PARECER

Ferramenta de busca online. Requisição de dados de pesquisa como forma de levantamento de dados pessoais para fins de investigação criminal. Intervenção nos direitos fundamentais à privacidade e à proteção de dados pessoais (autodeterminação informacional). Exigência de fundamento formal e material para a intervenção. Violação da reserva de lei. Ausência de norma autorizativa para a determinação judicial. Violação do princípio da proporcionalidade. Requisição de dados pessoais que atinge quantidade indeterminada de pessoas insuspeitas.

HELOISA ESTELLITA | LUCAS MONTENEGRO | ORLANDINO GLEIZER*

2022

* Lucas Montenegro e Orlandino Gleizer assinam este Parecer na condição de consultores externos em parceria com Estellita Sociedade de Advogados.

SUMÁRIO

A. CONSULTA 1

I. Contextualização fática 1

II. Quesitos 3

B. QUESITO 1: DA AUSÊNCIA DE AUTORIZAÇÃO LEGAL PARA A REQUISIÇÃO DOS DADOS EM EXAME 4

I. O direito de proteção de dados pessoais e a reserva de lei 5

1. O significado do direito de proteção de dados e da reserva de lei no ambiente jurídico alemão 5

2. O desenvolvimento no Brasil e a necessidade de fundamento em lei para medidas de tratamento de dados 9

3. Duas implicações importantes 12

a) Reserva de lei e limites à interpretação analógica 12

b) A distinção entre "dados estáticos" e "dados dinâmicos" 15

II. Ausência de norma autorizativa para a requisição 18

1. O Marco Civil da Internet (Lei n. 12.965/2014, MCI) 19

a) O MCI e as categorias de dados 19

b) O art. 22, MCI 26

c) O art. 10, § 1°, MCI 29

d) Conclusão parcial 31

2. A Lei de Interceptação Telefônica (Lei n. 9.296/96, LIT) 31

a) Do conceito de comunicação 31

b) Da medida autorizada pela LIT: o conceito de interceptação 33

c) Conclusão parcial 34

3. A busca e apreensão (arts. 240 ss., CPP) 34

C. QUESITO 2: PROPORCIONALIDADE DA MEDIDA CONCRETA 38

I. Falta de fundamentação concreta da medida 39

II. Idoneidade: das particularidades do armazenamento de dados da Pesquisa do Google 41

III. Necessidade 44

IV. Proporcionalidade em sentido estrito 46

1. O problema da circunvenção e da vigilância irrestrita 47
2. A predominante afetação de insuspeitos e o efeito inibitório 49
a) O desproporcional alcance da medida 49
b) O efeito inibitório da medida 52

D. RESPOSTA ANALÍTICA AOS QUESITOS 59

Quesito 1: A requisição de dados do Google Busca acima referida está autorizada por lei? 59

Quesito 2: A medida conforma-se aos requisitos constitucionais de proporcionalidade aplicáveis às intervenções em direitos fundamentais? 61

A. CONSULTA

I. Contextualização fática

Google Brasil Internet Ltda. (adiante, Consulente), por intermédio de seus advogados, Dr. Daniel Arbix, Dra. Taís Tesser e Dra. Giovanna Ventre, submete-nos Consulta sobre questões jurídicas debatidas nos autos do Recurso Extraordinário 1.301.250 (adiante, RE), pendente de julgamento no Supremo Tribunal Federal e sob a relatoria da Min. Rosa Weber.

Nos autos do processo n. 072026-61.2018.8.19.0001, do qual se origina a escalada judicial que culmina no RE acima indicado, apura-se a autoria e a materialidade de três homicídios qualificados, dois consumados e um tentado, ocorridos no dia 14 de março de 2018. Cinco meses após o cometimento dos crimes, em 27 de agosto de 2018, o Juízo da 4ª Vara Criminal do Rio de Janeiro-RJ proferiu decisão contendo *mais de 40* determinações de quebra de sigilo de dados telefônicos e telemáticos,[1] dentre as quais uma requisição de compartilhamento de dados pessoais dirigida à Consulente para que fornecesse

> "a identificação dos IP's ou `Device ID's que tenham se utilizado do Google busca (seja através do aplicativo ou sua versão web) no período compreendido entre o dia 10/03/2018 a 14/03/2018, para realizar consultas dos seguintes parâmetros de pesquisa: 'Mariele Franco' [sic}; 'Vereadora Mariele' [sic}; 'Agenda Vereadora Mariele' [sic}; 'Casa das Pretas'; 'Rua dos Inválidos, 122' ou 'Rua dos Inválidos'."

Contra essa decisão,[2] a Consulente impetrou mandado de segurança perante o Tribunal de Justiça do Rio de Janeiro,[3] que foi indeferido. Interposto Recurso em

---

[1] A título exemplificativo, foram deferidas a obtenção de e-mails atrelados a linhas celulares, bem como de dados cadastrais de celulares que tenham mantido contato com outros telefones, de histórico de chamadas, de acesso aos serviços de localização por GPS a critério e pelo período que a autoridade policial determinar, de identificação de todos os usuários de certa rede social que acessaram certas páginas em um período de sete dias etc.

[2] Segundo informou a Consulente, no curso das investigações, foram-lhe dirigidas mais de 40 ordens judiciais de quebra de sigilo de dados de usuários, incluindo dados de comunicação. Em resposta a tais determinações judiciais, a Consulente forneceu dados de aproximadamente 700 usuários.

[3] TJRJ, 1ª Câmara Criminal, Rel. Des. Katia Maria de Paula Menezes Monnerat, MS n. 0072968-96.2018.8.19.0000.

Mandado de Segurança (n. 60.698) no Superior Tribunal de Justiça (adiante, STJ), sua Terceira Seção lhe negou provimento, por maioria de votos, em 26 de agosto de 2020.[4]

Contra a decisão do STJ foi interposto o mencionado RE, cuja repercussão geral foi reconhecida pelo Plenário do Supremo Tribunal Federal em 27 de maio de 2021. Sinteticamente, considerou-se que se trata da "possibilidade da decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas" (p. 11); que a Corte já examinou a questão da proteção de dados pessoais na ADI 6.387 e examinará o tema da proteção de dados e do Marco Civil da Internet (Lei n. 12.965/2014) em dois outros casos: ADPF 403 e ADI 5527 (p. 11-12); que a questão da proteção de dados tem inegável caráter constitucional (p. 12); e que, no ARE 1.042.075, a "Corte reputou constitucional e reconheceu a repercussão geral em tema análogo sobre o sigilo de comunicações telefônicas" (p. 12), em que se discute a possibilidade de a autoridade policial acessar a agenda telefônica e o registro de chamadas de aparelho celular sem autorização judicial.

A Procuradoria Geral da República, em apertada síntese, manifestou-se pelo provimento parcial do recurso "com devolução do processo para reapreciação pelo Tribunal de origem à luz dos parâmetros a serem fixados pelo STF", parâmetros esses que foram sugeridos pela manifestação ministerial (p. 106-107), rogando, ainda, que seja determinada modulação de efeitos, para que o entendimento se aplique apenas aos pedidos de afastamento de sigilo em curso ou futuros (p. 105).

Em que pese o RE discutir outras questões jurídicas, este Parecer analisará exclusivamente aquelas relacionadas à já mencionada requisição de compartilhamento de dados pessoais de usuários que realizaram pesquisas no provedor da Consulente. Essa medida pode ser descrita, genericamente, como uma *requisição de fornecimento de*

[4] O Min. Sebastião Reis Júnior, vencido, entendia haver violação à privacidade "porque tais dados vão permitir não só saber onde eventualmente o usuário esteve em um período de 4 dias, bem como quais foram as buscas que fez na internet no mesmo período" (fl. 439), o que implicaria na necessidade de individualização e de justificativa da medida, pois, da forma como veiculada, "atinge um número não identificado de pessoas sem qualquer justificativa para tanto" (fl. 440).

dados pessoais;[5] enquanto medida de investigação no caso em análise, essa requisição é dotada, contudo, de um aspecto particular: os investigadores não partiram, como é usual, de conteúdos criminosos encontrados na internet, com a finalidade de alcançarem seus autores, senão que adotaram *certos parâmetros* por meio dos quais especulam ser possível obter elementos que auxiliem na identificação de suspeitos envolvidos nos homicídios. Por isso, a medida, com a finalidade de alcançar suspeitos, dirige-se essencialmente contra uma quantidade indeterminada de pessoas insuspeitas.

Por esta razão, a Consulente se vê diante de uma medida inusual. Tal como um braço da investigação estatal, não basta, nesse caso, que colabore para a identificação de pessoas responsáveis pela prática de ilícitos, mas deve, ela própria, realizar *buscas reversas* em seus servidores, a partir de certos parâmetros amplos, e revelar a órgãos da persecução penal dados pessoais de um grupo indeterminado de usuários insuspeitos.

II. Quesitos

Contextualizado o caso e apresentadas suas particularidades, submete-nos a Consulente os seguintes quesitos:

1. A requisição de dados da Pesquisa do Google acima referida está autorizada por lei?
2. A medida conforma-se aos requisitos constitucionais de proporcionalidade aplicáveis às intervenções em direitos fundamentais?

Este Parecer reporta-se exclusivamente aos fatos e às questões jurídicas debatidas no Recurso Extraordinário, bem como aos documentos exibidos e às informações prestadas pelos patronos da Consulente, referidos ao longo do texto. Ele foi elaborado em conformidade com o entendimento imparcial dos subscritores.

[5] Segundo o art. 5º, I, Lei n. 13.709/2018, Lei Geral de Proteção de Dados (LGPD), dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável.

B. QUESITO 1: DA AUSÊNCIA DE AUTORIZAÇÃO LEGAL PARA A REQUISIÇÃO DOS DADOS EM EXAME

Ciente de suas obrigações legais de proteger a intimidade e a vida privada de seus usuários (arts. 7º e 10, Lei n. 12.965/2014, Marco Civil da Internet, doravante MCI), apresentou-nos a Consulente, em primeiro lugar, um quesito simples: o ordenamento jurídico brasileiro autoriza a *requisição de informações* que lhe foi dirigida, enquanto empresa privada prestadora de serviços, no âmbito de uma investigação criminal?

A resposta a essa pergunta, adiantamos, é negativa. Ela é decorrência de princípios básicos da teoria jurídica dos direitos fundamentais e de sua aplicação às normas que autorizam medidas investigativas no processo penal brasileiro, as quais, por sua falta de sistematicidade e precisão, demandam análise mais detida. Poder-se-ia pensar que o fundamento legal para a medida estaria em dispositivos do MCI, ou nos dispositivos que autorizam busca e apreensão (arts. 240 ss., CPP) ou até mesmo em dispositivos da Lei de Interceptações Telefônicas (Lei n. 9.296/96, adiante LIT).

Por isso, a fundamentação da resposta negativa envolve o escrutínio de dois pressupostos: que a requisição em questão consiste em uma intervenção em direitos fundamentais, exigindo assim lei específica e determinada, que se pode chamar de *norma autorizativa*[6] (abaixo I); e que inexiste essa norma em nosso ordenamento jurídico (abaixo II).

[6] Para mais detalhes sobre o conceito de normas autorizativas, em contraposição às normas de competência, cf. GLEIZER, Orlandino. MONTENEGRO, Lucas. VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública*, Marcial Pons, 2021, p. 40 ss., com outras referências.

I. O direito de proteção de dados pessoais e a reserva de lei

1. O significado do direito de proteção de dados e da reserva de lei no ambiente jurídico alemão

Chega a ser lugar-comum, na ainda recente, mas já copiosa literatura jurídica sobre a proteção de dados, a referência à decisão do Tribunal Constitucional Alemão sobre a Lei do Censo Populacional, de 1983 (Volkszählungsurteil, BVerfGE 65, 1).[7] A notoriedade é justificada, pois a decisão de fato lançou as bases para ulterior desenvolvimento que culminaria na atual regulação europeia[8] e na adoção de regimes semelhantes em vários países, inclusive no Brasil, com a Lei n. 13.709/2018 (Lei Geral de Proteção de Dados, adiante LGPD). A grande novidade, sempre referida, foi o reconhecimento pelo Tribunal de um "novo" direito fundamental,[9] o direito fundamental à autodeterminação informacional, conferindo assim proteção constitucional *a todos os dados pessoais*.[10]

Mas a importância da decisão e o seu papel histórico na criação de leis voltadas à proteção de dados só podem ser verdadeiramente compreendidos quando são consideradas as *implicações concretas* do reconhecimento de um direito fundamental, em especial a exigência de *reserva de lei*.[11]

---

[7] Cf. apenas DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: DONEDA, Danilo *et. al.* (Coords.). *Tratado de proteção de dados pessoais.* Forense, 2021; SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados. DONEDA, Danilo *et. al.* (Coords.). *Tratado de proteção de dados pessoais.* Forense, 2021.

[8] Os principais diplomas normativos a nível europeu são hoje o Regulamento 2016/679 (Regulamento Geral de Proteção de Dados) e a Diretiva 2016/680.

[9] Para o Tribunal, o direito à autodeterminação informacional faz parte do regime de proteção da personalidade e seria apenas uma concretização do direito geral ao livre desenvolvimento da personalidade (art. 2, I, GG), cf. BVerfGE 120, 274 (303).

[10] Sobre o desenvolvimento histórico, na literatura alemã, cf. TINNEFELD, Marie-Theres. *et al. Einführung in das Datenschutzrecht.* 7 ed., Oldenbourg, 2020, p. 81 e ss. Para um amplo panorama histórico, RÜPKE, Giselher. LEWINSKI, Kai von. ECKHARDT, Jens. *Datenschutzrecht.* C.H. Beck, 2018, p. 7 e ss.

