferia e defensora de direitos humanos, atributos que caracterizam as vítimas usuais da violência em geral e da própria violência estatal.

Marielle era vereadora, membro de um dos Poderes políticos, eleita com expressiva votação, de bases eleitorais geralmente sub-representadas no espectro político brasileiro.

Conforme orientação da Comissão Interamericana de Direitos Humanos e do Alto Comissariado de Direitos Humanos das Nações Unidas, é dever prioritário do Estado garantir a proteção de defensoras e defensores dos direitos humanos.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

No caso de Marielle e Anderson, essa proteção não foi efetiva. Cabe, agora, a promoção da devida investigação, rompendo com o histórico de impunidade de crimes dessa natureza.

Marielle denunciou incansavelmente os abusos da Polícia Militar, as contradições do Direito Penal e o genocídio da juventude negra do país, pautas que são o alicerce do IBCCRIM. E é a sua luta que alerta para o risco de se expandir o Direito Penal, principalmente à custa de garantias constitucionais. Marielle sabia que, ao final, a vítima preferencial desse Direito Penal ampliado e distorcido seria o seu próprio povo, periférico, preto e pobre.

Diante dessas considerações, passa-se à análise jurídica do caso.

II. BREVE RESUMO

O presente recurso foi impetrado pelas empresas de tecnologia Google Brasil Internet LTDA e Google LCC, impugnando ordem judicial originária da 4ª Vara Criminal da Comarca do Rio de Janeiro/RJ no âmbito das investigações dos homicídios da Vereadora Marielle Franco e do Sr. Anderson Gomes, ocorridos no dia 14 de março de 2018.

Em síntese, o objeto da irresignação é a determinação da entrega, pelas recorrentes, dos endereços de IP (*Internet Protocol*) de qualquer pessoa que, no período de 10.3.2018 a 14.3.2018, tenha realizado buscas na plataforma das recorrentes com as seguintes palavras-chave: "Marielle Franco"; "Vereadora Marielle"; "Agenda Vereadora Marielle"; "Casa das Pretas "; "Rua dos Inválidos, 122"; e/ou, "Rua dos Inválidos".

Trata-se, portanto, de determinação de quebra de sigilo telemático de uma coletividade de pessoas, sem que se apontem elementos mínimos de sua relação com os fatos investigados. A questão constitucional, assim, diz respeito à possibilidade da quebra de sigilo de dados pessoais de um grupo de pessoas sem individualização específica ou, ainda, sem estabelecimento de critério que consiga determinar a quantidade de pessoas atingidas pela medida.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

No julgamento do recurso especial, a 3ª Seção do STJ, por maioria, negou-lhe provimento, deduzindo os seguintes fundamentos centrais:

(i) O direito ao sigilo de dados, garantido pelo art. 5º, inc. X, da Constituição Federal, não constitui direito absoluto, sendo possível seu afastamento por interesse público relevante, desde que com decisão judicial fundamentada na necessidade da medida para investigações criminais e ancorada em indícios de ocorrência de ilícito penal;

(ii) De acordo com jurisprudência reiterada do Supremo Tribunal Federal e do Superior Tribunal de Justiça, a quebra de sigilo de "dados informáticos estáticos" (ou registros) não está sujeita ao mesmo nível de proteção que a interceptação do "fluxo de comunicações", sendo a amplitude de proteção deste maior do que a daqueles;

(iii) A quebra do sigilo de "dados estáticos" não está sujeita aos limites da Lei 9.296/1996 (Lei de interceptações telefônicas), mas à Lei 12.965/2012 (Marco Civil da Internet), que, em seus artigos 13 e seguintes, estipula os seguintes requisitos para a determinação da medida: a) indícios de ocorrência de ilícito; b) fundamento a respeito da efetividade da quebra para a investigação; e c) indicação do lapso temporal a que se referem os dados requisitados. Não há, portanto, qualquer determinação legal para que haja a individualização da medida;

(iv) A determinação judicial diz respeito à entrega de dados registrais que identificam aparelhos utilizados pelos usuários, não estando necessariamente relacionados a pessoas;

(v) É justamente objetivo dos referidos dispositivos do Marco Civil da Internet possibilitar que esse tipo de técnica investigativa ocorra;

(vi) A proporcionalidade da medida se justifica pela complexidade e extrema gravidade do crime, notadamente por suas circunstâncias,

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

não havendo imposição de risco excessivo à privacidade e à intimidade.

Em suas razões recursais, as empresas alegam violação aos artigos 5º, X e XII, e 93, IX:

> I. Art. 5, X e XII, da Constituição Federal e o núcleo essencial da proteção à privacidade e aos dados pessoais: incompatibilidade com ordens exploratórias que afetam uma quantidade indeterminada de inocentes. Informações sobre pesquisas que uma pessoa realiza no âmbito privado de uso de um motor de busca na internet dizem respeito a pensamentos, interesses e opiniões que compõem a intimidade e a vida privada de alguém. Nesses termos, só pode haver mitigação do direito à privacidade sobre tais buscas de forma contextual, específica e baseada em justa causa com relação ao sujeito afetado pela intervenção — isto é, de forma individualizada. Viola a Constituição promover uma varredura genérica em dados de pesquisa, para fornecimento de lista genérica de dados pessoais de usuários insuspeitos, unidos pela circunstância singela de terem feito pesquisas por palavras-chave genéricas (incluindo termos comuns e populares como o nome de uma autoridade pública ou uma rua movimentada).
> II. Arts. 5, X e XII, e 93, IX da Constituição Federal: Inconstitucionalidade de ordens de quebra de sigilo com fundamentação insuficiente e inespecífica em relação à medida deferida. A Constituição impõe um dever específico de fundamentação para ordens de quebra de sigilo, que não se preenche com a mera alegação de que a medida seria imprescindível. A manutenção do regime republicano depende da fundamentação adequada das decisões restritivas de direito. Em sede de investigação criminal, trata-se primordialmente de dever que contemple de forma específica e contextual a justa causa para a restrição de liberdade fundamental dos indivíduos afetados. De fato, a vedação a quebras genéricas e a necessidade de demonstração da necessidade da medida são extraídas da própria Constituição, em especial da necessidade de fundamentação das decisões judiciais. Ainda que quebras de sigilo genéricas fossem admitidas — e não são, vale reiterar —, o ônus de fundamentação seria ainda maior — não menor, como supôs o v. acórdão recorrido.
> III. Art. 5, X e XII, da Constituição Federal e princípio da proporcionalidade, em suas três vertentes: medida que transfigura serviço de busca na internet em ferramenta de investigação para fins de criação de evidência criminal. As considerações do v. acórdão recorrido sobre a suposta proporcionalidade da medida são marcadamente genéricas sobre a ponderação entre privacidade e segurança pública. Em termos concretos e específicos, a ordem é: (i) inadequada, já que, mesmo que fosse compatível com o sistema constitucional, a medida não oferece mínima garantia de que levará ao autor ou aos autores do delito investigado – o serviço de buscas depende de uma conta ativa e pode ser objeto de apagamento ou edição, sendo certo que os termos de busca indicados são genéricos e associados a pessoas, projetos e locais de relevância pública; (ii) desnecessária: não basta a menção genérica de que a medida é necessária para

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

> viabilizar investigações — o que transformaria as salvaguardas legais de motivação e fundamentação de ordens judiciais e controle de proporcionalidade em mera fórmula ritual; e (iii) desproporcional em sentido estrito – um verdadeiro exercício de pescaria aleatória, a determinação aceita o dano colateral de quebrar o sigilo de milhares de inocentes que tenham simplesmente feito buscas na internet, assumindo que a medida extrema seria justificável pela possibilidade eventual de obter alguma pista sobre suspeitos adicionais.

III. AS NOVAS CIRCUNSTÂNCIAS SOCIAIS: MUDANÇAS TECNOLÓGICAS E O TRATAMENTO DE DADOS PESSOAIS

A fim de bem responder às questões propostas, é necessário iniciar por uma reflexão de ordem sociológica. Foram profundas e aceleradas as mudanças tecnológicas que alteraram a organização comunitária, tornando obsoletos e insuficientes conceitos antes aptos a explicar a dinâmica social:

> No estágio atual, a sociedade está encravada por uma nova forma de organização em que a informação é o elemento nuclear para o desenvolvimento da economia, substituindo os recursos que outrora estruturavam as sociedades agrícola, industrial e pós-industrial.
>
> Essa nova forma de organização social foi sedimentada em razão da evolução tecnológica recente, que criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais inimaginável. Os relacionamentos sociais foram energizados por um fluxo informacional que não encontram mais obstáculos físicos distanciais. Há uma nova compreensão (mais abreviada) da relação entre tempo-espaço, o que outrora acarretava maior cadência às interações sociais."[1]

É justamente por conta desse contexto que diversos ramos do pensamento estão voltando as suas atenções para o estudo dos impactos da tecnologia e da sociedade da informação em seus campos de análise, em especial, o uso da inteligência artificial em processos decisórios e a coleta massiva de dados pessoais. Aliada a estes, uma preocupação constante das sociedades democráticas

[1] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. GenForense: Rio de Janeiro, 2021, p. 4-5.

tem sido a expansão dos mecanismos de vigilância. Zuboff defende, por exemplo, a existência de um "capitalismo de vigilância"[2].