[11] Sobre a dogmática das intervenções em direitos fundamentais, cf., p. ex., PIEROTH *et. al.* Grundrechte. 36 ed., 2020, Rn. 253 e ss.; HUFEN, Friedhelm. *Staatsrecht*: Grundrecht II. 8 ed. C. H. Beck, 2020, § 8, Rn. 1 e ss. Na literatura brasileira, MENDES, Gilmar Ferreira. BRANCO, Paulo Gustavo. *Curso de direito constitucional.* 13 ed. rev. e atual. Saraiva, 2018,

A Alemanha conhece, desde o século XIX, a exigência de lei parlamentar para intervenções do Estado na liberdade e propriedade dos cidadãos.[12] Com a redemocratização no pós-guerra, a reserva de lei passou a ser reconhecida como um limite incontroverso a restrições de direitos fundamentais (art. 20, III, GG). Noutras palavras, o Tribunal, ao reconhecer o status constitucional dos dados pessoais, não quis simplesmente afirmar um compromisso abstrato com a proteção de dados ou apontar uma direção programática ou de otimização a ser seguida pelo Estado, senão que submeteu *toda intervenção na esfera protegida dos dados pessoais* à proteção que é própria dos direitos fundamentais, o que inclui a reserva de lei. Na decisão acima referida, isso é expressamente ressaltado: "Essas restrições [do direito à autodeterminação informacional] exigem, segundo o art. 2, I GG [...], um *fundamento em lei* (constitucional), do qual resultem, de forma clara e compreensível para o cidadão, os requisitos e a extensão da restrição [...]".[13]

Com isso em mente, não é difícil intuir o que se seguiu a esse reconhecimento e por que a decisão é tão paradigmática. Uma série de atividades do Estado que envolviam tratamento de dados pessoais passaram a necessitar de autorização em lei. Chegou-se a afirmar que a decisão provocou uma verdadeira "enchente de normas",[14] já que toda forma de tratamento de dados pessoais por órgãos estatais demandaria, agora sob a exigência de reserva de lei, fundamento legal determinado e proporcional. Ao mesmo tempo, as bases constitucionais lançadas pelo Tribunal Constitucional passaram a orientar a produção legislativa e os esforços de sistematização do direito de proteção

e-book, p. 284 e ss.; SARLET, Ingo Wolfgang, MARINONI, Luiz Guilherme, MITIDIERO, Daniel. *Curso de direito constitucional*. 8 ed. Saraiva, 2019, *e-book,* p. 542 e ss.

[12] Cf. HUFEN, Friedhelm. *Staatsrecht...*, § 9, nm. 2; GRECO, Luís. GLEIZER, Orlandino. A infiltração online no processo penal. *Revista Brasileira de Direito Processual Penal*, vol. 5, n. 3, p. 1483-1518, 2019, p. 1485 ss. [1486].

[13] BVerfGE 65, 1 (44), itálico nosso. Também em relação ao direito à confiabilidade e integridade de sistemas informáticos (BVerfGE 120, 274, 315): "o indivíduo somente tem de tolerar aquelas restrições de seu direito que tenham fundamento *em lei* constitucional" (itálico nosso).

[14] RÜPKE, LEWINSKI, ECKHARDT, *Datenschutzrecht...*, Rn. 69.

de dados em leis gerais, como se deu em 1990, com a ampla reforma realizada na Lei Federal de Proteção de Dados.

Essa nova orientação inaugurada pelo Tribunal Constitucional Alemão teve consequências também e especialmente para a *persecução penal*.[15] Como as demais intervenções em direitos fundamentais, medidas interventivas próprias do processo penal – entre nós, denominadas em regra de medidas cautelares[16] – também pressupõem autorização em lei, e com mais razão, pois estão dentre as mais graves à disposição do Estado para serem usadas contra seus cidadãos.[17] Obviamente, isso também vale para medidas investigativas que envolvam o tratamento de dados pessoais e, portanto, intervenham no direito à autodeterminação informacional ou em outros direitos mais específicos que protegem dados pessoais (sigilo das telecomunicações, sigilo postal, direito à confiabilidade e integridade de sistemas informáticos etc.).[18] Com o intenso processo de digitalização das últimas décadas, é natural que os órgãos de persecução penal passem a ter no tratamento de dados pessoais uma parte relevante de sua atividade. Ao mesmo tempo, as novas possibilidades de processamento computadorizado de dados fornecem a esses órgãos um enorme poder de acesso e monitoramento dos cidadãos, um potencial invasivo que não encontra paralelo nos métodos tradicionais de investigação.

Por essa razão, outras decisões importantes do Tribunal Constitucional Alemão que hoje dão substância à base constitucional do regime de proteção de dados do país dizem respeito justamente a medidas de processamento de dados empregadas

---

[15] Sobre a problemática, cf. a discussão em WOLTER, Jürgen. Datenschutz und Strafprozess. Zum Verhältnis von Polizeirecht und Strafprozessrecht, *ZStW* 107, pp. 793-842, 1995, p. 793 e ss. (com tradução para o português publicada em WOLTER, Jürgen. O inviolável e o intocável no direito processual penal. Reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Marcial Pons, 2018, p. 159 e ss.).

[16] Crítico quanto ao uso do conceito, GLEIZER, Orlandino. Busca estatal por informações digitais e intervenções em direitos fundamentais no processo penal (parte I). *JOTA*. Coluna Penal em Foco, 31.7.2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/busca-estatal-por-informacoes-digitais-e-intervencoes-em-direitos-fundamentais-no-processo-penal-31072019. Acesso em: 14. fev. 2022.

[17] Cf. GLEIZER, MONTENEGRO, VIANA, *O direito de proteção...*, p. 114 e ss.

[18] Ibid., p. 40 e ss.

em investigações criminais e na segurança pública.[19] A decisão sobre a infiltração online (Online-Durchsuchung), tal qual fizera a decisão do censo, estabelece não só a importância de fundamento legal, mas a exigência de que o próprio Poder Legislativo se encarregue de regular com clareza o tema.[20] Noutras palavras, a essencialidade da matéria *impede* que o Parlamento *delegue* sua regulação a outros poderes e *submete* a produção legislativa a *um estrito mandamento de clareza*.[21] E isso não apenas por questões procedimentais, mas também pela natureza essencialmente política das decisões a respeito do limite legítimo de intervenções estatais na esfera individual. Por isso, reconhece-se que "pelo menos a medida que está sendo autorizada, seus pressupostos autorizadores, suas consequências e seus limites, naquilo que dizem respeito à afetação da esfera dos indivíduos, são decisões a serem tomadas por seu representante [do indivíduo], o legislador".[22] Além disso, em razão das consequências da reserva de lei, o *Bundesgerichtshof* (tribunal alemão equivalente ao nosso Superior Tribunal de Justiça) também rechaça qualquer tentativa de fundamentar medidas combinando elementos de várias normas, pois isto implica violação da ideia de reserva de lei e do mandato de determinação.[23] No processo penal, isso significa que a norma que autoriza medida interventiva de investigação e de cautela tem de especificar com clareza o ensejo, a finalidade e os limites da medida. E, especialmente, que normas não podem ser combinadas, como se fossem uma customização de uma receita de bolo ao gosto do freguês, para autorizar aquilo que não está autorizado por um comando indubitável do legislador. Caso contrário, seria afetada não só a previsibilidade das

[19] BVerfGE 115, 320, Rasterfahndung (cruzamento automatizado de dados empregado na busca de pessoas); BVerfGE 120, 274, Online-Durchsuchung (infiltração online em sistemas informáticos); BVerfGE 125, 260, Vorratsdatenspeicherung (armazenamento indiscriminado de dados por empresas de telecomunicação para fins de persecução penal).

[20] BVerfGE 120, 274 (315 s.).

[21] A teoria da essencialidade (Wesentlichkeitslehre) e o mandamento de determinação (Bestimmtheitsgebot) são aspectos estabelecidos da dogmática de intervenções em direitos fundamentais, cf., p. ex.. PIEROTH *et. al. Grundrechte*..., Rn. 315 e ss., 365; cf. também GRECO, GLEIZER, A infiltração online..., p. 1485 ss. [1486 s.].

[22] GLEIZER, MONTENEGRO, VIANA, *O direito de proteção...*, p. 43 e ss.

[23] BGHSt 51, 211 (219, nm. 22).

intervenções, e, por conseguinte, a segurança jurídica, mas usurpada a reserva parlamentar. É assim, em resposta a esses princípios constitucionais do direito de proteção de dados, que o catálogo de normas que autorizam medidas específicas de tratamento de dados vem crescendo constantemente no Código de Processo Penal alemão.[24]

Em suma, pode-se afirmar que o direito de proteção de dados, inclusive no processo penal, tem na Alemanha uma clara configuração constitucional: "o forte arrimo nos direitos fundamentais é uma especificidade do direito de proteção de dados alemão."[25] Dela decorre, em primeira linha, a exigência de reserva de lei naquele país.

2. O desenvolvimento no Brasil e a necessidade de fundamento em lei para medidas de tratamento de dados

Essa forte arrimo nos direitos fundamentais *não é exclusiva* do direito de proteção de dados alemão. O direito brasileiro, sob influência do regime europeu de proteção de dados, segue um caminho semelhante.[26]

A LGPD insere a disciplina da proteção de dados explicitamente em uma moldura constitucional (art. 2º), mencionando, em clara referência à decisão do censo do Tribunal Constitucional Alemão, a autodeterminação informativa[27] (art. 2º, II) como um dos fundamentos da proteção de dados pessoais.

O Supremo Tribunal Federal (doravante, STF) segue o mesmo caminho. Em decisão do Plenário, de relatoria da Min. Rosa Weber, o direito à autodeterminação

---

[24] P. ex. §§ 98a, 100a, 100b, 100c, 100f, 100g, 100i, 100j, 100k StPO. O mesmo processo se verifica nas Leis Policiais, nas quais se regulam intervenções no âmbito de segurança pública. Sobre isso, cf. KINGREEN, Thorsten. POSCHER, Ralf. *Polizei- und Ordnungsrecht*. 11 ed., C.H. Beck, 2020, § 13, Rn. 1 e ss.

[25] LEWINSKI, Kai von. *Die Matrix des Datenschutzes*: Besichtigung und Ordnung eines Begriffsfeldes, Mohr Siebeck, 2014, p. 70.

[26] Para uma exposição mais aprofundada, cf. GLEIZER, Orlandino. MONTENEGRO, Lucas. VIANA, Eduardo. *O direito de proteção...*, p. 31 e ss.

[27] Neste Parecer, usaremos o termo autodeterminação *informacional* no lugar de autodeterminação *informativa*. O porquê dessa opção cf. em GLEIZER, MONTENEGRO, VIANA, *O direito de proteção...*, p. 23, nr. 12.

informacional foi reconhecido como uma decorrência dos direitos da personalidade.[28] Nos fundamentos da decisão, lê-se, por exemplo, que dados pessoais integram o "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)" e que "sua manipulação e tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional."[29] A culminação desse desenvolvimento veio com a recente Emenda Constitucional n. 115/2022, promulgada em 10/02/2022, que incluiu no *caput* do art. 5º da CF, o inciso LXXIX, segundo o qual "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". Assim, pode-se afirmar, sem temor, que o forte arrimo nos direitos fundamentais é também uma especificidade do direito de proteção de dados no Brasil.

Se isso é assim, é de fundamental importância que se extraiam as devidas consequências da escolha de veicular a proteção dos dados pessoais por meio de cláusula de direitos individuais. Uma delas é a exigência de lei autorizativa veiculada pelo Poder Legislativo.

A exigência de reserva de lei, enquanto decorrência do princípio do Estado de Direito e da separação de Poderes,[30] é amplamente reconhecida pela doutrina brasileira. Já *José Afonso da Silva* afirmava que a reserva de lei "consiste em estatuir que a regulamentação de determinadas matérias há de fazer-se necessariamente por lei formal".[31] Encontram-se hoje autores de renome que mencionam a reserva de lei como um limite formal às restrições de direitos fundamentais.[32] E não o fazem sem razão. A

---

[28] STF, ADI 6.387 MC-Ref, Tribunal Pleno, Min. Rosa Weber, DJe 12/11/2020.

[29] STF, ADI 6.387 MC-Ref, Tribunal Pleno, Min. Rosa Weber, DJe 12/11/2020, p. 10 do voto da Ministra Relatora.

[30] GLEIZER, MONTENEGRO, VIANA, *O direito de proteção...,* p. 40 e ss.; PÉREZ BARBERÁ, Gabriel. Reserva de ley, principio de legalidad y proceso penal. *En Letra.* Derecho Penal, p. 42–92, 2015, *passim*.

[31] SILVA, José Afonso da, *Curso de direito constitucional positivo*. 37 ed., Malheiros, 2013, p. 425.

[32] SARLET, MARINONI, MITIDIERO, Daniel. *Curso de direito...,* p. 549; MENDES, BRANCO, *Curso de direito...*, p. 249 e ss.; CANOTILHO, J. J. Gomes *et. al.* (Coords.). *Comentários à Constituição do Brasil*. 2 ed., Saraiva, 2018, *e-book,* p. 506; DIMOULIS, Dimitri, MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 8. ed. Revista dos Tribunais, 2021, p. 197. No direito português, cf. CANOTILHO, J. J. Gomes. Direito constitucional. Almedina, 2003, p. 256.

reserva de lei, enquanto limite à intervenção em direitos individuais, está positivada na CF e estabelece que ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei (art. 5º, II, CF).[33] Além dessa enunciação geral, o texto constitucional ainda afirma, expressa e inequivocamente, uma *reserva de lei parlamentar em matéria de direitos individuais* (art. 68º, § 1º, II, CF). Noutras palavras, o texto constitucional é claro ao exigir que o Congresso Nacional regule, ele mesmo, matéria concernente a direitos individuais, o que abrange, especialmente, restrições a esses direitos.

Uma vez que dados pessoais, conforme visto, são tidos, tanto pela jurisprudência constitucional, como pelo próprio Constituinte, como cobertos por cláusula protetiva que, em última análise, é referida ao regime geral de proteção da personalidade, trata-se aqui de direitos individuais, cujas restrições estão submetidas à reserva de lei parlamentar.[34] Isso vem sendo reconhecido inclusive pelo próprio legislador infraconstitucional. Já antes de todo esse desenvolvimento mais recente, havia uma sensibilidade no sentido de que medidas que implicassem grave intervenção na esfera de informações privadas demandariam autorização em lei. Tanto é assim que interceptações telefônicas ou captações ambientais só passaram a ser autorizadas nos termos da LIT.[35]

Com a entrada em vigor da LGPD, que estabelece as hipóteses segundo as quais o tratamento de dados pode ser realizado (art. 7º), tornou-se ainda mais clara a necessidade de autorização legal. Quanto ao tratamento de dados para fins de atividades de investigação e repressão de infrações penais, que não está submetido ao regime geral

---

[33] Assim também, GRECO, Luís. Introdução. In. WOLTER, Jürgen. *O inviolável e o intocável no direito processual penal*. Reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Marcial Pons, 2018, p. 21, 36.

[34] GLEIZER, MONTENEGRO, VIANA, *O direito de proteção*..., p. 40 ss.; ESTELLITA, Heloisa. O RE 1.055.941: um Pretexto para Explorar Alguns Limites à Transmissão, Distribuição, Comunicação, Transferência e Difusão de Dados Pessoais pelo COAF. *Revista de Direito Público*, v. 18, n. 100, pp. 606-636, out./dez., 2021, p. 609 e ss; MENDES, Laura Schertel. Uso de softwares espiões pela polícia: prática legal? *JOTA*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015. Acesso em: 5. fev. 2022.