O tema é, por óbvio, especialmente sensível para a Justiça Criminal. Medidas tomadas em nome da segurança pública e privada foram laboratórios para o desenvolvimento das novas tecnologias de tratamento de dados. Em 2013, Edward Snowden revelou que a National Security Agency (NSA), desde 2002, realizava o tratamento massivo e indiscriminado (ou seja, sem autorização legal individualizada) de metadados[3] em suas investigações, a fim de identificar suspeitos de envolvimento com grupos terroristas.

Em sequência, órgãos de segurança pública também passaram a utilizar essa tecnologia, de início restrita à Guerra ao Terror, em seu cotidiano. Assim, o processamento massivo de dados pessoais passou a ser combate à criminalidade. Os exemplos são múltiplos: além da quebra de sigilo em investigações criminais, há criação de sistemas de decisões automatizadas, como o sistema COMPAS[4], tecnologias de reconhecimento facial, policiamento preditivo (criação de padrões

---

[2] "*Industrial capitalism depended upon the exploitation and control of nature, with catastrophic consequences that we only now recognize. Surveillance capitalism, I have suggested, depends instead upon the exploitation and control of human nature. The market reduces us to our behavior, transformed into another fictional commodity and packaged for others' consumption. In the social principles of instrumentarian society, already brought to life in the experiences of our young, we can see more clearly how this novel capitalism aims to reshape our natures for the sake of its success*" (ZUBOFF, Shoshana. The Age of Surveillance Capitalism: **The Fight for a Human Future at the New Frontier of Power**. Nova Iorque: Publicaffairs, 2019, p. 440).

[3] "Consideram-se metadados 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 dados de localização geográfica do dispositivo (como Estação Rádio Base), códigos de identificação de dispositivos (como IMEI), etc." (ABREU, Jacqueline de Souza, ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil**: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2ª ed., 2017, p. 17).

[4] Acrônimo para *Correctional Offender Management Profiling for Alternative Sanction*, trata-se de sistema de inteligência artificial criado para realizar prognósticos de periculosidade no sistema de justiça criminal norte-americano, sendo decisivo em decisões da execução penal, como a liberdade condicional. "O programa COMPAS é frequentemente declarado racista: ele atribui a pessoas de pele escura, em princípio, uma maior probabilidade de reincidir. Isso ocorreria apesar de que o programa não leve de forma explícita a raça do afetado; a raça se correlacionaria com fatores como morar em região de alta criminalidade, falta de emprego fixo existência de conhecidos criminosos etc., fatores esses que estariam mais presentes em pessoas de pelo escura que em outros grupos demográficos" *in* GRECO, Luís. **Poder de julgar sem responsabilidade de julgador**: a impossibilidade jurídica do juiz-robô. São Paulo: Marcial Pons, 2020, p. 29.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

algoritmos que visam a prever ou a antecipar comportamentos criminosos a partir do tratamento massivo de dados), entre outros.

Alguns são por demais preocupantes. Recentemente, a utilização do *software* espião Pegasus revelou que técnicas de engenharia social serão uma realidade cada vez mais presente na prática de agências de segurança. No caso do Pegasus, o programa, maliciosamente instalado em *smartphones*, os transformava em dispositivos de espionagem completo, com acesso ao microfone, câmera, localização e tudo que fosse realizado no aparelho. Há sérios indícios de que o aparelho foi utilizado para a perseguição de adversários políticos[5].

No Brasil, o Tribunal de Contas da União autorizou a compra de sistema de inteligência denominado Harpia, o qual foi confundido com o sistema Pegasus. Desenvolvido por empresa brasileira, o *software* não realiza a invasão de dispositivos eletrônicos, ou seja, o "hackeamento" de celulares ou computadores, permitindo o acesso indevido a *e-mails*, aplicativos de mensagens ou qualquer outra aplicação do dispositivo. Realiza, contudo, o tratamento massivo de dados públicos disponíveis na internet, os quais podem ser considerados pessoais e sujeitos aos princípios de proteção de dados.

Na análise acerca da permissibilidade de compra do *software* Harpia, em caráter liminar, o TCU suspendeu a aquisição da ferramenta por possíveis riscos a direitos fundamentais:

> 103. Boa parte das argumentações se centrou agora no suposto perigo da contratação da solução da empresa Harpia, que teria os mesmos riscos embutidos da ferramenta Pegasus; que usaria dados oriundos de violações e de outras atividades potencialmente ilegais. No entanto, não foram trazidos aos autos concretamente evidências nesse sentido.
>
> 104. É inegável e justa a preocupação da denunciante quanto à contratação em exame. E este Tribunal, mediante Despacho do ministro relator, reconheceu o risco da aquisição da solução em fontes abertas, quanto à exposição indevida das informações obtidas, à precariedade do detalhamento da descrição da solução e das justificativas da contratação, ao desvio de finalidade, bem como quanto às

[5] De acordo com reportagem da BBC, há denúncias de que o Spyware Pegasus tenha sido utilizado para espionagem de políticos em diversos países do mundo. Disponível em: https://www.bbc.com/portuguese/internacional-57885795

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

> medidas para mitigar os riscos apontados. Por isso mesmo, determinou a realização de oitivas junto ao órgão contratante, e a outros atores envolvidos indiretamente nessa contratação. (TCU, acórdão nº 2678/2021, TC *014.760/2021-5,* Rel. Min. Bruno Dantas, j. 10.11.21).

Após, o TCU autorizou a compra do Harpia, por entender que o sistema de inteligência não era invasivo. Trata-se, de acordo com o julgado, de ferramenta que realiza análise de grande quantidade de dados públicos, sem a invasão de privacidade:

> 40. Enfatiza a Dint que não se trata de solução invasiva de dados pessoais, de pessoa natural ou jurídica, sem a observância do direito e garantia fundamental à intimidade, a vida privada, a honra e a imagem das pessoas, e sim de solução que visa condensar os dados disponíveis em fontes abertas (endereços, sites e redes sociais), indexadas ou não, para pesquisa por palavras específicas de interesse da inteligência de Segurança Pública, uma vez que as fontes abertas podem proporcionar grande quantidade de informações de domínio público, com o potencial de gerar conhecimento com alto valor agregado, de forma mais simples e com menor custo.
> 41. Nesse sentido, arremata a entidade que a solução é um meio de realizar pesquisa em uma grande quantidade de dados, coleta e posterior análise do que foi encontrado publicamente em todas as camadas da internet, e não somente em uma parte dela, como acontece atualmente. (TCU, acórdão nº 1331/22, TC nº *014.760/2021-5,* Rel. Min. Bruno Dantas, j. 08.06.22).

Ainda mais recentemente, foi divulgada informação de que a ABIN monitorou localização de telefones celulares por meio de software, o que foi possível apenas com a informação do número telefônico relativo ao aparelho a ser localizado[6].

Somada à compra desse tipo de aplicação (no próprio acórdão acima mencionado, há menção a diversas compras semelhantes no âmbito estadual), as agências de investigação já possuem acesso a um amplo acervo de dados e informações dos cidadãos, seja por bancos públicos ou pela determinação legal de

[6] Com informações: "Caso Abin: especialistas apontam falta de previsão legal e afronta a direitos constitucionais em uso de programa secreto". Disponível em: https://oglobo.globo.com/politica/noticia/2023/03/especialistas-apontam-falta-de-previsao-legal-e-afronta-a-direitos-constitucionais-em-uso-de-programa-secreto-de-monitoramento-pela-abin.ghtml. Último acesso em 4.5.23.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

guarda de registros imposta pelo Marco Civil da Internet[7]. Em linhas gerais, a Lei determina que haja a guarda de registros de conexão (por 01 ano) e de registros de acesso a aplicações de internet (por 06 meses). Em tese, à vista disso, há disponibilidade de acesso a boa parte das informações geradas pelo uso da internet no País, a depender de decisão judicial para sua liberação. Consequentemente, aquilo que separa os órgãos de segurança pública de ter acesso a todo esse volume de informações são os limites impostos pelo Direito Constitucional e pelo Direito Penal, justamente o debate aqui posto.

IV. QUESTÕES CONSTITUCIONAIS EM DEBATE

As razões recursais, como visto, apontam as seguintes violações ao texto constitucional: (i) proteção e privacidade de dados pessoais (art. 5º, X e XII); (ii) dever de fundamentação das decisões judiciais (art. 5º, X e XII, e art. 93, IX); e (iii) princípio da proporcionalidade (art. 5º, X e XII).

Em contrapartida, em seu parecer, a Procuradoria-Geral da República aponta para o necessário respeito aos deveres estatais de investigar (segurança pública como direito social, garantido pelo art. 6º da Constituição Federal), correlacionados com o direito à memória e à verdade. Tais deveres configurariam balizas da sociedade democrática, assumindo especial relevância para o presente caso.

Assim posta a controvérsia, é preciso admitir que não se está diante de um comum sopesamento no Direito Penal, que usualmente define seus limites e possibilidades a partir da contraposição entre garantias individuais e a persecução penal (art. 5º, XII, CF). A possibilidade de acesso a dados pessoais de um sem-número de pessoas remete a uma outra questão constitucional, recentemente incluída no texto constitucional pela Emenda Constitucional 115/2022:

> "LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."

[7] A respeito do tema, destaca-se o estudo "**Vigilância sobre as comunicações no Brasil**: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais." Disponível em: http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

Trata-se da positivação expressa de um direito fundamental cuja existência fora reconhecido por esse Supremo Tribunal Federal na ADI 6387, ou "Caso IBGE", a partir do conceito da autodeterminação informativa.

A autodeterminação informativa deve ser compreendida como "o poder de determinação do indivíduo com relação à coleta e ao tratamento de seus dados pessoais"[8]. Assim, trata-se de direito fundamental que deve ser entendido de forma autônoma ao da privacidade:

> O Tribunal formulou, assim, uma tutela constitucional mais ampla e abstrata do que o direito à inviolabilidade da esfera íntima e da vida privada. Essa tutela poderá ser aplicada em inúmeros casos futuros envolvendo a coleta, o processamento e o compartilhamento de dados pessoais no Brasil. O conteúdo desse direito fundamental exorbita aquele protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados, ao revés, refere-se a qualquer dado que identifique ou possa identificar um indivíduo[9].

Nesse sentido, o voto da Min. Rosa Weber no caso IBGE:

> A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos. Esses direitos são extraídos da interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do *habeas data* (art. 5º, LXXII), todos previstos na Constituição Federal de 1988.

A interpretação do novo dispositivo constitucional deve se dar, portanto, de forma independente do conceito de privacidade:

> A dinâmica de proteção dos dados pessoais foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade. Propugnar que o direito à proteção dos dados pessoais seria uma mera evolução do direito à privacidade é construção dogmática falha que dificulta a sua compreensão"[10].

---

[8] MENDES, Laura Schertel. *Habeas Data* e Autodeterminação Informativa: os dois lados da mesma moeda em **Direitos Fundamentais & Justiça**, Porto Alegre: n 39, 2018. p. 188.
[9] MENDES, Laura Schertel; FONSECA, Gabriel. STF reconhece Direito Fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393 *in* **Revista do Direito do Consumidor**, São Paulo: vol 130, 2020.
[10] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. GenForense: Rio de Janeiro, 2021, p. 95.

Dessa forma, tem-se, de um lado, a privacidade como **liberdade negativa**, ou seja, o direito do indivíduo de não sofrer interferência em sua esfera de intimidade; de outro, o direito à proteção de dados, cuja definição pode ser extraída do conceito de autodeterminação informativa, apresentado agora como direito fundamental autônomo e que compreende o fluxo de informações e estabelece seus limites, sendo, deste modo, uma **liberdade positiva**, de viés coletivo.

Para o presente parecer, o enfoque será no viés coletivo, na medida em que as demais peças processuais apresentadas já abordam a questão da privacidade e dos direitos individuais envolvidos. De resto, o direito à proteção de dados é positivação ocorrida posteriormente à formulação das teses. E, por fim, porque o IBCCRIM entende que o cerne do debate está na possibilidade de avançar o poder de investigação estatal de forma coletiva, não individualizada.

V. DA QUEBRA DE SIGILO DE DADOS DE UM NÚMERO INDETERMINADO DE PESSOAS

Para a compreensão do problema em sua forma coletiva, é preciso estabelecer algumas premissas a respeito da compreensão que deve se dar à utilização dos dados pessoais em Direito Penal, mesmo em casos individualizados. Fala-se em premissas no sentido de serem questões já reconhecidas nas demais peças processuais e pela jurisprudência desse Supremo Tribunal Federal.

(a.) Premissas: adoção, para fins criminais, do conceito de dados pessoais em sua vertente expansionista e superação do entendimento de que a proteção à privacidade é do fluxo comunicacional, não se aplicando a dados "registrais".

Há, atualmente, uma definição quase intuitiva de dado e que diz respeito ao próprio conceito de informação. Por dado, pode-se entender "fatos conhecidos

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

que podem ser registrados e possuem significado implícito"[11]. Dentre estes, é preciso identificar quais são os "dados pessoais", de forma a delimitar a abrangência do direito fundamental à proteção de dados.

Há duas principais concepções a respeito do conceito de dado pessoal: a reducionista e a expansionista. Ambas se diferem pela maneira com que uma pessoa natural pode ser relacionada com um dado. Para a corrente reducionista, dado, para ser considerado pessoal, deve ser diretamente relacionado a uma pessoa natural; já para a expansionista, deve estar presente a possibilidade de que o dado identifique uma pessoa natural. Em outras palavras, para a primeira corrente, um dado pessoal é aquele que se refere a uma pessoa identificada, enquanto, para a segunda, o dado é pessoal quando se refere a uma pessoa identificável. Nessa última hipótese, quando de um dado aparentemente anônimo se possa identificar a pessoa com a qual ele está relacionado, ele se enquadra no conceito. Assim, "há um vocabulário que, respectivamente, alarga (pessoa identificável) ou restringe (pessoa identificada) o escopo de uma lei de proteção de dados pessoais"[12].

Para uma melhor compreensão, na concepção reducionista, dado pessoal é aquele que vincula a informação à pessoa de maneira imediata e direita, como o CPF de alguém. Já em uma conceituação expansionista, o dado é pessoal quando identificável a uma pessoa natural. O vínculo entre as duas informações, portanto, pode se dar de maneira indireta, como é o caso dos registros de conexão. Assim:

> [a] expansionista aposta em uma lógica mais flexível, que desconsidera a associação exata entre uma informação e uma pessoa. Dado pessoal pode ser qualquer tipo de informação que permita a sua identificação, ainda que o vínculo entre o dado e um indivíduo não seja estabelecido de prontidão, mas de forma mediata ou indireta. Um dado para ser pessoal deve ser, portanto, a projeção de uma pessoa identificável[13].

Dessa forma, o conceito é expandido através de uma noção diversa da correlação direta, mas acerca da possibilidade de esse dado identificar alguém

[11] ELMASRI, Ramez; NAVATHE, Sham. **Sistemas de banco de dados**. São Paulo: Pearson Addison Wesley, 2011, p. 3.
[12] BIONI, Bruno Ricardo. **Xeque-Mate**: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação(GPoPAI-USP), 2016, p. 4.
[13] *Idem*, p. 17.

(por isso o uso do vocábulo **identificável**). A definição faz sentido no contexto das novas tecnologias de processamento de dados e de inteligência artificial, as quais tornam cada vez mais difícil o processo de anonimização de um dado. Em realidade, com o atual estágio tecnológico, a criação da antinomia do dado pessoal, isto é, o dado anônimo, se torna tão difícil que já é considerada como impossível[14].

Colocando as duas concepções em paralelo, percebe-se que o conceito reducionista entende que um dado **anônimo** seria aquele que não tem relação direta com uma pessoa natural, ao passo que o expansionista leva em consideração a ideia de que aquele dado, aparentemente anônimo, pode ser vinculado a uma pessoa por meio de processos de reversão.

Por conta da grande disponibilidade de técnicas que transformam um dado aparentemente anônimo em outro que consegue identificar uma pessoa natural, é que decisões[15] e legislações[16] atinentes à proteção de dados têm adotado um conceito expansionista. Da mesma forma, a legislação brasileira encampou uma conceituação expansionista para dado pessoal, como evidencia o art. 5º da LGPD:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Também o Marco Civil da Internet, cuja aplicação ao Direito Penal é

[14] *Idem*.
[15] Para os fins desse artigo, é de se mencionar a decisão da Corte Europeia de Justiça no caso *Patrick Breyer v. Bundesrepublik Deutschland* (2016).
[16] A General Data Protection Regulation (GDPR), legislação europeia de proteção de dados define o dado pessoal, em seu art. 4(1): "'*personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*".

pacífica, em seu decreto regulamentador, Decreto nº 8.771, conceitua o termo de forma expansiva:

> Art. 14. Para os fins do disposto neste Decreto, considera-se:
> I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e II - – tratamento de dados pessoais - – toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O conceito expansivo de dado pessoal já foi assentado pelo Supremo Tribunal Federal no julgamento do Caso IBGE, conforme se lê na própria ementa do acórdão:

> Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.