[35] Cf. o paradigmático precedente do Plenário do STF no HC 69.912, sob relatoria do Min. Sepúlveda Pertence, no qual a Corte julgou ilegal uma interceptação telefônica determinada judicialmente por falta de lei que a disciplinasse na época (DJ 25/03/1994).

de proteção de dados da LGPD (art. 4º, III, d), a lei ressalta que será "regido por legislação específica", que "deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei" (art. 4º, § 1º, LGPD). O MCI regula em parte e de forma bastante específica a matéria ao cuidar das condições de armazenamento de dados pessoais por provedores de aplicações de internet (art. 15 e ss., MCI), bem como as condições de seu compartilhamento com órgãos de persecução penal (art. 22, c.c. art. 10, MCI).

Há, portanto, razões de sobra para que se reconheça uma reserva de lei para medidas de tratamento de dados pessoais por órgãos de persecução penal.[36] Essa é uma premissa fundamental e inarredável para que se possa responder adequadamente ao primeiro quesito.

Por esta razão é que, com o presente caso, o STF tem preciosa oportunidade para reafirmar a exigência de reserva de lei em matéria de intervenções em direitos fundamentais, uma exigência que, entre nós, nem sempre tem recebido a reverência que lhe cabe enquanto princípio basilar do Estado de Direito.

3. Duas implicações importantes

a) Reserva de lei e limites à interpretação analógica

Não se deve confundir a reserva de lei, que é geral e aplicável a todo o Direito Público, com o estrito princípio de legalidade vigente no Direito Penal.[37] Contudo, tanto da reserva de lei como do princípio da legalidade decorrem, no mínimo, consideráveis

[36] *Pérez Barberá* acentua a necessidade de se pensar no processo penal como um "processo informacional", "um processo caracterizado especificamente pela obtenção, uso e circulação de informações", do que decorre que "toda ingerência do Estado – no âmbito do processo penal – neste direito do imputado a um controle da informação que lhe concerne requer, necessariamente, de expressa e prévia autorização legal, conforme exige a vigência do princípio da reserva de lei" (PÉREZ BARBERÁ, Gabriel. A prova como informação e a "autodeterminação informacional": Direito fundamental do imputado. In. RAMOS, João Gualberto Garcez. ESQUIVEL, Carla Liliane Waldow (Orgs.). *Ciência penal em perspectiva comparada*: ensaios & reflexões. Boreal, p. 57–79, 2016, p. 66-67).

[37] KUDLICH, Hans. *Münchener Kommentar zur StPO*, Einleitung, Band I, C. H. Beck, 2014, Rn. 602; ROXIN, Claus. GRECO, Luís. *Strafrecht*: AT, Band I. 5ed., C.H. Beck, 2021, § 5, Rn. 43a.

restrições à possibilidade de analogia. Do contrário, a própria noção de reserva de lei perderia o sentido, já que a inexistência de lei sempre poderia ser substituída por uma interpretação analógica.

Por essa razão, na Alemanha, embora a analogia no processo penal não seja em geral proibida, a doutrina majoritária reconhece uma proibição de analogia no âmbito de medidas coercitivas e investigativas que intervenham em direitos fundamentais.[38] Se a medida não estiver discriminada em lei, conclui-se que não há autorização legal para sua realização, e o recurso à analogia significaria perverter a vontade do legislador. Exceções a essas regras são admitidas apenas em casos de medidas bagatelares ou no caso das denominadas *faculdades anexas*, isto é, medidas acessórias que são tipicamente necessárias para realizar a medida principal e que, por isso, são implicitamente autorizadas por ela (p. ex. a prisão em flagrante também autorizaria lesões corporais leves, quando estritamente necessárias para deter o suspeito em fuga).[39] Obviamente, essa proibição de analogia também é aplicável a medidas de investigação que envolvam o tratamento de dados pessoais. Isso foi enfatizado pela jurisprudência alemã, p. ex., em relação à infiltração online em sistemas informáticos (Online-Durchsuchung).[40] Medidas autorizadas em lei, como o monitoramento de telecomunicações ou a busca e apreensão, não serviriam de fundamento legal para a infiltração online, que consistiria em uma intervenção de outra natureza.[41] Por isso, foi preciso que o legislador estabelecesse uma autorização legal específica para a infiltração online (atual § 100b, StPO).

Por ser decorrência da noção de reserva de lei reconhecida também por nossa CF, os mesmos princípios têm de valer para o processo penal brasileiro. Na

---

[38] WOHLERS, Wolfgang. GRECO, Luís. *Systematischer Kommentar zur Strafprozessordnung.* Band II, 5 ed., Carl Heymanns, 2016, Vor § 94 e ss., Rn. 2.

[39] Mais detalhes, em GLEIZER, Orlandino. Begleitmaßnahmen als Überwindung typischerweise zu erwartenden Widerstands. *Goltdammer's Archiv für Strafrecht*, 2021, 395 ss. (GA 2021, 395).

[40] BVerfGE 120, 274, 315 ss.; BGHSt 51, 211. Em língua portuguesa, cf. recente tradução do texto de HOFFMANN-RIEM, Wolfgang, A Proteção Jurídica Fundamental da Confidencialidade e da Integridade dos Sistemas Técnicos de Informação de Uso Próprio. *Revista de Direito Público*, v. 18, n. 100, p. 457–499, 2021.

[41] Cf. GRECO, GLEIZER, A infiltração online..., p. 1483–1518.

doutrina pátria, fala-se em exigência de legalidade para as medidas cautelares, o que significa que "medidas cautelares processuais penais são somente aquelas previstas em lei e nas hipóteses estritas que a lei autoriza."[42] *Gustavo Badaró*, por exemplo, busca um fundamento para essa exigência na Convenção Americana sobre Direitos Humanos (art. 7º, CADH), que, segundo posicionamento do STF, goza de natureza supralegal.[43] Pode-se mencionar, nesse contexto, também o art. 30, CADH, que é explícito quanto à exigência de lei para a restrição a direitos e liberdades previstos na Convenção.[44] Sem prejuízo dessas fundamentações, que também são corretas, não é necessário ir tão longe. Em essência, a legalidade das medidas cautelares, exigida pela doutrina, não é outra coisa senão uma manifestação consequente da exigência de reserva de lei, para a qual, como exposto, há claro fundamento constitucional. Da reserva de lei decorre que não é possível empregar analogia para suprir fundamento legal inexistente. Medidas cautelares e investigativas, inclusive aquelas de tratamento de dados pessoais, exigem autorização taxativa em lei.[45]

Aplicando-se essas considerações ao primeiro quesito discutido neste Parecer, conclui-se que a requisição de dados obtidos por meio de busca reversa determinada judicialmente só é um instrumento legítimo à disposição dos órgãos de persecução penal se houver uma norma autorizativa aprovada pelo Parlamento, que autorize e delineie com clareza seus contornos. Por isso, é necessário, num próximo

---

[42] BADARÓ, Gustavo. *Processo Penal*. 10 ed., RT, 2022, p. 1177.

[43] Ibid., p. 1178.

[44] "As restrições permitidas, de acordo com esta Convenção, ao gozo e exercício dos direitos e liberdades nela reconhecidos, não podem ser aplicadas senão de acordo com leis que forem promulgadas por motivo de interesse geral e com o propósito para o qual houverem sido estabelecidas"), dentre eles o direito à privacidade (art. 11, nr. 2). Segundo *Pérez Barberá*, na Argentina, a reserva de Parlamento para intervenções em direitos fundamentais decorre do disposto no art. 30 da CIDH, que ali tem status constitucional (cf. PÉREZ BARBERÁ, Reserva de ley..., p.47). E a Corte Interamericana de Direitos Humanos reconheceu que a expressão "leis" do art. 30 deve ser entendida como lei em sentido formal, ou seja, proveniente do Parlamento (Opinião Consultiva 8/86, de 09/05/1983, *apud* PÉREZ BARBERÁ, Reserva de ley..., p. 47, nota 10).

[45] Nesse mesmo sentido, afirma *Pérez Barberá* que do "principio general de reserva de ley se infieren entonces las prohibiciones de retroactividad (lex praevia), de analogía (lex stricta) y de la costumbre como fuente (lex scripta), así como el mandato de determinación (lex certa) y el de proporcionalidad. Dichos corolarios no son, pues, exclusivos del principio de legalidad del Derecho penal material, sino de toda reserva de ley que tenga la fuerza de una reserva de Parlamento" (PÉREZ BARBERÁ, Reserva de ley..., p. 46-47).

passo, esmiuçar, uma a uma, as medidas de tratamento de dados autorizadas para fins de persecução penal, a fim de saber se a busca reversa aqui examinada encontra arrimo em alguma delas.

b) A distinção entre "dados estáticos" e "dados dinâmicos"

Antes, no entanto, é preciso esclarecer um ponto que também decorre da inserção do direito de proteção de dados brasileiro na moldura constitucional de direitos individuais fundamentais.

Um dos argumentos apresentados para justificar a requisição de dados aqui examinada tem por base uma distinção entre "dados estáticos" e "dados dinâmicos",[46], extraindo-se dessa diferença consequências para os níveis de proteção de cada uma dessas categorias.[47] "Dados estáticos" seriam aqueles armazenados em registros, servidores ou bancos de dados, mas que não integram um processo de comunicação em tempo real, enquanto os "dados dinâmicos" seriam informações transmitidas por interlocutores de um processo de comunicação no momento que este acontece. Os primeiros estariam abrangidos pelo art. 5º, X, CF, no qual está positivada a inviolabilidade da intimidade e da privacidade; os segundos, pelo art. 5º, XII, CF, que protege diversas formas de comunicação. Com base nisso, embora o texto constitucional em ambos os casos fale em inviolabilidade, afirma-se uma diferença no grau de proteção.[48]

Essa tese merece alguns esclarecimentos. Não se desconsidera que a distinção entre "dados estáticos" e "dados dinâmicos" possa ser útil para delimitar os âmbitos de proteção de diferentes direitos fundamentais. É possível que o art. 5º, XII, CF, destine-se apenas à proteção do processo de comunicação à distância, de sorte que só

[46] Ou "em fluxo", como prefere LIGUORI, Carlos. *Direito e criptografia*. Saraiva Jur, 2021, *e-book*, item 4.1.1.1.

[47] STJ, RMS 60.698, fls. 427-428.

[48] Assim, por exemplo, lê-se no acórdão recorrido: "decerto que o art. 5º, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, repita-se, o acesso a esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma" (STJ, RMS 60.698, ementa, item 4).

estariam abrangidos por seu âmbito de proteção os dados em trânsito. Disso não decorre, no entanto, uma distinção *a priori* acerca do nível de proteção; muito menos, seria legítimo, com base nessa distinção, justificar um processamento de "dados estáticos" sem base legal, sob o argumento de que os direitos fundamentais estabelecidos pelo art. 5º, X, CF, gozariam de uma tutela mais débil.

Afinal, a proteção dada pelo art. 5º, X, CF – reforçada pelo recente reconhecimento da autodeterminação informacional como direito fundamental – é, por si só, *suficiente para produzir os efeitos típicos de um direito fundamental individual, dentre os quais, como visto, figura a exigência da reserva de lei*.[49] Que o Constituinte tenha posto diferentes âmbitos da vida sob diferentes cláusulas protetivas é importante, em primeira linha, para que se saiba exatamente em qual direito se está intervindo. As intervenções exigem, como tais, no entanto, autorização em lei. *Tércio Sampaio Ferraz Jr.*, que parece ter sido o primeiro na doutrina brasileira a defender uma distinção nos termos expostos acima, não deixa de apontar, contudo, os fundamentos legais em que estão baseadas medidas de vigilância fiscal, que eram o objeto de seu artigo.[50]

Além disso, em face do intenso processo de digitalização a que assistimos hoje, a tese de que essas espécies de dados correspondem a uma diferença de proteção dificilmente se sustenta.[51] Os sistemas informáticos dispõem atualmente de uma capacidade de processamento e armazenamento de dados sem precedentes na história da humanidade. Adicione-se a isso o fato de que a utilização de computadores, aparelhos

---

[49] No mesmo sentido, STF, MS 38.189 MC/DF (decisão monocrática do Min. Gilmar Mendes): "Como mencionado acima, uma vez que os dados de registros e de comunicações pessoais indubitavelmente são albergados pelo direito fundamental à privacidade (art. 5º, incisos X e XII, da Constituição Federal), é importante perquirir se existe previsão legal que define sob quais circunstâncias esse sigilo constitucional pode ser afastado."

[50] FERRAZ JR., Tércio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista Da Faculdade De Direito da Universidade De São Paulo*, 88, 1993, p. 451 e ss. Somente anos depois da publicação do artigo é que a internet passou a ser comercializada no Brasil como anota LIGUORI, Carlos. *Direito e...* item 4.1.1.1. Uma revisita do próprio autor ao texto de 1993 pode ser encontrada em FERRAZ JR., Tercio Sampaio. O sigilo de dados, o direito à privacidade e os limites do poder do Estado: 25 anos depois. In: ANTONIALLI, Dennys. ABREU, Jacqueline De Souza (Orgs.). *Direitos fundamentais e processo penal na era digital*. Internetlab, 2018, v. 1, p. 20–41.

[51] Nesse sentido, cf. ABREU, Jacqueline de Souza. Comentário ao REsp 1.782.386/RJ – STJ (Acesso a agenda de contatos de celular por autoridade policial sem autorização judicial). ***Revista dos Tribunais***, vol. 1026, pp. 371-406, 2021.

celulares e outros sistemas informáticos são hoje ubiquitários e de tal forma integrados ao cotidiano das pessoas, que uma boa parte de suas vidas, incluindo trabalho e relações sociais, dá-se por meios digitais. Dados pessoais e sistemas informáticos têm adquirido enorme importância para o livre desenvolvimento da personalidade. Ao mesmo tempo, a grande quantidade de informações armazenadas em computadores pessoais e aparelhos celulares ou fornecidas por meio de uso de aplicativos de internet traz consigo uma particular vulnerabilidade.

Diante desse quadro, seria um *grave erro* supor que apenas informações transmitidas de forma instantânea merecessem uma proteção rigorosa.[52] Foi pensando nisso, aliás, que o Tribunal Constitucional Alemão reconheceu, para além da autodeterminação informacional, também, a confidencialidade e a integridade de sistemas informáticos como concretização dos direitos da personalidade.[53] Afinal, a infiltração no computador ou smartphone de uma pessoa, por exemplo, mesmo quando só permita o acesso a "dados estáticos" ali armazenados (e-mails, conversas em aplicativos de trocas de mensagens, fotos, vídeos, notas, dados de online banking, histórico de pesquisas, arquivos em nuvem etc.), pode ter potencial invasivo até mesmo maior do que escutas telefônicas.[54] Isso também vem sendo reconhecido pelo próprio STF, para o qual a evolução tecnológica revelou a impropriedade de se utilizar a dicotomia entre dados estáticos e dinâmicos para esvaziar a proteção garantida aos dados pessoais.[55]

---

[52] Nesse mesmo sentido, LIGUORI, Carlos. *Direito e...*, item 4.1.1.1: "Questiona-se, no cenário atual, até que ponto essa diferenciação jurídica faz sentido sob a perspectiva técnica. Dentre os motivos, podemos destacar a instantaneidade na comunicação de dados provida pela Internet (o que dificulta tecnicamente a identificação do momento em que estes dados estão, de fato, 'em fluxo'), e a multiplicidade de modalidades de comunicação online, bastante distintas entre si (e-mails, mensagem instantânea em sistemas criptografados ponta a ponta, VoIP etc.)."