No entanto, a despeito de tudo isso, em matéria penal, a jurisprudência dominante segue apegada ao conceito de "dado registral", entendimento firmado a partir do clássico texto de Tércio Sampaio Ferraz Júnior, "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do estado" (o próprio autor pugna, nesses autos e em outras oportunidades, pela superação dos precedentes originários desse texto):

> O entendimento doutrinário até hoje predominante, que também encontra eco em decisão do Supremo Tribunal Federal, 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. Esse entendimento exclui, portanto, do âmbito de proteção do dispositivo não somente o conteúdo de comunicações armazenadas, registradas ou gravadas como também as informações geradas a respeito das circunstâncias nas quais as

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

> comunicações ocorreram (metadados). Em razão dessa limitação, diversos autores têm argumentado em favor de novas interpretações desse dispositivo, no sentido de levar em conta os avanços da tecnologia e as enormes quantidades de conteúdos e registros de comunicações que passaram a ser armazenadas em dispositivos pessoais, como computadores e aparelhos celulares. Diante disso, as disputas interpretativas a respeito da extensão dessa garantia constitucional reacenderam, tal como exploraremos abaixo[17].

Ao não utilizar o conceito de dado pessoal para fins criminais, mas de dados registrais, a jurisprudência pátria limita a aplicação do direito fundamental à privacidade, não alcançando o direito fundamental inserido pela EC 115/2022:

> Assim, o limite das decisões judiciais na matéria parece ser o da proteção do fluxo de comunicações, sendo os dados classificados como 'registros'. É justamente ao não incorporar o conceito de dado pessoal, mas de dados registrais, que a proteção constitucional apenas do fluxo de comunicações é possível, pois, ao assumir o conceito de 'dado pessoal', uma série de outras proteções são acionadas[18].

Assim, o reconhecimento de um direito fundamental à proteção de dados e da autodeterminação informativa, bem como a compreensão de que não existem mais dados irrelevantes, leva necessariamente à superação do entendimento anteriormente firmado, o que já vem sido percebido nas decisões desse Tribunal.

No julgamento do ARE 1.042.075, o Min. Gilmar Mendes abriu divergência para defender a tese de que o acesso a registro telefônico de celulares apreendidos com acusados depende de prévia decisão judicial, equiparando a proteção constitucional da inviolabilidade dos dados às das comunicações. O mesmo se verifica na decisão do *HC* 168.052[19]:

> *Habeas corpus*. (...) 2. Acesso a aparelho celular por policiais sem autorização judicial. Verificação de conversas em aplicativo WhatsApp. Sigilo das comunicações e da proteção de dados. Direito fundamental à intimidade e à vida privada. Superação da jurisprudência firmada no *HC* 91.867/PA. Relevante modi-

[17] ABREU, Jacqueline de Souza, ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil**: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2ª ed., 2017, p. 16.
[18] FERREIRA, André da Rocha. Tratamento de dados pessoais em investigações criminais: o direito fundamental à autotedeterminação informativa como limite constitucional *in* **Revista Brasileira de Ciências Criminais**, ano 29, v. 185, 2021, p. 124.
[19] STF, HC 168.052, 2ª T., rel. Min. Gilmar Mendes, j. 20.10.2020.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

> ficação das circunstâncias fáticas e jurídicas. Mutação constitucional. Necessidade de autorização judicial. 3. Violação ao domicílio do réu após apreensão ilegal do celular. 4. Alegação de fornecimento voluntário do acesso ao aparelho telefônico. 5. Necessidade de se estabelecer garantias para a efetivação do direito à não autoincriminação. 6. Ordem concedida para declarar a ilicitude das provas ilícitas e de todas dela derivadas. (HC 168052; Órgão julgador: Segunda Turma; Relator(a): Min. GILMAR MENDES; Julgamento: 20.10.2020; Publicação: 02.12.2020). Grifamos.

Em seu voto, o Relator aponta:

> No julgamento do *HC 91.867/PA* (Segunda Turma, de minha relatoria, DJe 20.9.2012), destaquei a diferença entre *comunicação telefônica* e *registros telefônicos*, os quais receberiam proteção jurídica distinta. Naquela oportunidade, defendi a impossibilidade de interpretar-se a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral, porquanto a proteção constitucional seria da comunicação, e não dos dados. Creio, contudo, que a *modificação das circunstâncias fáticas e jurídicas*, a promulgação de *leis posteriores* e o significativo *desenvolvimento das tecnologias da comunicação, do tráfego de dados e dos aparelhos smartphones* leva, nos dias atuais, à solução distinta. Ou seja, penso que se está diante de típico caso de *mutação constitucional*

Desse modo, caso seja necessária a utilização de dados pessoais em investigações criminais, a autodeterminação informativa serve como limite, tal qual o direito à privacidade protege a inviolabilidade das comunicações, seguindo o voto do *HC* 168.052:

> No âmbito infraconstitucional, as normas do art. 3º, II, III; 7º, I, II, III, VII; 10 e 11 da Lei 12.965/2014 – o marco civil da internet – estabelecem diversas proteções à privacidade, aos dados pessoais, à vida privada, ao fluxo de comunicações e às comunicações privadas dos usuários da internet. A norma do art. 7º, III, da referida lei é elucidativa ao prever a inviolabilidade e sigilo das comunicações privadas armazenadas (dados armazenados), salvo por ordem judicial. Percebe-se, portanto, que a legislação infraconstitucional avançou para possibilitar a proteção dos dados armazenados em comunicações privadas, os quais só podem ser acessados mediante prévia decisão judicial – matéria submetida à reserva de jurisdição. Entendo que o avanço normativo nesse importante tema da proteção do direito à intimidade e à vida privada deve ser considerado na interpretação do alcance das normas do art. 5º, X e XII, CF.

Dessas premissas, algumas conclusões já podem ser extraídas para fixação de tese constitucional ao presente caso: (i) para fins do Direito Penal, a

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

jurisprudência deve adotar o conceito de dado pessoal expansionista; (ii) incorporar, para fins criminais, o arcabouço da disciplina de proteção de dados; (iii) é necessária a superação do entendimento de que a proteção ao sigilo das comunicações e à privacidade se estende apenas ao fluxo da comunicação, e não aos dados armazenados, que não mais se sustenta no ambiente de proteção a dados pessoais, com estatura constitucional.

Esses parâmetros, por certo, devem ser aplicados a casos em que há quebra do sigilo de dados pessoais de forma individualizada. E, com o estabelecimento dessas premissas, é possível conferir resposta mais objetiva ao quesito proposto: o ordenamento jurídico brasileiro, por meio de uma leitura do direito fundamental à proteção de dados, admite a violação de sigilo, para fins de investigação criminal, de um sem-número de pessoas?

(b) Da autodeterminação informativa e seu caráter de direito fundamental coletivo e difuso.

Com a positivação do direito fundamental à proteção dos dados (art. 5º, LXXIX, CF), bem como da decisão no Caso IBGE, a autodeterminação informativa assume a condição de chave de leitura para o presente caso. A autodeterminação informativa, entendida aqui como a garantia e o poder do indivíduo de determinação com relação à coleta e ao tratamento de seus dados pessoais[20], deve ser interpretada em duas dimensões, a individual e coletiva:

> Não há sobreposição, contudo, entre autodeterminação informativa e proteção de dados, nem privacidade e outros direitos de personalidade. Isso já se dá – mas não exclusivamente – pelo fato de o direito à autodeterminação informativa apresentar uma dupla dimensão individual e coletiva, no sentido de que garantida constitucionalmente não é apenas (embora possa ser, como direito subjetivo individual, o mais importante) a possibilidade de cada um decidir sobre o acesso, uso e difusão dos seus dados pessoais, mas também – e aqui a dimensão metaindividual (coletiva) – se trata de destacar que a autodeterminação informativa constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só

[20] MENDES, Laura Schertel. *Habeas Data* e Autodeterminação Informativa: os dois lados da mesma moeda em **Direitos Fundamentais & Justiça**, Porto Alegre: n 39, 2018. p. 188.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

> (*right to be alone*) (cf. Hornung; Schnabel, 2009, p. 85-86). Dito de outro modo, "a proteção de dados é, enquanto proteção de direitos fundamentais, espinha dorsal de uma democracia liberal" (cf. Spiecker, 2018, p. 55-56)[21].

Assim, além de um âmbito individual, inerente à concepção do direito fundamental à proteção de dados, há também um âmbito de proteção transindividual, de liberdade positiva, essencial para a concretização de uma série de pressupostos constitucionais, de livre comunicação, livre desenvolvimento, entre outros:

> As leis de dados pessoais estão passando por uma transformação estrutural significativa. Inicialmente concebidas a partir de uma moldura liberal clássica de "direitos individuais" – o acesso aos meus dados, a proteção dos meus direitos e a reparação individual por danos –, a guinada dada pela General Data Protection Regulation (GDPR) e por novas legislações como a brasileira e a indiana (ainda em fase de discussão) colocou em evidência a necessidade de pensar a proteção de dados pessoais por uma perspectiva de "direitos coletivos" – a avaliação do impacto à comunidade, a proteção dos nossos direitos fundamentais e a reparação coletiva por violações éticas e aos valores da sociedade (...) A coletivização da proteção de dados pessoais pode ser descrita por quatro elementos básicos. O primeiro é a crescente importância da linguagem dos "direitos difusos" e "direitos coletivos", fazendo com que os casos sejam avaliados por uma perspectiva de violação à sociedade – ou, mais precisamente, a violação aos "valores da sociedade" –, para além de questões privadas que pudessem ser resolvidas por mecanismos de reparação compensatórios. Esse fenômeno foi chamado por Mauro Cappelletti, ainda na década de 1980, de "desprivatização do direito" (CAPPELLETTI, 1985), ou seja, a ideia de que os interesses anteriormente considerados privados sejam considerados como sociais. (...) Esse elemento é claro tanto na GDPR quanto na LGPD com relação ao conjunto de obrigações imposto aos controladores e operadores de dados, que devem documentar suas atividades, realizar avaliações de impacto à proteção de dados pessoais no caso de inovações de alto risco às liberdades e direitos fundamentais e adotar o "princípio da prevenção", que consiste na "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (LGPD, art. 6º, inciso VIII)[22].

Assim, a análise a respeito da permissibilidade da quebra de sigilo de dados pessoais sem individualização deve se dar pela compreensão dos riscos que a medida enseja, principalmente no aspecto da vigilância generalizada. A Min. Rosa Weber, em seu voto no caso IBGE, observou:

---

[21] SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais *in* **Assunto Especial**. RDP, Brasília, Volume 17, n. 93, 58-81, maio/jun. 2020. Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias, p. 49.

[22] ZANATTA, Rafael. **A tutela coletiva na proteção de dados pessoais** *in* Revista dos Advogados de São Paulo, Revista n. 144, nov, 2019, p. 202-203.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

> A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos. Esses direitos são extraídos da interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do *habeas data* (art. 5º, LXXII), todos previstos na Constituição Federal de 1988.
>
> (...)
>
> A força normativa da constituição pode e deve ser atualizada e reconceitualizada para preservar garantias individuais que constituem a base da democracia constitucional e que hoje são diretamente ameaçadas pelo descompasso entre o poder de vigilância e a proteção da intimidade. Embora as novas tecnologias de comunicação tenham se tornado condição necessária para a realização de direitos básicos – como se faz evidente no campo da liberdade de expressão, de manifestação política e de liberdade religiosa – verifica-se que esses mesmos avanços tecnológicos suscitam riscos generalizados de violação de direitos fundamentais básicos, para além da questão comunicacional.

A doutrina autorizada aponta para os mesmos riscos:

> É importante a compreensão do debate que se apresenta; ao fim e ao cabo, estamos falando de limites à persecução penal em grande escala: a quantidade de dados que agências de segurança tratam pode gerar uma situação de vigilância permanente dos cidadãos, bem como expandir os problemas já existentes no sistema de justiça criminal. Tratar dados pessoas de maneira massiva tem relação com a utilização de dados pessoais para categorizar indivíduos (*profiling*) ou determinados grupos (*grouping*). Tem estrita relação com a tomada de decisões por sistema automatizados e oferecem uma aparência de neutralidade, mas que já demonstrou tomar decisões discriminatórias e potencialmente perigosas para os sistemas democráticos. Rapidamente, podemos elencar alguns usos de dados pessoais no sistema de justiça criminal: interceptação ou requisição de dados para investigações criminais; polícia preditiva (*big data policing*); utilização de novas tecnologias de vigilância (como reconhecimento facial); gerenciamento de decisões no sistema de justiça criminal (decisões do Poder Judiciário tomadas por algoritmos) e, ainda, técnicas de *data mining* em situações de *dragnet policing*, ou seja: quando há um tratamento de dados pessoais de um sem número de pessoas para buscar a autoria de determinado delito. *Dragnet policing* são ações coordenadas da polícia para a captura de suspeitos (por exemplo, barricadas em estradas), os quais já atingem também meios tecnológicos, como é, justamente, o caso de Marielle Franco: obtenção de uma série de dados pessoais, de um sem-número de cidadãos, a fim de tentar individualizar uma conduta.
>
> Em se tratando de gestão da segurança pública, o registro e o tratamento indiscriminado de informações atingem uma dimensão individual, na

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

> reprodução massiva e automatizada de padrões que, diga-se, já existiam no direito penal (como, por exemplo, de seletividade). Assume, também, uma dimensão coletiva a partir da ideia de uma vigilância constante, perigoso fenômeno que só é possível a partir do uso de novas tecnologias computacionais[23].

Os riscos podem ser mensurados a partir de estudos criminológicos sobre o tema e até mesmo na literatura relativa à disciplina de proteção de dados e privacidade, a qual já indica que há um alto risco de abuso e excessos envolvidos.

A bem da verdade, o que se discute é um permissivo jurisdicional para que, em sabendo da existência de um fato supostamente criminoso, as agências de segurança possam investigar, através da obtenção de dados pessoais, um sem-número de pessoas. Tudo isso por meio de critérios investigativos a serem criados e posteriormente submetidos ao crivo do Poder Judiciário. Importante salientar que não se está advogando por uma individualização direta dos indivíduos a serem investigados, pois, de fato, a obtenção de dados pessoais pode auxiliar na identificação de autores de práticas delituosas graves. Assim, mesmo uma quebra de sigilo coletiva é possível, desde que haja uma limitação do alcance e estejam comprovadas a efetividade e a necessidade da quebra.

Recentemente, por exemplo, nos autos do Inq. 4879, diante da perpetuação de ataques terroristas contra a Democracia e as instituições do Estado brasileiro, pela invasão e depredação das sedes dos Três Poderes da República em 08.01.2023, o Min. Alexandre de Moraes determinou a guarda, por empresas de telecomunicação, de informações de geolocalização de aparelhos telefônicos de usuários que estivessem na imediação da Praça dos Três Poderes e do Quartel-General de Brasília, na data e horário em que os fatos ocorreram. Ainda que não haja uma individualização específica dos responsáveis, a obtenção desses dados pode auxiliar na identificação dos autores desse grave atentado, havendo uma limitação territorial e temporal para a extensão da medida.

A permissão, sem embargo, para que agências de segurança, notadamente a polícia judiciária, tratem dados de um sem-número de pessoas,

[23] FERREIRA, André da Rocha. Tratamento de dados pessoais em investigações criminais: o direito fundamental à autotedeterminação informativa como limite constitucional *in* **Revista Brasileira de Ciências Criminais**, ano 29, v. 185, 2021, p. 137.

sem uma individualização dos fundamentos para tanto, fere o conteúdo do direito à proteção de dados. Isso porque o núcleo do direito fundamental tem relação com o controle que os cidadãos têm do fluxo de seus dados:

> A tutela jurídica dos dados pessoais é um imperativo que impõe uma nova fronteira aos direitos de personalidade, a fim de que o fluxo informacional não seja corrosivo à esfera relacional da pessoa humana e, por tabela, ao livre desenvolvimento de sua personalidade. Por isso, o direito à proteção de dados pessoais reclama uma normatização própria que não pode ser reduzida a uma mera 'evolução' do direito à privacidade, mas encarada como um novo direito da personalidade que percorre, dentre outras liberdades e garantias fundamentais, a liberdade de expressão, de acesso à informação e de não discriminação. Em última análise, trata-se da nossa própria capacidade de autodeterminação.[24]

Dessa maneira colocada, a perspectiva de que os indivíduos possam ter seus dados pessoais tratados em investigações criminais pelo simples fato de terem realizado uma pesquisa na *internet*, ou cruzado por um local em determinado momento, ou seja, desenvolvendo suas personalidades livremente pelo uso da internet, fere o texto constitucional.