[53] Cf. BVerfGE 120, 274 (302 ss.).

[54] Cf. BVerfGE 120, 274 (308).

[55] Revendo entendimento anterior acerca da proteção de dados baseada na distinção originalmente proposta por *Ferraz Júnior*, afirmou o Min. Gilmar Mendes, recentemente: "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"(STF, HC 168.052, Segunda Turma, Min. Rel. Gilmar Mendes, m. v., DJe. 02/12/2020, p. 3 do voto, cf. também p. 5).

Por fim, em face das atuais possibilidades técnicas, os serviços informacionais digitais oferecidos aos cidadãos já disponibilizam condições tecnológicas para o armazenamento de dados concomitantemente à sua produção e transmissão pelo usuário. Não seria constitucionalmente legítimo que os órgãos estatais contornassem os exigentes pressupostos das medidas interventivas, como as impostas para a interceptação telefônica, por exemplo, por meio de simples requisições dirigidas aos provedores de aplicações determinando o compartilhamento do conteúdo das comunicações armazenadas de seus clientes, simplesmente argumentando que, encerrado o trânsito (ou fluxo), os dados estáticos estariam desprotegidos.

A diferenciação genérica e anacrônica entre "dados estáticos" e "dados dinâmicos" não serve como justificativa para diferenciar a gravidade das medidas de intervenção informacional. É necessário, pelo contrário, apontar a norma específica que autoriza a medida e demonstrar sua proporcionalidade no caso concreto.

II. Ausência de norma autorizativa para a requisição

Estabelecida a premissa de que todo e qualquer tratamento de dados pessoais exige autorização específica em lei, é necessário escrutinar os dispositivos legais do ordenamento jurídico brasileiro que tenham âmbitos de aplicação próximos ao objeto da decisão judicial aqui examinada. Em primeiro lugar, analisaremos as normas do MCI que foram utilizadas pelo acórdão recorrido para fundamentar a negativa de provimento ao RMS (1). Em seguida, examinaremos outras normas que, embora não tenham sido explicitamente referidas no acórdão, também possuem certa proximidade temática: os dispositivos da LIT (2) e os do CPP referentes à busca e apreensão (arts. 240 ss.) (3).

1. O Marco Civil da Internet (Lei n. 12.965/2014, MCI)

O acórdão recorrido aponta os arts. 22 e 23 c.c. o art. 10, § 1°, do MCI, como aqueles que tratariam "especificamente do procedimento de que cuidam os autos".[56] A partir deles iniciaremos, portanto, a análise dos dispositivos infraconstitucionais.

a) O MCI e as categorias de dados

O MCI estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Para que a prestação de tais serviços possa ser cobrada, para que sejam garantidos os direitos dos usuários e a responsabilização daqueles que, utilizando-se desses serviços, praticam condutas ilícitas por meio da internet, o MCI criou um regime de retenção e fornecimento de certos dados, classificando-os *em categorias claramente definidas*. É à luz dessas categorias de dados que se devem compreender os arts. 10, § 1°, 22 e 23, MCI.

Nesse como em outros aspectos importantes, o regramento brasileiro tem suas raízes estruturais no regime europeu de proteção de dados. O direito alemão, por exemplo, conhece, desde a década de 90, uma *classificação jurídica de dados pessoais* envolvidos tanto no uso de serviços de telecomunicações,[57] como nas demais formas de telemídia[58], inclusive na internet.[59-60] Um *primeiro* grupo de dados, chamados de *dados*

[56] STJ, RMS 60.698, fl. 409, item 7 da ementa.

[57] Telekommunikationsdienstunternehmen-Datenschutzverordnung - TDSV , de 12.7.1996, BGBl. 1996 I, p. 982 e ss.

[58] Telemídia é um conceito empregado no Direito alemão para se referir a serviços eletrônicos de informação e comunicação (§ 1 I S. 1. TMG), sendo aplicável hoje sobretudo a serviços oferecidos pela internet. Em mais detalhes, AUERNHAMMER, Hebert. *DSGVO/BDSG – Kommentar*, § 1 TMG, Carl Heymanns Verlag, 2020, Rn. 7 e ss.

[59] Teledienstedatenschutzgesetz (TDDSG), de 22.7.1997, BGBl. 1997 I, p. 1870, 1871. Hoje a regulação é feita por uma única lei voltada à proteção de dados em ambos os setores (Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien, TTDSG).

[60] Para a classificação a seguir, Cf. BÄR, Wolfgang. Aktuelle Rechtsfragen bei strafprozessualen Eingriffen in die Telekommunikation. *MMR* 2000, pp. 472-480, 2016; SEITZ, Nicolai. *Strafverfolgungsmaßnahmen im Internet*, Heymanns, 2004, S. 69 ff.

de conexão ou tráfego,[61] é formado por aqueles dados necessários para possibilitar o uso do serviço ou a posterior cobrança por seu uso: registros relativos ao início e ao fim do uso do serviço, à espécie de mídia utilizada e a elementos de identificação do usuário do serviço (p. ex. número do telefone, no caso de telecomunicações; endereço de IP [Internet Protocol], no caso de uso de aplicativos de internet etc.). Um *segundo* grupo, denominado de *dados cadastrais,*[62] abrange os dados necessários para constituir e alterar a relação contratual entre prestadora de serviço e cliente, p. ex., nome, endereço, profissão, dados para a cobrança etc. O *terceiro* grupo, o dos *dados de conteúdo,* diz respeito àquelas informações produzidas durante a utilização do serviço que *constituem o próprio objeto de sua prestação*, p. ex. as informações trocadas em uma conversa por aplicativos de mensagens ou referentes ao uso de um aplicativo de internet, como a Pesquisa do Google, o Mercado Livre, a Amazon, o sistema de pesquisa de jurisprudência do STF, fotos e documentos armazenados em nuvem etc. Para fins de tratamento de dados pessoais no processo penal, confere-se a essa distinção uma importância central, pois o acesso a dados pessoais de *conteúdo* representa uma intervenção bem mais grave do que o acesso aos dados de *conexão* e *cadastro*, de modo que, no caso das telecomunicações, p. ex., o acesso a dados de conteúdo tem de satisfazer os limites rígidos previstos pela lei de monitoramento das telecomunicações.[63]

A partir de 2000, a *União Europeia* também passou a empregar essa distinção em seus esforços de harmonização da legislação de telecomunicações no ambiente europeu. A Diretiva 2002/58/CE reconheceu, como já fazia o direito alemão, uma classe dos "dados de tráfego". Num passo seguinte, editou a Diretiva 2006/24/CE, em muitos aspectos assemelhada ao MCI. Essa Diretiva previa a retenção somente de dados pessoais de *localização e tráfego* gerados no contexto de comunicações eletrônicas ou de redes públicas de comunicação; e havia, inclusive, a afirmação expressa de que ela

---

[61] Em alemão, *Verbindungs-* ou *Verkehrsdaten*.

[62] Em alemão, *Bestandsdaten*, que também poderia ser traduzido como *dados constitutivos do serviço*.

[63] Cf. BÄR, Aktuelle Rechtsfragen...., pp. 472-480.

não era aplicável *ao conteúdo* das comunicações eletrônicas, incluindo as informações consultadas por meio da utilização de uma rede de comunicações eletrônicas (Art. 1º, nr. 2[64]). Por força de sua transposição para os ordenamentos jurídicos dos Estados-Membros, esses conceitos tornaram-se a moldura que passou a orientar a regulação da matéria no ambiente europeu. Na transposição dessas normas para seu direito nacional, a *Espanha*, p. ex., fez consignar expressamente na sua Ley 25/2007[65] que: "se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas" (art. 1, nr. 3).

Essa mesma distinção, inaugurada no contexto europeu, aparece, finalmente, na regulação do uso da Internet no Brasil pelo MCI, que abrange tanto formas de comunicação via internet (p. ex. Skype, serviços de correio eletrônico ou de mensagens instantâneas), como o uso das demais aplicações (aplicativos de compras, online banking, pesquisas, músicas etc.).

Tal qual o modelo alemão, o MCI adota o conceito de *dados cadastrais*, ou seja, aqueles que informam qualificação pessoal (nome, prenome, estado civil e profissão do usuário), filiação e endereço (art. 10, § 3º, MCI, c.c. art. 11, § 2º, Decreto n. 8.771/2016) dos usuários de acesso à internet e aplicações; e que, por implicarem interferência menos grave na privacidade, podem ser revelados até mesmo a autoridades administrativas, nos termos da legislação aplicável (art. 10, § 3º, MCI, c.c. arts. 11 e 12 do Decreto n. 8.771/2016[66]).

---

[64] "A presente directiva não é aplicável ao conteúdo das comunicações electrónicas, incluindo as informações consultadas utilizando uma rede de comunicações electrónicas".

[65] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

[66] Sobre a discussão do acesso a dados cadastrais no âmbito do disposto no art. 13-A do CPP, cf. voto do Min. Edson Fachin na ADI 5.642, proferido em 17/06/2021.

Contempla também um equivalente para o grupo dos *dados de tráfego* – também chamados de *metadados,*[67] ou dados sobre dados[68] –, que no MCI encontra-se subdividido em *registros de conexão* e *registros de acesso a aplicações de internet*. Os primeiros são dados coletados pelo provedor da conexão (Oi, Sky, Claro, GVT etc.); os últimos, pelas empresas provedoras de aplicações de internet. Uma aplicação de internet é definida como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet" (art. 5º, VII), como, por exemplo, os navegadores (Microsoft Edge, Google Chrome, Safari, Mozilla etc.), os sites (aplicativos) de mapas, os aplicativos de compras (Rappi, Mercado Livre etc.), de bancos, de transporte (Movit, Uber, 99 etc.) assim como as ferramentas de busca/pesquisa, a exemplo do buscador do Yahoo, do Google e do Tripadvisor.

Os dados relativos ao *registro de conexão* abarcam "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" (art. 5º, VI). Essas informações devem ser retidas pelo período de um ano pelos administradores de sistemas autônomos de provisão de conexão à internet (art. 13, *caput*). Quanto aos elementos que compõem os *registros de acesso a aplicações de internet*, o MCI os define como "o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (art. 7º, VIII) e determina sua retenção pelo prazo de seis meses (art. 15, *caput*).

---

[67] Segundo KIFT, Paula. NISSENBAUM, Helen. Metadata in Context - An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program. *Journal of Law and Policy for the Information Society*, v. 13, n. 2, pp. 333–372, 2016, p. 339, a primeira vez que a U. S. Supreme Court distinguiu dados de conteúdo de metadados foi em 1878, justamente em caso no qual se questionava o acesso ao conteúdo em contraposição ao acesso a dados externos (*outward form and weight*) de materiais de correspondência físicos.

[68] Metadados são "dados sobre dados", p. ex., relativamente a uma carta, os metadados são o nome do remetente e o do destinatário, seus endereços, o peso, o selo postal e o carimbo do serviço postal. Sobre o conceito de metadados, cf. ABREU, Jacqueline de Souza. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. *Revista Brasileira de Políticas Públicas*, v. 7, n. 3, p. 24–42, 2017, p. 32. Sobre metadados em serviços de telefonia, cf. ABREU, Jacqueline de Souza. Guarda obrigatória de registros de telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais. In. *¿Nuevos paradigmas de vigilancia?* Miradas desde América Latina: Memorias del IV Simposio Internacional Lavits. Buenos Aires: [s.n.], pp. 295–306, 2017, p. 296. Uma análise ontológica e normativa dos metadados à luz do programa da NSA de coleta indiscriminada de metadados em serviços de telefone fazem KIFT, NISSENBAUM, Metadata in Context..., p. 333–372.

Como se vê claramente, nem os dados relativos ao *registro de conexão*, tampouco os dados relativos ao *registro de acesso a aplicações de internet* compreendem o *conteúdo* da conexão ou do acesso a aplicações, isto é, aquilo que o usuário faz uma vez conectado ou uma vez que tenha acessado uma aplicação. De forma didática e no que diz respeito ao registro de acesso a aplicações de internet, essa categoria abrange *a data e hora que um determinado endereço de IP* acessou o Microsoft Edge, o Rappi, o Uber, a Pesquisa do Google etc., *mas não* o histórico de navegação no Edge, os pedidos no Rappi, as corridas no Uber, ou as pesquisas no Google. Em suma, a categoria de dados para a qual há um dever de retenção (armazenamento)[69] *não abrange o conteúdo do uso dos serviços de conexão e de aplicações*.[70]

Pelo contrário, o paralelo com a classificação no contexto europeu revela que a intenção do legislador foi especificar com clareza as classes de dados a serem obrigatoriamente retidos (armazenados) pelos prestadores de serviço na internet, distinguindo esses dados daqueles referentes ao *conteúdo* do uso dos serviços.

Segundo relata *Monteiro*, desde o início das discussões do PL 2.126/2011, a questão do armazenamento de registros eletrônicos era um ponto central dos debates legislativos, especialmente no que tange aos registros de acesso a aplicações. Aqui se tratava de balancear, de um lado, a intimidade e a privacidade dos usuários e, de outro, a obtenção do material probatório necessário para a solução das demandas judiciais em

---

[69] Os deveres de *retenção* e de *compartilhamento* de dados previstos no MCI (arts. 13 e ss. e 22, MCI) se restringem, como dissemos, aos dados relativos ao registro de conexão e de acesso a aplicações de internet. Isso não exclui a possibilidade de que outros dados sejam tratados pela empresa, desde que o tratamento encontre outro fundamento legal, como, por exemplo, o consentimento do usuário, e atenda aos demais requisitos da LGPD. No entanto, neste último caso, não há que se falar em *dever* de retenção, muito menos de compartilhamento. O *dever de compartilhamento* limita-se aos dados previstos no art. 22 do MCI (cf. adiante).