Ademais, uma medida que atinja uma coletividade de pessoas estende os limites do direito penal, cuja intervenção se dá por meio de indícios de que determinada pessoa haja cometido um crime, sendo ilegal o prosseguimento de investigações que não seguem essa regra. Assim, a mera ocorrência de um fato delituoso não pode justificar que qualquer pessoa seja escrutinada a partir de suas atividades cotidianas (pesquisas na internet, localização de celular, sites que acessou).

Esse cenário cria a possibilidade, ainda que virtual, de que as agências de segurança investiguem e classifiquem os hábitos de qualquer pessoa, típico de estados autoritários. No presente caso, por exemplo, os dados pessoais e as pesquisas relacionadas podem ser utilizados para classificações de fins políticos. Desse modo, ainda mais grave a situação em que a possibilidade de que milhares de dados pessoais sejam tratados de uma só vez para a investigação de um determinado fato criminoso, sem sequer haver uma legislação específica, estabelecendo-se um novo paradigma para a maneira como se entende o direito

[24] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. GenForense: Rio de Janeiro, 2021, p. 89-90.

penal. Lembra-se, ainda, que se trata de novas tecnologias, cuja utilização para fins criminais, e os riscos associados, estão em processo de compreensão, demandando, assim, debates e legislações específicas. A mera analogia com outras leis existentes, como a Lei de Interceptações Telefônicas, não parece, por essa razão, o caminho adequado a se tomar.

Em análise de tema similar, a saber, a possibilidade de infiltração virtual no aparelho celular de um suspeito de um crime (em outras palavras, o "hackeamento" do dispositivo para monitoramento constante das atividades de um suspeito de crime), Greco e Gleizer concluem pela impossibilidade de fazê-lo, ainda mais sem que haja regulamento específico a respeito da matéria:

> Em síntese, podemos dizer que a infiltração online, como meio processual-penal de obtenção oculta e remota de provas armazenadas em sistemas informáticos é uma medida cada vez mais atraente na era da digitalização, em que informações necessárias ao processo estão, muitas vezes, apenas registradas em formato de dígitos 0-1, e não mais em papéis apreensíveis por meio de medidas convencionais, como a busca e apreensão. Em ordenamentos jurídicos que conhecem direitos fundamentais, ela é, no entanto, certamente uma intervenção. Em qual(is) direito(s) fundamental(is) ela intervém é a primeira pergunta a ser respondida. A resposta a essa pergunta pode nos levar, como na experiência alemã, a reconhecer a necessidade de um específico direito fundamental que proteja os indivíduos dos riscos que a vida cercada de dispositivos informáticos pode lhes criar. A concretização de um direito à integridade e confiabilidade no uso de dispositivos informáticos parece ser uma boa resposta, dada pelo BVerfG, ao problema: um direito que proteja não apenas contra invasões à privacidade, mas também contra manipulações em sistemas informáticos privados, de modo que os indivíduos possam confiar em seu uso e, assim, desenvolver livremente suas personalidades na era da digitalização.
>
> Um direito fundamental à integridade e confiabilidade no uso de sistemas informáticos deve criar altos obstáculos interventivos, tendo em vista as sérias consequências que uma intervenção pode criar para a vida dos indivíduos que tenham seus sistemas informáticos acessados por terceiros, especialmente agentes estatais. Esses pressupostos estão sendo discutidos há algum tempo pela ciência e pelos tribunais alemães e podem servir de parâmetro para a elaboração de uma norma autorizativa ainda inexistente no direito brasileiro. Na ausência de norma autorizativa para a infiltração online no ordenamento jurídico brasileiro, a ilegitimidade da medida é evidente. O Estado só pode atuar nos limites das autorizações do povo, conferidas por seus representantes no parlamento.
>
> Como essa autorização inexiste no Brasil, é vedado às instâncias de persecução infiltrar-se em computadores de forma oculta. No Brasil, o acesso ao conteúdo de

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

> sistemas informáticos tem de fazer uso da busca e da apreensão do dispositivo físico em que esse conteúdo se encontra armazenado[25].

Trata-se de situação correlata à do presente parecer. Ao buscar o fundamento que autoriza o compartilhamento de dados pessoais sem individualização em legislações correlatas, há um desrespeito aos princípios do direito penal, notadamente do direito penal mínimo e da *ultima ratio* e dos princípios de proteção de dados e da privacidade.

A ausência de uma legislação específica faz com que haja um risco ainda maior de desrespeito a direitos individuais e coletivos. O que deve ser feito, por exemplo, quando os dados pessoais foram de titularidade de crianças ou adolescentes? Ou, ainda, quando houver o encontro fortuito de provas de outros delitos? Enfim, são múltiplas as possibilidades, cuja adequação não parece ser possível em uma decisão judicial, ainda mais com a empírica relativização jurisprudencial do dever de fundamentação contido no art. 93, IX, da Constituição Federal.

Finalmente, há um problema material: as agências de segurança, principalmente por ausência de determinação legal, não contam com políticas de respeito aos princípios de proteção de dados. A história autoritária do Direito Penal brasileiro não parece indicar que determinações judiciais, por si só, garantam que haja respeito ao modo com que os dados devem ser tratados em havendo uma disseminação da prática, a qual já aparece em algumas decisões:

> AGRAVO REGIMENTAL NO RECURSO EM MANDADO DE SEGURANÇA. QUEBRA DE SIGILO DE DADOS ESTÁTICOS. SERVIÇO DE GEOLOCALIZAÇÃO. MARCO CIVIL DA INTERNET NÃO VIOLADO. POSSIBILIDADE. PRECEDENTES DESTE STJ. CASO CONCRETO. EXTRAPOLAÇÃO DA DECISÃO DE QUEBRA DE SIGILO EM FACE DE NÚMERO INDETERMINADO DE PESSOAS. PRINCÍPIO DA PROPORCIONALIDADE NÃO OBSERVADO IN CASU. NECESSIDADE DE REFORMA DA DECISÃO. RECURSO DE AGRAVO REGIMENTAL CONHECIDO E PARCIALMENTE PROVIDO. CONCESSÃO PARCIAL DA SEGURANÇA. (...) II - De acordo com o entendimento consolidado no col. Supremo Tribunal Federal, "os direitos e garantias individuais não tem caráter absoluto. Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das

[25] GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal — Notícia sobre a experiência alemã *in* **Rev. Bras. de Direito Processual Penal**, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set.-dez. 2019, p. 1551-1512.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição" (MS n. 23.452/RJ, Segunda Turma, Rel. Min. Celso de Mello, DJe de 12/5/2000). III - Na hipótese vertente, observa-se que a determinação judicial rechaçada, em parte, se referiu a dados estáticos antes coletados (registros de geolocalização), relacionados à identificação de usuários que operaram em área delimitada e por intervalo de tempo indicado. Tal situação configura apenas quebra de sigilo de dados informáticos estáticos e se distingue das interceptações das comunicações dinâmicas em si, as quais dariam acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. IV - O tema já foi enfrentado por esta Corte Superior, vejamos: "Na espécie, a ordem judicial direcionou-se a dados estáticos (registros), relacionados à identificação de usuários em determinada localização geográfica que, de alguma forma, possam ter algum ponto em comum com os fatos objeto de investigação por crimes de homicídio.(...) A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, (...) A quebra do sigilo de dados, na hipótese, corresponde à obtenção de registros informáticos existentes ou dados já coletados (...) Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros (...) Logo, a quebra do sigilo de dados armazenados, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas (...)" (RMS n. 62.143/RJ, Sexta Turma, Rel. Min. Rogério Schietti Cruz, DJe de 8/9/2020). V - Convém registrar que a quebra de sigilo em tela foi decretada por decisão judicial devidamente fundamentada, após pedido expresso da autoridade competente, no seio de investigação formal, tendo, como referência, fatos concretos relacionados ao suposto cometimento de crime grave. VI - Na situação exposta, a r. decisão de origem foi clara ao delimitar tempo e espaço, nos seguintes termos: "a quebra de sigilo de dados telemáticos dos usuários que tenham utilizado os serviços da empresa G B I L e G LLC num raio de 500 metros das coordenadas geográficas Latitude 21 o 35 ´42.6 ´S e Longitude 41 o. 28 ´36.9 ´ ´W no período abrangido entre 10:00hs e 14:00hs do dia 09/05/2020 (...)" (fl. 112). VII - Contudo, a r. decisão acima extrapolou os limites do entendimento firmado por esta Corte Superior, ao determinar o acesso amplo e irrestrito aos seguintes dados, verbis:"1) que seja dado acesso amplo e irrestrito dos e-mails vinculados aos aparelhos identificados. 2) Que seja fornecido o conteúdo do G. 3) Que seja fornecido o conteúdo do G fotos (incluindo os respectivos metadados - geomarcação). 4) Que seja fornecido o conteúdo do G D. 5) Que seja fornecida a lista de contatos. 6) Que seja fornecido o histórico de localização, incluindo os trajetos pesquisados no g m, w ou outros que importem a função GPS. 7) Que

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

> sejam fornecidas as consultas (pesquisas) realizados pelo usuário (s) do dispositivo. 8) Por fim, que sejam relacionadas as contas do G P, incluindo APPs baixados (downloads) ou comprados, lista de desejos, pessoas e informações das eventuais contas" (fl. 112). VIII - Trata-se de matéria recentemente enfrentada pela Sexta Turma desta Corte Superior, em julgado no qual foi assentada a tese de que dados que refletem informações íntimas (como o acesso irrestrito a fotos e conteúdo de conversas), quando a ordem de quebra de sigilo se voltar a universo indeterminado de pessoas, devem ser afastados desta possibilidade (AgRg no RMS 59.716/RS, Sexta Turma, Rel. Min. Sebastião Reis Júnior, DJe de 17/8/2021). IX - Importante, contudo, sedimentar que a ordem *in casu* foi dirigida a provedor cuja relação é regida pelo Marco Civil da Internet, o qual não prevê, dentre os requisitos que estabelece para a quebra de sigilo, que a decisão judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada facilmente por outros meios (arts. 22 e 23 da Lei n. 12.965/2014). Entretanto, o referido fundamento não subsiste nos casos em que haja a possibilidade de violação da intimidade e vida privada de pessoas não comprovadamente relacionadas à investigação criminal (AgRg no RMS 59.716/RS, Sexta Turma, Rel. Min. Sebastião Reis Júnior, DJe de 17/8/2021). Agravo regimental conhecido e parcialmente provido para reconsiderar a decisão monocrática anterior. Segurança concedida em parte para determinar a limitação da quebra de sigilo de dados aos IPS e Device IPs dos eventuais usuários que ingressaram na área e momento delimitados à fl. 112.
> (AgRg no RMS n. 68.119/RJ, relator Ministro Jesuíno Rissato [Desembargador Convocado do TJDFT], Quinta Turma, julgado em 15/3/2022, DJe de 28/3/2022.)

Decisões semelhantes foram proferidos nos RMS 64.941/RJ e no RMS 68.119/RJ. Em Cortes Estaduais, semelhante fenômeno é visto em decisões, como, por exemplo:

> 1-) Mandado de segurança para não haver quebra do sigilo telemático coletivo e exploratório sobre dados de geolocalização de um conjunto indeterminado de usuários da Google. Não concessão. 2-) Decisão que não é sucinta, mas, mesmo que o fosse, está suficientemente fundamentada. Nulidade, com afronta do art. 93, inciso IX, da Constituição Federal inexistente. 3-) Os requisitos constitucionais fazem-se presentes. Não há violação de direito à intimidade, vida privada, honra, imagem ou direito de comunicação. Esses direitos são fundamentais, todavia, não são absolutos, cedem ao interesse público, mesmo porque, basta deixar tudo em sigilo. 4-) Os requisitos legais, especificamente, da Lei no 12.965/2014 não foram desprezados: existem fundados indícios da ocorrência do roubo; há justificativa motivada da utilização dos registros solicitados para investigação e há período ao qual se referem os registros. **Não há necessidade de se especificar quem será investigado ou ser a diligência a única possível para as investigações**. 5-) Decisão de Primeiro Grau mantida. (TSJP, MS 2145603-41.2021.8.26.0000, 11ª Câmara de Direito Criminal, Rel. Des. Tetsuzo Namba, j. 4.8.21, destaque acrescido.)

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

Veja-se, desse modo, que o alerta inicial desse parecer já começa a se desenhar: a utilização da quebra do sigilo de dados pessoais de um sem-número de pessoas como prática investigativa corriqueira, expandindo o direito penal e a vigilância. Por essa razão, uma análise exclusiva do caso concreto não dá conta de perceber os riscos envolvidos na permissibilidade da medida.

Em suma, o que se buscou demonstrar, pela análise da disciplina de proteção de dados aplicada ao Direito Penal, é que a violação do sigilo de informações de um número indeterminado de pessoas apenas pela possibilidade de se identificar a autoria delitiva de um fato supostamente criminoso fere o direito fundamental à proteção de dados, notadamente em seu caráter coletivo, bem como princípios do Direito Penal, destacando-se os da mínima intervenção e da *ultima ratio*.

A situação é ainda mais grave, pois não há regulação específica para a matéria, cujo ineditismo e riscos associados não podem ser comparados com outras medidas de investigação até antes adotadas, como o alcance de uma interceptação telefônica, na medida que tratam de ambientes controlados em torno de indivíduos que são suspeitos do cometimento de um delito.

Sequer o Marco Civil da Internet, à época de sua promulgação, poderia prever que o avanço tecnológico no tratamento de dados pessoais ofereceria tantos riscos. Assim, o simples fato de que o legislador não tenha definido explicitamente que é necessária a individualização da quebra de sigilo dos dados pessoais não autoriza a intervenção em um sem-número de pessoas, na medida em que a legislação é regida pelos princípios da proteção de dados. A interpretação do dispositivo legal que autoriza o franqueamento dos dados pessoais para investigações criminais deve, portanto, se dar a partir de uma ótica protetiva, não de redução de direitos.

A omissão do legislador não pode ser interpretada em desfavor das garantias individuais e coletivas. A quebra de sigilo prevista pelo art. 13 e ss. do Marco Civil da Internet tem muito mais relação com a necessidade dessa técnica investigativa para o descobrimento da autoria de crimes cometidos no ambiente virtual do que o uso indiscriminado em todos os tipos de delitos. Por exemplo,

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

quando determinada pessoa invade dispositivo informático, alguns rastros podem levar à identificação do autor do delito, como o próprio IP. Nesse caso, a agência de segurança, de posse do dado pessoal, identifica a pessoa natural a ele correspondente. Desse modo, não está contida, na intenção do legislador, a ideia de que a quebra do sigilo de dados pessoais representasse uma ameaça ao próprio uso da internet, na medida em que o objetivo da lei é, precisamente, garantir a liberdade de expressão, o livre desenvolvimento do indivíduo e garantir a presunção de inocência, conforme se lê da própria exposição de motivos do Projeto de Lei que originou a legislação:

> No terceiro capítulo, ao tratar da provisão de conexão e de aplicações de internet, o anteprojeto versa sobre as questões como: o tráfego de dados, a guarda de registros de conexão à Internet, a guarda de registro de acesso a aplicações na rede, a responsabilidade por danos decorrentes de conteúdo gerado por terceiros e a requisição judicial de registros. As opções adotadas privilegiam a responsabilização subjetiva, como forma de preservar as conquistas para a liberdade de expressão decorrentes da chamada Web 2.0, que se caracteriza pela ampla liberdade de produção de conteúdo pelos próprios usuários, sem a necessidade de aprovação prévia pelos intermediários. A norma mira os usos legítimos, protegendo a privacidade dos usuários e a liberdade de expressão, adotando como pressuposto o princípio da presunção de inocência, tratando os abusos como eventos excepcionais.[26]

Nesse trecho, percebe-se que o legislador optou por respeitar os direitos individuais e reafirmar princípios básicos do direito penal: responsabilização subjetiva e presunção de inocência, afastando-se, de pronto, a possibilidade de uma quebra coletiva sem individualização própria de dados. A individualização da autoria, mesmo que de forma indiciária, faz parte do próprio conceito de delito, não podendo estar afastada da decisão judicial que autoriza a quebra do sigilo de dados pessoais.

O presente parecer teve como enfoque a questão da coletividade da decisão, na medida em que apresenta um maior risco a uma expansão autoritária do direito penal. No entanto, é de se dizer que não apenas a medida carece de legalidade na possibilidade da quebra coletiva sem individualização de um sem-

[26] Exposição de motivos do Marco Civil da Internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=912989. Último acesso em 3.5.23.

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

número de cidadãos, conforme já demonstrado, mas também no que diz respeito aos dados que são requeridos pela autoridade investigante.

Nas premissas do presente parecer, pugnou-se pela adoção do conceito de dado pessoal na jurisprudência criminal. Incorporar tal categoria atrai o escopo de proteção da disciplina da proteção de dados para dentro do direito penal (conforme já determina a LGPD e já explicado anteriormente). Dentro da concepção de dados pessoais, contudo, existem diversas classificações (por exemplo, alguns dados são considerados sensíveis, outros públicos, enfim, diversas categorizações). Para o presente caso, é importante destacar que a medida carece, também, de ausência de previsão legal para os dados que estão sendo requisitados.