[70] "O art. 10 entabula um dever de disponibilização dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas. Todavia, fica claro da leitura da lei que tanto o escopo do dever de disponibilização quanto as condicionantes dessa disponibilização assumem limites e critérios diferenciados quando se trata de registros de conexão e de acesso vis a vis os conteúdos das comunicações privadas em si. Os registros de conexão à internet equivalem, na forma da lei, simplesmente ao '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' (art. 5º, inciso VI). Trata-se, portanto, dos chamados metadados, os quais podem ser tecnicamente acessados por empresas de aplicativos sem que seja necessário violar o padrão de criptografia ponta-a-ponta. Esses dados, no entanto, não revelam qualquer elemento do conteúdo da comunicação" (STF, MS 38.189 MC, Min. Gilmar Mendes, 2021).

torno de ilícitos praticados por meio da internet.[71] Esse balanceamento se deu por meio da determinação de retenção obrigatória (prescrita em lei) do mínimo necessário, ou seja, apenas de "registros de 'acesso' à aplicação, por período delimitado de tempo, não incluindo eventuais registros de 'navegação' do usuário quando este já estiver 'dentro' da aplicação, uma vez que tais dados podem revelar os hábitos de uso do serviço".[72] Confirma-se, assim, a importância fundamental da distinção entre, de um lado, dados de conteúdo e, de outros, dados envolvidos em registros de conexão e de acesso a aplicações de internet (metadados).

Além disso, essa distinção corresponde aos objetivos da lei ao exigir dos provedores de conexão e aplicativos o armazenamento dos registros. Afinal, não seria razoável, além de implicar numa violação à privacidade e à proteção de dados, exigir que empresas provedoras de serviços na internet *mantivessem obrigatória e preventivamente registros de todo o conteúdo* produzido por seus usuários, apenas para mantê-los à disposição em caso de necessidade futura. Dentre os precedentes que tratam da matéria, merece destaque o voto da Min. Rosa Weber na ADI 5.527, na qual se examina a constitucionalidade dos arts. 10, § 2º, e 12, incisos III e IV, MCI: "*a obrigação de guarda de metadados, de que trata o art. 15 do Marco Civil da Internet, não se estende a conteúdo*. O referido preceito é expresso ao determinar, aos provedores de aplicações de internet, a guarda, sob sigilo, dos registros de acesso (metadados)" (p. 22, itálico nosso). Na linha do regramento europeu e da letra clara do próprio MCI, acrescentou que tal "obrigação, à evidência, não se estende ao **conteúdo** das comunicações" (grifo original). Isso, prossegue, "equivaleria a determinar que companhias telefônicas armazenassem as

[71] MONTEIRO, Renato Leite. Da proteção aos registros, aos dados pessoais e às comunicações privadas. In. DEL MASSO, Fabiano. ABRUSIO, Juliana. FLORÊNCIO FILHO, Marco Aurélio. *Marco civil da internet* – Lei 12.965/2014. Revista dos Tribunais, pp. 139-153, 2014, p. 143-144.

[72] Ibid., p. 143. No mesmo sentido, FURLANETO NETO, Mário. GARCIA, Bruna Pinotti. Da guarda de registro de acesso a aplicações de internet na provisão de aplicações. In. LEITE, George Salomão. LEMOS, Ronaldo (Orgs.). *Marco Civil da Internet*. Atlas, p. 773–790, 2014: "Propriamente em relação ao conflito intimidade x segurança jurídica, não parece despontar prejuízo a quaisquer das facetas, uma vez que os registros *não recaem sobre o conteúdo das aplicações* propriamente ditas, mas tão somente sobre o momento de acesso a elas, preservando-se a intimidade do internauta na rede" (p. 788, itálico nosso). Também ARAS, Vladimir. A questão penal no marco civil. 2010, *passim*. Disponível em: https://blogdovladimir.files.wordpress.com/2010/01/artigo-marco-civil-da-internet.pdf. Acesso em: 24 nov. 2021.

gravações de todas as chamadas realizadas por seus usuários, por igual período, para que ficassem à disposição em caso de eventual mandado judicial para sua disponibilização" (p. 23).[73]

Pelo contrário, o MCI busca, de um lado, assegurar às empresas as informações necessárias para prestar o serviço ou realizar cobranças; de outro, que seja possível identificar o autor de um ato ilícito praticado *por meio do uso desses serviços*, considerando que a anonimidade na internet favorece o cometimento de crimes e dificulta a investigação. Originalmente, aliás, o PL 2.126/2011 nem sequer previa a obrigatoriedade da guarda dos registros de acesso a aplicações, que era facultativa e só se tornaria obrigatória em face de determinação judicial (arts. 12 e 13). Em virtude da dificuldade que esse regime imporia para a identificação de autores de ilícitos praticados por meio da internet, a determinação de retenção foi introduzida após acirrados debates parlamentares.[74]

Portanto, o sentido da lei é o de permitir que o afetado (a vítima, ou a "parte interessada", para usar a linguagem do art. 22 MCI, a exemplo do Ministério Público), ao tomar conhecimento de um conteúdo ilícito como, por exemplo, uma postagem ofensiva no Twitter, possa requerer judicialmente os dados de *registro de acesso à aplicação*, com o que poderá obter a data e hora de uso da aplicação de internet a partir de um determinado endereço de IP. De posse desse endereço de IP e por meio da obtenção

---

[73] Reportando-se aos dados do registro de acesso à aplicação, o STJ também ressalta que o dever de retenção não alcança os dados referente ao uso (conteúdo) das aplicações: "Inexiste obrigação legal para o armazenamento, por qualquer prazo, das informações ao [sic] conteúdo das mensagens trocadas em perfil do Facebook" (ementa, item 2); "a obrigação de guarda diz respeito apenas aos dados referentes ao acesso (data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço de IP) a aplicações da internet, no caso, à conta. Nada diz a lei quanto às mensagens ou *demais conteúdos do aplicativo*" (p. 18/6) (STJ, AgRg no RMS 56.496, Sexta Turma, DJe 30/04/2018). E, há pouco, essa mesma Corte decidiu que no "Marco Civil da Internet, há apenas duas categorias de dados que devem ser obrigatoriamente armazenados: os registros de conexão (art. 13) e os registros de acesso à aplicação (art. 15). A restrição dos dados a serem armazenados pelos provedores de conexão e de aplicação visa a garantir a privacidade e a proteção da vida privada dos cidadãos usuários da Internet. Não há, assim, previsão legal atribuindo aos provedores de aplicações que oferecem serviços de e-mail, como é o caso da recorrida, o dever de armazenar as mensagens recebidas ou enviadas pelo usuário e que foram deletadas" (STJ, RE 1.885.201, Terceira Turma, DJe 25/11/2021, item 6 da ementa).

[74] Cf. CABELLO, Marcos Antônio. Da guarda de registros de acesso a aplicações de internet. In. LEITE, George Salomão. LEMOS, Ronaldo (Orgs.). *Marco Civil da Internet*. Atlas, p. 711-726, 2014, p. 713-715, 722.

dos dados de *registro de conexão,* será possível encontrar ou se aproximar da identidade do usuário da máquina a que corresponde àquele endereço.[75]

Por isso, é de fundamental importância, que se diferenciem dados de conteúdo dos demais dados que, segundo o regramento do MCI, são objeto de deveres de retenção e compartilhamento. Essa distinção está na base do modelo adotado pelo ordenamento brasileiro para a regulação da internet e condiz com os fundamentos da proteção de dados hoje positivados na LGPD e na Constituição Federal.

b) O art. 22, MCI

Com base nesses conceitos e distinções, cumpre examinar a disciplina do MCI acerca da determinação judicial de fornecimento de dados retidos à parte interessada, que é objeto do disposto no art. 22:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
>
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
>
> I - fundados indícios da ocorrência do ilícito;
>
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
>
> III - período ao qual se referem os registros.

A linguagem clara e certeira do *caput* não deixa qualquer dúvida quanto ao limite do objeto das decisões judiciais nele fundadas: "fornecimento de registros de conexão ou de registros de acesso a aplicações de internet".

Como o conteúdo da busca/pesquisa, ou melhor, o termo pesquisado, extrapola o conceito de *registro de acesso*, na medida em que também revela o que o usuário fez durante o acesso à Pesquisa do Google, *padece de ilegalidade inequívoca* a ordem que determina, com base no art. 22 do MCI, que "o provedor de aplicação de internet GOOGLE INC, forneça a identificação dos IP's ou 'DEVICE IDs' que tenham se

[75] Cf. CABELLO, Da guarda de..., p. 712.

utilizado do Google Busca (seja através do aplicativo ou sua versão WEB) no período compreendido entre o dia 10/03/2018 a 14/03/2018, para realizar consultas dos seguintes parâmetros de pesquisa: 'MARIELE FRANCO', 'VEREADORA MARIELE', 'AGENDA VEREADORA MARIELE', 'CASA DAS PRETAS', 'RUA DOS INVÁLIDOS, 22' ou 'RUA DOS INVALIDOS'".

Foi a própria lei que fixou o conteúdo semântico das expressões *registros de conexão* e *registros de acesso a aplicações de internet* utilizadas pelo *caput* do art. 22, que estão definidas no art. 5º, VI e VIII, MCI.

As definições são, ademais, condizentes com a classificação já exposta e com o próprio sentido que orienta a retenção dos registros: viabilizar a responsabilização pelos danos decorrentes do conteúdo ilícito gerado por usuários.[76] Como visto, coube ao MCI prever mecanismos para que se pudesse identificar o responsável por conteúdos danosos. E daí a razão pela qual, imediatamente após cuidar da responsabilidade por danos decorrentes de conteúdo gerado por terceiros (Cap. III, Seção III), o MCI passa a tratar "da requisição judicial de registros" (Cap. III, Seção IV). O art. 22, MCI, cria um mecanismo para que aquele que já conhece o conteúdo ofensivo, mas que ainda desconhece sua autoria, possa, por meio a obtenção dos dados de registro de conexão e de acesso a aplicações, identificar o autor e, então, promover as medidas de reparação de danos e de responsabilização penal cabíveis.[77]

Foi de uma interpretação sistemática que o Min. Gilmar Mendes, em decisão recente e já mencionada,[78] concluiu que o MCI diferencia a disponibilização dos registros

---

[76] É o que o CGI.br chama de "inimputabilidade da rede", segundo o qual "o combate a ilícitos deve atingir especificamente os responsáveis finais, aqueles que de fato cometeram o crime, e não aqueles que operam os meios utilizados para uso da Internet" (COMITÊ GESTOR DA INTERNET NO BRASIL. O CGI.br e o Marco Civil da Internet: Defesa da privacidade de todos que utilizam a Internet; Neutralidade da rede; Inimputabilidade da rede. Disponível em: https://www.cgi.br/media/docs/publicacoes/4/CGI-e-o-Marco-Civil.pdf. Acesso em: 24 nov. 2021, p. 10).

[77] Neste sentido, STJ, REsp 1.829.821, Terceira Turma, Rel. Min. Nancy Andrighi, DJe 31/08/2020, com ulteriores referências a diversos precedentes daquela Corte. Cf. também ABREU, Jacqueline de Souza. In. CRUZ, Francisco Carvalho de Brito. MARCHEZAN, Jonas Coelho. SANTOS, Maike Wile dos. *O que está em jogo na regulamentação do Marco Civil da Internet?* Relatório final sobre o debate público promovido pelo Ministério da Justiça para a regulamentação da Lei 12.965/2014. Internetlab, 2015., p. 24; CABELLO, Marcos Antônio. Da guarda de..., p. 721.

[78] Medida Cautelar no MS 38.189, Min. Gilmar Mendes, decisão monocrática, p. 15-17.

de conexão e acesso a aplicações da disponibilização do conteúdo das comunicações entabuladas em tais aplicações. Registros de conexão e acesso a aplicações abrangem apenas metadados, que não revelam o conteúdo da conexão ou do acesso à aplicação. A disponibilização do acesso ao conteúdo não teria sido disciplinada no MCI e dependeria de lei ulterior, *inexistente entre nós*. Assim, concluiu: "podemos afirmar que, pelo menos no âmbito do Marco Civil da Internet, é discutível, ao menos em tese, se os provedores de aplicações podem ou não ser obrigados, e sob em que [sic] circunstâncias, a disponibilizarem o acesso a dados pessoais e ao conteúdo de comunicações privadas armazenadas".[79]

No caso sob exame, a requisição dos dados da ferramenta de busca não se limita aos registros de acesso a aplicações de internet, senão que *abrange também dados de conteúdo*. Diferentemente dos casos para os quais foram concebidas as normas do MCI, as autoridades de investigação não estão, aqui, de posse de determinado conteúdo – p. ex., uma postagem no Facebook ou um produto ilegal exposto em um site de vendas – cujo autor precisa ser identificado para responsabilizá-lo pelo ilícito cometido. Pelo contrário, a investigação diz respeito a crime que não ocorreu na internet e pretende primeiro saber se determinados termos ('Mariele Franco' [sic], ' vereadora Mariele' [sic], 'Casa das Pretas' etc.) foram pesquisados, para daí chegar aos identificadores associados aos usuários aos quais se atribui a realização da referida pesquisa — cujo conteúdo, ademais, é, em si mesmo, lícito. Noutras palavras, com a obtenção das informações pretendidas, as autoridades passariam a dispor de duas informações de natureza distinta: (i) passariam a saber se foi feita a pesquisa de certos termos (dados de conteúdo) e (ii) que essas pesquisas foram feitas a partir de certos endereços IP (metadados ou registro

[79] No mesmo sentido, ABREU, Passado, presente..., p. 34: "O Marco Civil da Internet não institui, explicitamente, a obrigação de que aplicações de internet tenham habilidade de quebrar sigilo. Quando obriga que empresas retenham informações, o dever se estende apenas a registros (IP, data e hora de acesso), o que as obriga a, necessariamente, ser capazes de atender a pedidos de quebra de sigilo apenas desses metadados (art. 15). Portanto, o dever jurídico, extraído do direito brasileiro vigente, de que aplicações de internet sejam capazes de quebrar sigilo de conteúdo de comunicações não é evidente; carece de fundamentação — e pode muito bem ser que a conclusão seja de que não exista".

de acesso a aplicações de internet). Contudo, o art. 22 MCI confere ao juiz o poder de requisitar apenas estes últimos (ii), e não os primeiros (i).

Em suma, o art. 22 MCI não autoriza o compartilhamento dos dados requeridos na ordem judicial, pois a requisição envolve a revelação de dados de *conteúdo*.

c) O art. 10, § 1º, MCI

O acórdão recorrido refere-se, em conexão com o art. 22, MCI, também ao art. 10, § 1º, do mesmo diploma legal. O dispositivo determina que o provedor somente estará obrigado a disponibilizar os registros de conexão e acesso a aplicações, "de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º". Uma vez que a lei fala em registros de acesso a aplicações "associados a dados pessoais", poder-se-ia supor que requisições como a ora analisada estariam abrangidas por esse dispositivo. Trata-se de equívoco.

Isso porque também o art. 10, § 1º, MCI, expressa o sentido que orienta a retenção e fornecimento dos registros por força da lei. Ele autoriza o fornecimento de "outras informações que possam contribuir *para a identificação do usuário ou do terminal*", deixando claro que esse conjunto de dispositivos legais pretende viabilizar a *identificação da pessoa* que gerou conteúdo ofensivo ou cometeu crimes por meio da internet,[80] *mas não* a realização de pescaria por rede de arrasto (*fishing expeditions*), valendo-se indiscriminadamente de dados de uso (conteúdo) de aplicações de internet para, num lance de sorte, talvez chegar a algum suspeito da prática de um crime que sequer ocorreu na internet.

[80] Conferir a motivação do relator do Substitutivo para a redação do artigo em MOLON, Alessandro. Substitutivo oferecido em Plenário em substituição à Comissão Especial destinada a proferir parecer ao Projeto de Lei n. 2.126, do Poder Executivo, que "estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil", 2014, p. 36-37. Em comentário ao art. 10, § 1º, MCI, a motivação ressalta "o verdadeiro objetivo da lei: tornar possível a disponibilização de registros de conexão e de acesso de usuário mediante ordem judicial" (p. 37).

Sustentar o contrário significaria *subverter* todo o sentido dos conceitos e regras positivados no MCI. O art. 22, MCI, inserido na Seção IV ("Da Requisição Judicial de Registros"), claramente restringe o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. O art. 10, § 1º, MCI, inserido na Seção II ("Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas"), cujo objetivo é, como o nome da Seção indica, proteger a segurança dos dados armazenados,[81] precisa ser lido também à luz do art. 22, MCI. *Se, ao contrário, o art. 10, § 1º, MCI, for interpretado como compreendendo todo e qualquer dado pessoal, inclusive dados de conteúdo, o art. 22, MCI, que tem precisamente a função de regular a requisição judicial de dados, perde seu objeto e deixa simplesmente de fazer sentido.*

Daí que os dados pessoais ou outras informações "que possam contribuir para a identificação do usuário ou do terminal", a que faz menção o art. 10, § 1º, MCI, podem ser somente dados de natureza semelhante àqueles cujo fornecimento é autorizado pelo art. 22, MCI, e que podem contribuir para *identificar* o usuário a partir de determinado conteúdo ilícito que já se conhece. Pode-se mencionar, como exemplos desses "dados pessoais ou outras informações" no sentido do art. 10, § 1º, MCI, os metadados que não foram incluídos nas definições de registros de conexão e de acesso a aplicações de internet, como p. ex. o tipo de navegador (browser) utilizado para acessar um site. Além disso, podem estar abrangidos por esse dispositivo também os dados cadastrais, em relação aos quais o próprio art. 10, § 3º, MCI, autoriza o fornecimento às autoridades administrativas que detenham competência legal para a sua requisição.

[81] Assim, por exemplo, a fundamentação do relator do Substitutivo deputado Alessandro Molon: "A Seção II, que precede o art. 10, foi renomeada de 'Da Guarda de Registros' para 'Da Proteção aos Registros, Dados Pessoais e Comunicações Privadas', de modo a melhor descrever o objetivo dos artigos seguintes, que foram reformulados, para melhor proteger a privacidade dos usuários" (MOLON, Alessandro, Substitutivo oferecido em Plenário em substituição à Comissão Especial destinada a proferir parecer ao Projeto de Lei n. 2.126, do Poder Executivo, que "estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil", 2014, p. 36-37).

d) Conclusão parcial

Em suma, as regras de retenção e fornecimento de dados pessoais do MCI estão inseridas no contexto das categorias e finalidades reconhecidas por esse diploma legal, as quais encontram paralelos em outros ordenamentos.

Quanto ao fornecimento de dados para fins de persecução penal, *os dispositivos referidos se restringem ao compartilhamento de metadados* que possam contribuir para a *identificação* de um usuário na internet. *Os arts. 10 § 1º, 22 e 23, MCI, não autorizam* a requisição de dados de conteúdo e, portanto, a medida sob análise *não pode ser fundamentada nesse diploma legal*.

2. A Lei de Interceptação Telefônica (Lei n. 9.296/96, LIT)

É possível encontrar, ainda que de forma tímida, opiniões no sentido de que a requisição endereçada à Consulente encontraria fundamento legal em dispositivos da LIT. A timidez se justifica, pois a proposta esbarra no óbice de se tratar, na melhor das hipóteses, de uma *ilegal analogia*. A LIT autoriza e regula apenas a *interceptação de comunicações telefônicas* (art. 1º) e *em fluxo* (art. 1º, par. único) e não se aplica ao caso sob exame.

a) Do conceito de comunicação

Os serviços prestados pela Consulente e objeto do caso em questão não se qualificam como comunicações telefônicas. O conceito de comunicações, como é reconhecido majoritariamente pela doutrina, pressupõe a participação de ao menos duas pessoas naturais no processo de troca de informações, uma vez que o vocábulo (do latim, *communicare*) denota *tornar uma informação comum (a alguém)*.[82] Porém, os dados

[82] Cf. GLEIZER, MONTENEGRO, VIANA, *O direito de proteção...*, p. 122; GLEIZER, Orlandino. A proteção de dados por duas portas nas intervenções informacionais. *Revista de Estudos Criminais*, v. 19, n. 79, p. 211-230, 2020, p. 211, p. 215. Com outras referências; ROXIN, Claus. SCHÜNEMANN, Bernd. *Strafverfahrensrecht*. 29 ed., C.H. Beck, 2017, § 36, nm. 4; uma demonstração mais detalhada do problema encontra-se em HEINRICH, Manfred. Surfen im Internet und

almejados pela autoridade policial não são dados oriundos de comunicações telefônicas: eles foram produzidos por meio de processos de pesquisa em bancos de dados (no caso, na internet).

Ao fazer uso do vocábulo "comunicação", não teve o legislador a intenção de autorizar a interceptação de qualquer forma de transferência de dados à distância, senão apenas daquelas que objetivem que uma pessoa natural torne uma informação comum a outra. A eleição do vocábulo "comunicação" impede interpretação contrária, que equivaleria a dizer que também as pesquisas em bibliotecas, os pagamentos por cartões de crédito e os dados bancários, ou seja, quaisquer transferências de informações à distância (pela internet), seriam telecomunicação passível de interceptação autorizada pela LIT. O mero ato de buscar ou disponibilizar uma informação em um determinado espaço, p.ex., em um livro ou em um site, não constitui um processo de comunicação. Vale citar passagem de *Roxin/Schünemann*:

> "Discute-se se a participação de uma só pessoa [no processo de comunicação] seria suficiente, p. ex., caso alguém envie um e-mail a si mesmo (de modo afirmativo, Vassilaki, JR 2000. 447). O sentido natural do termo comunicação seria extrapolado caso ele também fosse empregado em situações nas quais nenhuma informação é compartilhada pela ausência de um interlocutor em relação ao qual algo se torne communis, ou seja, comum. Além disso, a proximidade com o solilóquio e até mesmo com o próprio pensamento é bastante acentuada a ponto de não permitir o acesso ao conteúdo 'solipsista'."[83]

Pelas mesmas razões, não se pode alargar o conceito de comunicação da LIT para alcançar qualquer troca de informações que, na atual sociedade dos processamentos computacionais, possa ser interceptável, *como se (tele)comunicação*

Cloud Computing zwischen Telekommunikationsüberwachung und Online-Durchsuchung. *ZIS,* vol. 09, pp. 421-430, 2020, p. 421.

[83] ROXIN, SCHÜNEMANN, *Strafverfahrensrecht...*, § 36 Rn. 5: "Streitig ist, ob das *Vorhandensein eines einzigen Menschen* ausreichend ist, etwas wenn jemand sich selbst eine E-Mail schickt (bejahend *Vassilaki*, JR 2000. 447). Der natürliche Wortsinn erscheint aber erstens überstrapaziert, wenn man auch dann von Kommunikation spricht, wenn nichts mitgeteilt wird, weil es keinen Zweiten gibt, mit dem man communis, also Gemeinsam macht. Ferner liegt die Nähe zum Selbstgespräch und sogar zum Denken selbst eher nahe, dass man auf ‚solipsistische' Inhalte keinen Zugriff erlaubt".

fosse. Essas considerações já seriam suficientes para negar a aplicação da LIT ao caso em análise, mas há mais.

b) Da medida autorizada pela LIT: o conceito de interceptação

A requisição de dados dirigida à Consulente também não poderia ser fundamentada na LIT por uma outra razão: não se trata de uma medida de *interceptação*. Os dados requisitados, além de não terem sido produzidos por processos de telecomunicação, não estão *em fluxo* e, por isso, não *podem e nem poderiam ter sido interceptados*. Eles já estariam, em tese, armazenados nos servidores da Consulente e não foram produzidos em momento posterior à ordem judicial, mas antes dela. E isso faz toda a diferença.

A medida de interceptação das telecomunicações autorizada pela LIT (art. 1º ss.) é extremamente invasiva. É possível dizer que, ao lado da captação ambiental (art. 8º-A ss., LIT), a interceptação de telecomunicações é a medida informacional mais invasiva da sistemática processual penal vigente. E ela teria um grau ainda mais invasivo caso autorizasse também a coleta (oculta, visto que a interceptação é medida oculta) de dados produzidos em processos de comunicações já findos. A simples escolha de um termo com significado tão específico como *interceptação* já indica que não é possível interceptar objeto que não está em fluxo. Interpretação contrária violaria a manifesta intenção do legislador, que se revela na escolha dos termos (legais), o propósito da norma e o princípio da reserva de lei (e com isso os direitos fundamentais dos afetados).

Por essas razões, não parece razoável aplicar a LIT ao caso para fundamentar a exigência de entrega de dados que, além de não serem oriundos de processo de telecomunicação, não estão em fluxo, *como se a medida consistisse em uma interceptação*.

c) Conclusão parcial

Por estas razões, conclui-se que fundamentar a medida dirigida à Consulente em dispositivos da LIT exige um recurso interpretativo inaceitável para intervenções em direitos fundamentais, porque seria necessário tratar os dados requisitados como se fossem dados de comunicação e a medida como se fosse uma interceptação. Analogias, no entanto, não são autorizadas neste contexto. Essas razões nos parecem suficientes para afirmar que as normas autorizativas de interceptação telefônica dispostas na LIT não se prestam a fundamentar a requisição objeto do Recurso Extraordinário.

Surpreendidos, entretanto, por ordens judiciais determinando medidas como a presente, que carecem de fundamento legal, é compreensível que os destinatários recorram aos parâmetros de proporcionalidade da LIT para se oporem judicialmente ao seu cumprimento no caso concreto. O raciocínio é o de que uma tal medida, que, na prática, pode ser ainda mais grave que a interceptação (que, por sua vez, é uma das medidas mais graves autorizadas no ordenamento jurídico brasileiro), não deveria ser autorizada, nem mesmo pelo legislador, para casos que não satisfaçam, pelo menos, os requisitos da LIT. Este argumento *a fortiori*, no entanto, não autoriza uma analogia destinada a contornar a inexistência de autorização legal. Isso porque o recurso aos pressupostos da LIT poderiam até funcionar, analogicamente, para avaliar a necessidade da medida no caso concreto, mas não teriam o condão de superar o óbice central e logicamente precedente da *ausência de lei* que autorize a medida de forma geral.

3. A busca e apreensão (arts. 240 ss., CPP)

Muito embora nos pareça induvidoso que os dispositivos sobre a busca e apreensão (arts. 240 e ss., CPP) não se aplicam à hipótese ora examinada, deles trataremos brevemente em razão de sua proximidade temática, apenas para exaurir a argumentação.

A espécie de dados que almeja a autoridade policial poderia, eventualmente, ser obtida por uma medida de busca e apreensão. É até mesmo provável que dados

sobre pesquisas efetuadas em ferramentas como o buscador do Google tenham sido armazenados em suportes físicos eletrônicos. A própria natureza desses dados não embaraça a sua utilização enquanto prova penal caso sejam encontrados em dispositivos informáticos apreendidos durante medida de busca dos arts. 240 ss., CPP. Questões de proporcionalidade poderiam/deveriam impor cautelas adicionais a depender das circunstâncias, mas pelo menos os dados relativos ao investigado e ao crime poderiam, a princípio, ser legitimamente valorados.[84]

No entanto, a *medida em si* não está autorizada pelos arts. 240 ss., CPP, que tratam da busca e apreensão. Essas normas autorizam a medida de *busca* (art. 240, *caput,* CPP), não de *requisição*.[85] Ou seja, as normas autorizam a ação de buscar. E isso não é preciosismo. Do ponto de vista teórico, esse limite é o desdobramento mais natural da reserva de lei em relação a normas autorizativas: "como regra, a norma tem de prever a concreta medida interventiva, e isso não apenas por meio de uma conceituação 'funcional' (obter informações, descobrir, esclarecer etc.), que é a linguagem das normas determinadoras de tarefas ou de competências, e sim com termos mais 'naturalísticos', que descrevam o concreto meio que as instâncias de persecução se valerão para cumprir a função que lhes é legalmente atribuída".[86] Porque aquilo que não está expressamente autorizado simplesmente não está autorizado.

Mas os problemas não param aí.

A busca é uma medida pensada e equilibrada para situações distintas da presente. Para sua execução, por exemplo, prevê-se coerção física (§§ 2º e 3º do art. 245, CPP). Os dispositivos tratam tão somente do procedimento de apreensão de pessoa ou coisa (§ 4º do art. 245 CPP). E os demais dispositivos estão todos atrelados à hipótese de busca física. É difícil, da leitura conjunta dos dispositivos, alcançar outra conclusão.

---

[84] No mesmo sentido, MOURA, Maria Thereza Rocha de Assis. BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. In. WOLKART, Erik Navarro *et. al.* (Coord.). *Direito, processo e tecnologia.* 2 ed., Thomson Reuters, 2021, p. 493 e ss.

[85] Reconhecendo, ainda que implicitamente, essa distinção, Ibid., p. 493 ss.

[86] GRECO, Introdução..., p. 39.

Além disso, eles *não criam um dever de colaboração do afetado* para com as autoridades públicas durante a execução da medida. O correspondente dever de tolerância do afetado, que fundamenta a busca forçada (§§ 2º e 3º do art. 245, CPP), não cria deveres de entrega dos objetos. E na hipótese de buscas executadas em sedes de empresas, não haveria ônus a seus representantes caso as autoridades não encontrassem os objetos buscados. Requisições coercitivas por força de multa, no entanto, *baseiam-se em deveres de colaboração inexistentes na lei*, já que a obrigação pela execução da medida é transferida àquele a quem se endereça a requisição. Além disso, requisições dessa natureza geram atritos jurídicos dos quais essas normas não cuidam. Não estão disciplinados os pressupostos autorizadores da requisição, as hipóteses de conflitos em seu cumprimento, o prazo para esse cumprimento, a natureza dos dados a serem entregues, os deveres em relação aos indivíduos afetados diretamente pela requisição etc., a fim de que o requisitado pudesse analisar a sua legalidade.