Isso porque o Marco Civil da Internet restringe quais os dados pessoais que devem ficar armazenados: por 01 ano, os registros de conexão e, por 06 meses, os registros de acesso a conexão. O MCI faz referência, ainda, a outra categoria de dados pessoais, os dados cadastrais, cuja entrega para autoridades administrativas prescinde de decisão judicial (art. 10º, §3º). No art. 5º do MCI, há expressa menção ao significado de cada termo:

> 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.

Dessa forma, a obrigação de guarda para entrega é para que provedores de conexão guardem os registros de conexão e as aplicações de internet (caso em que se enquadra a Recorrente), ou seja, guarde tão somente os chamados **metadados** (definição na N.R. de nº 3 do presente parecer). Quer dizer que não há previsão de guarda (e, portanto, de entrega para autoridades investigantes) do conteúdo produzido pela navegação dos usuários na internet. Caso contrário, estaria à disposição do Direito Penal brasileiro todo e qualquer conteúdo disponível na Internet sem que haja expressa autorização legal para tanto. Portanto, o pedido carece de legalidade também quando requer seja entregue o conteúdo das

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

pesquisas de internet de usuários, que não podem ser considerados "registros de acesso a aplicações de internet".

Assim, está-se diante de dois desrespeitos ao princípio da reserva legal: o primeiro no tocante à possibilidade de haver a quebra coletiva e não individualizada do sigilo de dados pessoais dos usuários e o segundo com relação aos próprios dados pessoais requeridos, cuja obtenção não conta com previsão legal específica.

Por fim, é de se ressaltar que o conteúdo requerido é, na sua essência, absolutamente lícito, tratando-se de pesquisas de conteúdo legítimo e que, sem uma devida individualização, não implicam em participação em qualquer atividade criminosa.

Em suma, a medida investigativa permite a seguinte situação: quebra de sigilo coletiva sem individualização (sem-número de cidadãos), com a disponibilidade, por parte das agências investigativas, de todo o conteúdo produzido na internet e sem a necessidade de que o cidadão afetado pela medida tenha cometido qualquer ato ilícito (ou que haja fundamentação apontando para indícios de uma prática ilícita). Com base em todo o exposto, retorna-se à preocupação inicialmente apresentada: em se permitindo a referida medida, há grande risco de uma expansão autoritária do direito penal, além da criação de um estado de vigilância permanente do conteúdo produzido na internet.

Assim, a resposta ao quesito proposto, acerca da possibilidade de quebra do sigilo de dados pessoais de um sem-número de pessoas, é pela impossibilidade constitucional da medida.

VI. CONCLUSÃO

De um modo geral, tentou-se apresentar uma perspectiva a respeito do mérito do presente julgamento que diga respeito aos riscos coletivos que a técnica investigativa pretendia pelo Ministério Público do Rio de Janeiro enseja, notadamente por uma leitura do direito fundamental à proteção de dados de forma autônoma ao da privacidade. Em linhas gerais, esse o caminho traçado e as conclusões que podem ser extraídas:

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

(i) Como premissa, entendeu-se por assinalar que é o momento de a jurisprudência criminal adotar o conceito de dado pessoal, mesmo em casos em que se objetiva à quebra individualizada do sigilo, abandonando-se a noção de dado registral. O conceito de dado pessoal é fornecido pelo Decreto nº 8.771/16 e pela Lei Geral de Proteção de Dados. Com isso, necessário também que haja a superação do entendimento de que a proteção constitucional da intimidade e da privacidade é relativa ao fluxo de informações e não à informação em si também para todos os casos que envolvam a matéria penal e dados pessoais;

(ii) No ordenamento jurídico atual, não há permissão para que as agências de segurança tenham acesso a dados pessoais de um sem-número de indivíduos. Essa ideia esbarra no núcleo do direito fundamental à proteção de dados, na medida em que enseja grave risco de um cenário de vigilância permanente (proporcionalidade em sentido estrito). Também impede que as pessoas tenham controle do fluxo de seus dados pessoais, haja vista que a técnica não seria utilizada relativamente a pessoas que potencialmente tenham cometido alguma ilegalidade, podendo haver tratamento de dados pessoais em decorrência da simples utilização da internet ou pelo simples deslocamento em determinadas coordenadas geográficas. Dessa forma, há risco altíssimo a direitos coletivos difusos, como o livre desenvolvimento da personalidade e a liberdade de expressão;

(iii) O cenário é agravado pela ausência de previsão legal para tanto, sendo possibilitado apenas por uma leitura analógica do Marco Civil da Internet, cujos limites teriam de ser definidos por decisão judicial. Há ainda mais riscos a direitos fundamentais ao ser realizada uma análise material da situação, em que agências de segurança ainda não estão devidamente treinadas e orientadas a tratar dados pessoais de modo a respeitar os princípios da matéria (proteção de dados, guarda de dados etc.);

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

(iv) A aplicação análoga de outras legislações não é possível no presente caso, não apenas por ferir princípios de Direito Penal, mas também porque se trata de situação nova, oriunda de novas tecnologias, as quais possibilitam um alcance jamais imaginado por qualquer outra técnica de investigação.

Esses, em suma, os argumentos do parecer do IBCCRIM.

De São Paulo para Brasília, em 15 de maio de 2023.

renato stanziola vieira
Assinado de forma digital por renato stanziola vieira
Dados: 2023.05.15 12:35:50 -03'00'

Renato Stanziola Vieira

OAB/SP 189.066

DEBORAH MACEDO DUPRAT DE BRITTO PEREIRA
Assinado de forma digital por DEBORAH MACEDO DUPRAT DE BRITTO PEREIRA
Dados: 2023.05.15 10:00:30 -03'00'

Deborah Duprat

OAB/DF 65.698

RAQUEL LIMA SCALCON
Assinado de forma digital por RAQUEL LIMA SCALCON
Dados: 2023.05.15 13:44:56 -03'00'

Raquel Lima Scalcon

OAB/SP 439.421

Paula Nunes Mamede Rosa

OAB/SP 309.696

THEUAN CARVALHO GOMES DA SILVA:39203254862
Assinado de forma digital por THEUAN CARVALHO GOMES DA SILVA:39203254862
Dados: 2023.05.15 09:43:37 -03'00'

Theuan Carvalho Gomes

OAB/SP 343.446

ANDRE DA ROCHA FERREIRA
Assinado de forma digital por ANDRE DA ROCHA FERREIRA
Dados: 2023.05.15 15:51:58 -03'00'

André da Rocha Ferreira

OAB/RS 102.517

POLLYANA DE SANTANA SOARES:35765142877
Assinado de forma digital por POLLYANA DE SANTANA SOARES:35765142877
Dados: 2023.05.15 09:53:07 -03'00'

Pollyana de Santana Soares

OAB/SP 312.413

ANA CAROLINA GONCALVES SOARES
Assinado de forma digital por ANA CAROLINA GONCALVES SOARES
Dados: 2023.05.15 13:57:26 -03'00'

Ana Carolina Soares

OAB/RJ 210.214

LUCAS ASSAYAG BATISTA
Assinado de forma digital por LUCAS ASSAYAG BATISTA
Dados: 2023.05.15 11:58:46 -03'00'

Lucas Assayag Batista

OAB/SP 459.139

João Vicente Tinoco

OAB/RJ 211.245

JOSE EDUARDO RANGEL CURY
Assinado de forma digital por JOSE EDUARDO RANGEL CURY
Dados: 2023.05.15 10:34:23 -03'00'

José Eduardo Rangel Cury

OAB/RJ 230.217

FILIPA DE MARTINS HENRIQUES
Assinado de forma digital por FILIPA DE MARTINS HENRIQUES
Dados: 2023.05.15 14:42:58 -03'00'

Filipa de Martins Henriques

OAB/RJ 218.221

ANDERSON BEZERRA LOPES
Assinado de forma digital por ANDERSON BEZERRA LOPES
Dados: 2023.05.15 14:33:24 -03'00'

Anderson Bezerra Lopes

OAB/SP 274.537

ANDRE VINICIUS OLIVEIRA DA PAZ:36275039884
Assinado de forma digital por ANDRE VINICIUS OLIVEIRA DA PAZ:36275039884
Dados: 2023.05.15 10:19:12 -03'00'

André Vinícius Oliveira da Paz

OAB/SP 461.549

Instituto Brasileiro de Ciências Criminais – IBCCRIM
Rua XI de Agosto, 52 – 1º andar – Centro – São Paulo – SP – CEP 01018-010
Tel.: (11) 3110-4010 – Site: www.ibccrim.org.br

ELIAKIN TATSUO YOKOSAWA PIRES DOS SANTOS

Assinado de forma digital por ELIAKIN TATSUO YOKOSAWA PIRES DOS SANTOS
Dados: 2023.05.15 12:21:38 -03'00'

Eliakin T. Y. Pires dos Santos

OAB/SP 386.266