Aliás, parece evidente que, fosse esse ofício dirigido a um particular no lugar de uma empresa, dificilmente alguém cogitaria dizer que se trata de uma medida de busca e muito menos apontar como seu fundamento os dispositivos dos arts. 240 ss., CPP. *Quem requisita não precisa buscar*. Por isso, a medida de requisição, em muitos cenários, pode ser mais gravosa do que a busca forçada. Um indivíduo, por exemplo, que saiba não estar em posse do objeto buscado abrirá sua casa diante da leitura do mandado judicial, acompanhará a medida e, terminada esta, ver-se-á livre de quaisquer outros deveres. A Consulente, por sua vez, precisou vir à última instância do Poder Judiciário para tentar livrar-se dos deveres que lhe foram impostos. Isso é argumento suficiente para demonstrar que *dever de tolerância não é o mesmo que dever de colaboração*. Medida de busca, portanto, não se confunde com medida de requisição.

Além disso, sabem todos que muitas empresas de tecnologia do porte da Consulente operam globalmente e, assim, armazenam dados em diferentes jurisdições. Por isso, ordens de busca de dados, muitas vezes, precisam ser realizadas pelos

mecanismos próprios da cooperação internacional.[87] Nessas hipóteses, requisitar a entrega dos dados seria uma forma de contornar ilegitimamente esses mecanismos e as legislações aplicáveis, inclusive as relativas à proteção de dados no âmbito das transferências internacionais de dados e cooperação internacional.[88] Não há dúvida de que é mais fácil forçar a colaboração das empresas do que proceder pelas vias próprias. No entanto, isso parece reforçar ainda mais o argumento.

É claro que o legislador prevê hipóteses de colaboração de empresas por meio de requisições.[89] E a existência de previsão faz toda a diferença. Se a empresa souber, de antemão, que está obrigada pela legislação do território a entregar certos dados mediante requisição, ela pode optar, por exemplo, por encerrar suas operações no respectivo território (sobram exemplos disso pelo mundo), ou por informar seus clientes/usuários a respeito (o que é obrigação legal em vários ordenamentos), ou até mesmo por deixar de produzir determinados dados (o que é perfeitamente legítimo como modelo de negócio[90]). Isso tudo, porém, é inviável na ausência de determinação legal clara, já que a empresa, nesse caso, acaba sendo surpreendida por uma medida que não sabia ser juridicamente possível.

Portanto, autorizar a requisição de dados *como se busca fosse* também configuraria analogia. E, em matéria de intervenções em direitos fundamentais, como visto, isso significa violação do princípio da reserva de lei, que protege *todas* as cláusulas de direitos fundamentais (art. 5º, II, CF).

---

[87] WOHLERS, GRECO, *Systematischer Kommentar...*, § 94, Rn. 26; aprofundando, METZ, Martin, SPITTKA, Jan. Datenweitergabe im transatlantischen Rechtsraum – Konflikt oder Konsistenz? *ZD*, 2017, p. 361.

[88] Cf., ilustrativamente, ABREU, Jacqueline de Souza. Proteção da privacidade e cooperação jurídica internacional. In. CRUZ, Francisco Brito. SIMÃO, Bárbara. *Direitos fundamentais e processo-penal na era digital*: teoria e prática em debate. Internetlab, 2021, *passim*.

[89] Sobre a diferença entre normas autorizativas e normas de competência/atribuição, que não autorizam intervenções em direitos fundamentais, vis-à-vis aos arts. 129, I e VIII, e 144, § 5º, CF, e ao art. 6º do CPP, cf. ESTELLITA, O RE 1.055.941..., p. 611-612, com ulteriores referências.

[90] MOURA, BARBOSA, Dados digitais..., p. 495.

C. QUESITO 2: PROPORCIONALIDADE DA MEDIDA CONCRETA

Os representantes da Consulente nos dirigiram questão adicional: a requisição de dados de pesquisa seria, neste caso específico, materialmente constitucional? Em outras palavras: a requisição dirigida à Consulente conforma-se aos requisitos de proporcionalidade aplicáveis a intervenções em direitos fundamentais?

A dificuldade para responder a essa questão decorre diretamente do tópico anterior (B). Afinal, a exigência de proporcionalidade, enquanto requisito material de justificação para intervenções em direito individuais fundamentais, pressupõe que os requisitos formais de justificação estejam satisfeitos: a existência de lei formal expressamente autorizativa. Como tal lei inexiste, todo o exame terá de ser realizado a título meramente *hipotético*, ou seja, supondo haver uma norma autorizativa, aprovada pelo Parlamento, para medidas como a busca reversa aqui examinada.

O juízo de proporcionalidade diz respeito a uma relação entre meios e fins.[91] O fim perseguido pelo Estado no caso em análise é o de *elucidação de uma suspeita de cometimento de crime*. O meio empregado para realizar o fim é uma medida de tratamento de dados, a saber, o *compartilhamento compulsório de dados de usuários de uma aplicação de buscas na internet*. Há que se verificar, portanto, se o compartilhamento de dados dos usuários é um meio proporcional em face do fim que se pretende alcançar.

O procedimento amplamente reconhecido para verificar a justificação material divide-se em três passos: examinar a idoneidade, a necessidade e a proporcionalidade em sentido estrito. É o que faremos adiante, não sem antes tecer breves considerações sobre a falta de fundamentação da ordem judicial que determinou o compartilhamento dos dados.

[91] Sobre o princípio de proporcionalidade aplicado a medidas de tratamento de dados, cf. GLEIZER, MONTENEGRO, VIANA, *O direito de proteção...*, p. 49 e ss.

I. Falta de fundamentação concreta da medida

A decisão limitou-se à seguinte consideração para deferir todas as mais de 40 medidas de intervenção em direitos fundamentais (cf. acima A):

> "Compulsando os autos, tenho que se encontram íntegros os motivos a ensejarem o deferimento do pedido ora apresentado, eis que imprescindível para a linha de investigação adotada, bem como pelo fato de que não há outro meio viável a permitir o avanço da instrução criminal.
>
> Assim, conclui-se que as medidas ora pleiteadas são providências que se impõem, pois indispensáveis para se chegar a todos aqueles que, de alguma forma, possam ter participação no crime que se apura, bem como das circunstâncias em que se desenvolveu o fato criminoso.
>
> Pelo exposto, DEFIRO a QUEBRA DE SIGILO DE DADOS TELEFÔNICOS, ESPELHAMENTO DE MENSAGENS, QUEBRA DE SIGILO DE DADOS TELEMÁTICOS E INTERCEPTAÇÃO TELEFÔNICA." (fl. 1375; desta mesma fl. até a de nr. 1382 elenca-se dezenas de intervenções em direitos fundamentais de pessoas conhecidas e desconhecidas[92]).

As inúmeras razões que fundamentam a nulidade da decisão não podem ser abordadas neste Parecer sem que sejam sacrificadas outras que merecem maior atenção. Assim, basta demonstrar a inexistência tanto de motivação, como de fundamentação legal.

Sob o aspecto da motivação, a decisão, por sua vaguidão, serve (como de fato serviu no caso concreto) para qualquer outro caso ou requerimento. Afinal, em qualquer investigação e para qualquer medida investigativa pode-se dizer que "as medidas ora pleiteadas são providências que se impõem, pois indispensáveis para se chegar a todos aqueles que, de alguma forma, possam ter participação no crime que se apura, bem como das circunstâncias em que se desenvolveu o fato criminoso". Tudo o que diz a decisão pode ser aplicado a qualquer outro inquérito. Como todas as medidas

[92] Ilustrativamente: obtenção de e-mails atrelados a linhas celulares; dados cadastrais de celulares que tenham mantido contato com outros; extratos de contas de linhas; histórico de chamadas; interrupção de fluxo de dados via internet e aplicativos de mensagens instantâneas a critério da autoridade policial; informação, em tempo real, dos locais de onde os terminais interceptados estão sendo utilizados no momento da transmissão e recebimento de dados bem como de seus interlocutores; acesso aos serviços de localização por GPS a critério e pelo período que a autoridade policial determinar; identificação de todos usuários de certa rede social que acessaram certas páginas em um período de sete dias etc.

interventivas em direitos fundamentais exigem proporcionalidade para sua admissibilidade, em qualquer caso, face a qualquer sujeito de direito e em relação a qualquer medida restritiva, pode-se dizer que esta é "imprescindível para a linha de investigação adotada, bem como pelo fato de que não há outro meio viável a permitir o avanço da instrução criminal [sic]". E, paradoxalmente, a melhor prova de que havia outros meios para permitir o avanço da investigação é dada pela própria decisão que, como dito, contém mais de 40 determinações de intervenção em direitos fundamentais. Por que não seria suficiente, neste momento, a quebra de sigilo telefônico ali mesmo determinada? Por que todas as medidas precisam ser realizadas a um só tempo e não sucessivamente? Quais são os motivos concretos que justificariam pelo menos as medidas mais invasivas? Há suspeitas, por exemplo, de que mandantes do crime tenham realizado pesquisas pelo Google a partir daqueles parâmetros? Não se trata de capricho: a resposta a essas perguntas é mandatória frente àqueles que terão seus direitos sacrificados em prol da investigação.

Neste caso, no entanto, a decisão seria aprovada no *teste de falta de motivação* elaborado pelo Min. Sepúlveda Pertence: "a melhor prova da ausência de motivação de um julgado é que a frase enunciada, a pretexto de fundamentá-lo, sirva, por sua vaguidão, para a decisão de qualquer outro caso".[93] Pela mesma razão não sobreviveria ao que determina o art. 315, § 2º, CPP (na redação dada pela Lei n. 13.964/2019), que prescreve que qualquer decisão judicial não se considerará fundamentada quando se limitar à paráfrase de ato normativo sem explicitar sua relação com a causa (inc. I), ou não explicar o motivo concreto da incidência no caso de conceitos jurídicos indeterminados (inc. II), ou quando indicar "motivos que se prestariam a justificar qualquer outra decisão" (inc. III).

[93] HC 76.258, DJU 24/04/1998, p. 04, grifamos. *Gomes Filho*, em publicação clássica sobre o tema, qualifica este tipo de proceder como motivação aparente, o que, segundo ele, "equivale a dizer inexistente" (GOMES FILHO, Antonio Magalhães. *A motivação das decisões penais*. Revista dos Tribunais, 2001, p. 186).

O desinteresse pelo disposto no art. 93, IX, CF, se manifesta também na redação incorreta do nome de uma das vítimas, a Vereadora Marielle Franco[94], apontado como parâmetro para a requisição determinada. Por fim, como a medida ora analisada foi decretada pela primeira vez precisamente na decisão que a autorizou, não a socorre nem sequer a sugestão de motivação *per relationem* feita neste trecho: "tenho que se encontram íntegros os motivos a ensejarem o deferimento do pedido ora apresentado", pois inexistia decisão anterior determinando a medida aqui analisada.

Sob o aspecto da fundamentação legal da decisão, o vício é equivalente. Considere-se apenas que os requisitos legais para as dezenas de quebras são diversos quanto se trata dos dados protegidos pela LIT, ou quando se trata de dados protegidos pelo MCI (cf. acima item B).[95]

Se o juízo de proporcionalidade é, como dito, um juízo de relação entre dois polos, um deles inexiste no caso sob exame, o que dificulta ou até mesmo impede sua análise. Contudo, dada a gravidade da intervenção autorizada pelo juízo de piso, cumpre fazer as considerações que sejam possíveis sobre os elementos do juízo de proporcionalidade da medida.

II. Idoneidade: das particularidades do armazenamento de dados da Pesquisa do Google

Idoneidade significa que o meio escolhido é apto a promover o fim em questão. Para aferir se a medida em análise é idônea, é necessário, antes, conhecer com mais detalhes o sistema da Pesquisa do Google, tendo em vista que os investigadores requisitam a identificação dos IP's ou dos Device ID's que tenham se utilizado do Google Busca (seja por meio do aplicativo ou sua versão web) no período compreendido entre

[94] Foram assim redigidos: "'MARIELE FRANCO' [sic], 'VEREADORA MARIELE' [sic], 'AGENDA VEREADORA MARIELE' [sic]". É verdade que o sistema de Pesquisa do Google também retornaria os resultados para o nome grafado errado, todavia, esses resultados seriam parcialmente diferentes caso o nome tivesse sido grafado da forma correta.

[95] A Procuradoria-Geral da República, em sua manifestação nos autos do RE, segue, na essência, esse mesmo entendimento ao requerer a devolução do feito ao tribunal de origem para avaliar a necessidade e a subsidiariedade da medida (p. 106 do Parecer).

os dias 10/03/2018 e 14/03/2018, para realizar consultas com os seguintes parâmetros de pesquisa: 'Mariele Franco' (sic); 'Vereadora Mariele' (sic); 'Agenda Vereadora Mariele' (sic); 'Casa das Pretas'; 'Rua dos Inválidos, 122' ou 'Rua dos Inválidos'.

Concentrando-se tão somente em seus aspectos probatórios, é inquestionável que a requisição de dados pessoais contribuiria, no máximo, para a revelação de dados que a Consulente tem armazenados. E aqui residem problemas ainda não abordados.

Qualquer computador conectado à internet pode acessar sites com distintas funcionalidades, ou seja, aplicações de internet – para usar a linguagem do MCI –, como o google.com. Google.com é um site de buscas que, como outros do mesmo gênero, tem como serviço "encontrar o que seu usuário busca na internet". Entretanto, isso não significa que o Google sempre conhece o usuário de sua ferramenta de busca.

Todos os computadores conectados à internet possuem um endereço de IP. Os dispositivos móveis também possuem o *Device-ID*, um código que identifica usuários móveis, permitindo acompanhar dispositivos individuais. Por meio desses endereços, os computadores, incluindo os smartphones, transformam-se em terminais que enviam e recebem informações (digitais, porque na forma de dígitos 1 e 0).

O mesmo ocorre, por exemplo, em consulta à biblioteca do STF. No endereço «http://portal.stf.jus.br/textos/verTexto.asp?servico=bibliotecaConsultaAcervoStf» (que, por definição, também é uma aplicação de internet), ao clicar no botão "pesquisar", o usuário receberá dados que o redirecionam a outro servidor de busca, desta vez alocado no site do Senado Federal. Nesse servidor, ele dará comandos (inserindo palavras de pesquisa) a partir de seu endereço de IP e, neste mesmo endereço de IP, receberá os dados que buscou. Nessa aplicação, o usuário pode fazer a busca por palavras (tema, autor, título, ano etc.) para encontrar livros, artigos etc. Tudo o que essas aplicações de internet deverão reter, com relação a esse acesso, serão os dados relativos à data e ao horário da consulta e o endereço de IP do computador e ou do dispositivo que as acessou.

A fim de melhorar a experiência dos usuários, aplicações de internet costumam permitir que seus clientes realizem um cadastro pessoal no próprio site. Por

meio desse cadastro, que no caso do Google é chamado de Conta Google, o usuário pode se identificar (por log-in) e, assim, o Google passará a fornecer seus serviços não apenas ao IP "X", mas também ao usuário "Y". Dessa forma, conhecendo os dados fornecidos pela pessoa que faz as buscas, o Google pode personalizar o serviço e, seguindo no exemplo anterior, a biblioteca pode oferecer outras funcionalidades como a indicação de obras similares às já pesquisadas. Por isso, certos serviços que demandam personalização só podem ser fornecidos a quem faz o log-in na aplicação.

No entanto, o Google não tem como compelir seus usuários a esse registro pessoal feito por log-in, que é, por isso, *opcional*. Qualquer um pode fazer pesquisas no buscador do Google sem se identificar pessoalmente. Isso tem consequências importantes.

Em primeiro lugar, a empresa só poderia oferecer, a princípio, informações sobre as pesquisas por determinados parâmetros, caso essas buscas tenham sido realizadas por usuários que tenham se identificado antes de usar a ferramenta de buscas (log-in, usuários logados). Ou seja, apenas os usuários do Google que o utilizaram de maneira identificada – o que, provavelmente, excluiria criminosos profissionais ou pessoas minimamente preocupadas em não deixar rastros – teriam suas buscas reveladas. Isso porque os dados de pesquisa ficam armazenados nos "Históricos de Pesquisa" da conta de um usuário identificado/logado. Quem não estava logado no momento da pesquisa não seria atingido pela medida, pois sua informação não seria armazenada.

Em segundo lugar, os usuários que se identificam ao Google, ou seja, aqueles que estão logados ao fazer a pesquisa, também têm o direito de optar pelo não armazenamento do "Histórico de Pesquisa" ou pela eliminação desses dados a qualquer tempo, inclusive de maneira automatizada. O sistema o faz de forma imediata e sem possibilidade de reversão.[96] É importante relembrar que não há um dever legal de guarda de informações sobre o *uso* da aplicação (ou seja, dados de conteúdo; cf. acima B.II.1.a.),

[96] Todas estas informações estão disponíveis nesta página: https://support.google.com/websearch/answer/6096136?hl=pt-BR&co=GENIE.Platform%3DAndroid#zippy=%2Cexcluir-o-histórico-de-pesquisa-automaticamente.

e que um dever nesses moldes equivaleria, por exemplo, a obrigar as prestadoras de serviços de telecomunicação a gravar e armazenar todas as conversas telefônicas ocorridas; uma medida de severa afetação a direitos fundamentais que seria impensável em regimes constitucionais democráticos. Por isso, a existência de dados de conteúdo sobre as buscas (uso do aplicativo) e o armazenamento desses dados dependem do tipo de atividade do usuário (logado ou não) e da possibilidade efetiva de eliminação a qualquer tempo de tais informações. Por essas razões, o conjunto de dados que seria entregue aos investigadores conteria apenas os resultados armazenados pelo usuário e que não tenham sido excluídos por ele posteriormente. Por isso, os dados ali armazenados seriam, provavelmente, de pessoas que não estavam preocupadas em esconder vestígios de sua participação em um crime tão chocante.

E, neste ponto, cumpre chamar a atenção para o risco de que esse grande volume de dados pudesse ficar sujeito a riscos de tratamento não autorizado, por erro ou mesmo por má-fé. São notórios os recorrentes vazamentos de dados sob controle de autoridades públicas brasileiras. Além disso, como visto, inexiste lei dispondo sobre medida, o que quer dizer que não há dispositivos sobre acautelamento/segurança da informação, eliminação dos dados desnecessários, controle de finalidade do tratamento etc., em sentido diametralmente oposto às diretrizes das legislações protetivas de dados pessoais que determinam sua minimização, o controle de finalidade e a adoção de medidas de segurança (cf. art. 6º, LGPD).

Por esses aspectos, parece claro que a decisão recorrida troca a privacidade de muitas pessoas insuspeitas por um resultado duvidoso: a efetivação de uma medida possivelmente inidônea.

III. Necessidade

Necessidade, no sentido aqui empregado, significa que não há meios menos gravosos e de igual eficiência à disposição do Estado para realizar um fim determinado. Em outras palavras, o meio é necessário se não houver outro, com a mesma eficácia, que implique menor restrição ao direito atingido. No direito de proteção de dados, essa

exigência material de constitucionalidade concretiza-se, por exemplo, nos princípios gerais de minimização dos dados e limitação temporal (cf. p. ex. art. 6°, III, LGPD; art. 5°, 1, c, Regulamento Geral de Proteção de Dados europeu).[97]

Quanto a este elemento do juízo de proporcionalidade, a decisão peca pela falta de fundamentação (cf. logo acima, item I), a despeito do caráter extremamente invasivo das medidas que determina, de modo que não há elementos suficientes para aferir as razões que levaram à requisição dos dados de pesquisa. O que há são elementos que infirmam sua necessidade.

Eles decorrem da contextualização da medida de busca reversa ordenada entre as demais que foram objeto da ordem judicial, as quais, apesar de não serem objeto deste parecer, têm de ser consideradas para fins de análise da requisição aqui examinada. Em termos gerais, a decisão defere pedidos de "quebra de sigilo de dados telefônicos, espelhamento de mensagens, quebra de sigilo de dados telemáticos e interceptação telefônica". Concretamente, isso significa, contudo, um catálogo de mais de 40 (!) medidas, envolvendo requisições de dados de toda sorte.

Dentre elas, vale ressaltar, em especial, que o mandado judicial expedido ao Google Inc. para "quebra de sigilo de dados telemáticos" abrangia a questionável determinação de identificação dos Device IDs com todos os endereços de IP vinculados a aparelhos celulares de pessoas que transitaram no polígono em que se deu o crime, no horário correspondente. Partindo dessas informações de localização, a decisão determina a devassa dos dados referentes aos aparelhos celulares identificados, muitos deles, dados de conteúdo (aplicativos baixados, compras efetuadas, contatos na agenda, fotos, histórico de localização, backup de aplicativos de trocas de mensagens, dentre outros).[98]

---

[97] Cf., em mais detalhes, GLEIZER, MONTENEGRO, VIANA, *O direito de proteção...*, p. 64.

[98] Uma outra questão, que não é objeto de nossa análise nesta oportunidade, é a relativa à constitucionalidade do acesso aos dados de geolocalização por falta de norma autorizativa. Não obstante, o fato de que foi determinada juntamente com o acesso aos dados de busca já é suficiente para demonstrar a falta de necessidade desta última medida.

Ainda que se pudesse aceitar a validade de uma determinação de fornecimento dos dados com base em coordenadas geográficas, por exemplo, não é compreensível por que os dados referentes à ferramenta de busca seriam também necessários. Afinal, o compartilhamento dos dados de localização no polígono do crime poderia até constituir uma medida menos gravosa, já que dizem respeito ao trânsito de pessoas em um espaço público. O acesso a dados da Pesquisa do Google, por sua vez, tem potencial de atingir aspectos mais íntimos da personalidade, pois a busca é algo que em regra se faz de forma solitária e revela propensões, interesses, hábitos, desejos e traços fundamentais da personalidade do usuário (cf. abaixo item IV, 2). Esta última medida, portanto, é mais gravosa até mesmo do que a requisição de dados de localização e, além disso, menos eficiente. Essa preocupação de escalonamento, de forma a autorizar primeiro as medidas menos graves, para só então, se necessário, autorizar as mais graves, a decisão também não apresenta.

Em suma, há boas razões para refutar a necessidade da medida: o fato de uma medida dessa gravidade inserir-se dentre outras quarenta denota, como dito, que, no melhor dos cenários, ela poderia ter sido deixada para momento ulterior, após exauridas as demais.

IV. Proporcionalidade em sentido estrito

Por fim, o juízo acerca da proporcionalidade em sentido estrito (exigibilidade ou adequação) pressupõe que a gravidade da intervenção estatal e os interesses comuns perseguidos estejam em uma relação equilibrada: uma exigência de ponderação justa entre gravidade da intervenção e interesses perseguidos.[99] Os critérios para essa ponderação são notoriamente problemáticos, e uma discussão aprofundada sobre esse

[99] Cf., HUFEN, *Staatsrecht*..., p. 117. Cf. ainda, BERNAL PULIDO, Carlos B. *El principio de proporcionalidad y los derechos fundamentales.* 4 ed. Universidad Externado de Colombia, 2014, p. 874 e ss; BONAVIDES, Paulo. *Curso de direito constitucional.* 33 ed. Malheiros, 2018, p. 405 e ss.; GUERRA FILHO, Willis Santiago. *Processo constitucional e direitos fundamentais*. 4. ed., 2005, p. 91 e ss.

problema extrapolaria os limites deste Parecer. Há, no entanto, pelo menos dois aspectos da medida decretada que evidenciam sua desproporcionalidade.

1. O problema da circunvenção e da vigilância irrestrita

Um desses aspectos diz respeito ao problema da circunvenção e da vigilância irrestrita. "Circunvenção" seria o correspondente literal em português para um conceito frequente na doutrina processualista penal alemã (*Umgehung*).[100] O conceito é empregado para designar um artifício que consiste em contornar os limites legais, evitando-os. Esse conceito pode ser muito esclarecedor no caso sob exame, pois a medida determinada conduz, em última análise, a uma circunvenção das normas legais vigentes para medidas de investigação no processo penal.

A medida de busca reversa determinada consiste na requisição de dados de pesquisa de usuários do aplicativo de buscas do Google, sendo uma dentre as muitas informações requisitadas a provedores de aplicativos pela ordem judicial. A decisão utiliza, para isso, a rubrica "quebra do sigilo de dados telemáticos" e submete o descumprimento da requisição ao pagamento de multa, além de ressaltar a possível incursão em crime de desobediência (art. 330 CP). A rubrica não imprime sentido técnico no âmbito do processo penal, porque não há uma medida genérica que autorize a quebra de qualquer dado telemático, senão várias medidas autorizadas de forma específica. Posta nesses termos, a ordem judicial pressupõe que uma requisição desses dados a provedores de conexão e de aplicativos é uma medida à disposição das autoridades de persecução penal. Uma prova disso é que foram requisitados não somente os dados de busca do Google, mas também, e sob ameaça de multa, dados de usuários do Facebook, Whatsapp e Waze. Requisições dessa natureza dirigem-se assim, em princípio, a qualquer empresa provedora de aplicações e têm por objeto potencialmente qualquer dado.

Considerando que aplicações de internet são cada vez mais utilizadas e estendem-se a vários aspectos da vida, indo de *streaming* de músicas até a procura de

[100] Sobre a opção pela tradução como "circunvenção", cf. GRECO, Luís. Introdução..., p. 28.

parceiros para relacionamentos íntimos, o acesso fácil a esses dados por meio de simples requisição judicial faz com que os órgãos de investigação nem sequer precisem recorrer a medidas estabelecidas em lei, para as quais há limites mais claros, evitando-as, portanto. Assim, por exemplo, se os órgãos de investigação precisam ter acesso a determinados e-mails ou a dados armazenados em uma nuvem, não é necessário realizar busca e apreensão, atendendo a seus requisitos legais, para ter acesso a um aparelho celular e, por esse meio, aos dados que interessam, senão que é suficiente requisitar às respectivas empresas, sob pena de multa, as informações desejadas. Também o acesso a conversas em aplicativos de trocas de mensagens não precisaria estar submetido a exigências comparáveis com o que vale para a interceptação telefônica, pois bastaria requisitar à empresa o envio de tais mensagens. Isso não é possível graças a barreiras técnicas erigidas pelas próprias empresas (p. ex. criptografia de ponta a ponta), a fim de proteger a privacidade de seus usuários. Todavia, em princípio, seria possível requisitar tais informações com base numa simples "quebra de sigilo telemático", sem que para isso houvesse uma autorização legal fixando os pressupostos e limites da medida.

O problema da circunvenção é, na verdade, uma decorrência de um problema anterior e mais grave: o de que a possibilidade de requisição e posterior cruzamento de dados colhidos por aplicativos implique que os órgãos de persecução penal tenham acesso praticamente irrestrito a dados pessoais dos cidadãos. Como já mencionado algumas vezes ao longo deste parecer, vive-se hoje uma transposição de boa parte da vida das pessoas para meios digitais conectados à internet. A quantidade de dados pessoais produzidos e armazenados pelos diversos aplicativos não tem precedente histórico. Paralelamente, técnicas e instrumentos estatísticos de análise e processamento de dados (*big data*) têm hoje um potencial assustadoramente preciso de revelar padrões de comportamento e traços de personalidade (perfilização).

É imprescindível que o desenvolvimento tecnológico seja acompanhado por um equivalente desenvolvimento jurídico, sem o qual o titular dos dados pessoais fica completamente desprotegido e a noção de privacidade torna-se, a rigor, inviável. No regime geral de proteção de dados, a proteção à personalidade e à privacidade exige

que o tratamento de dados seja fortemente lastreado nas hipóteses legais. Do mesmo modo, é fundamental que haja regras para o tratamento de dados no âmbito da persecução penal.[101] Supor que as autoridades de investigação, por meio de simples requisição de informações, possam não só ter acesso aos dados pessoais de usuários de todo e qualquer aplicativo, mas também livremente cruzar esses dados com outros e extrair disso inferências adicionais, significaria que os órgãos de persecução penal, dotados de enorme potencial ofensivo para os cidadãos, gozam de possibilidades praticamente irrestritas de coleta e processamento de dados, vedadas em outros setores. Não seria exagero afirmar que esse cenário flerta francamente com um Estado de vigilância total.

Como se vê, a circunvenção das autorizações legais existentes abre as portas para atividades de investigação não submetidas a quaisquer limites, qualitativos ou quantitativos, permitindo o exercício de vigilância estatal irrestrita.

2. A predominante afetação de insuspeitos e o efeito inibitório

a) O desproporcional alcance da medida

Por fim, um outro aspecto também revela a desproporcionalidade *stricto sensu* da medida: a *ampla afetação de insuspeitos*.

Suspeito e insuspeito são termos técnicos da teoria processual penal.[102] Diferentemente da pena, medidas interventivas no âmbito da investigação não podem ser autorizadas apenas contra os responsáveis por um crime, já que elas têm por objetivo, exatamente, descobrir quem são esses responsáveis.[103] Por isso, "o que fundamenta a possibilidade de um indivíduo ser penalmente investigado/processado é o *grau de*

[101] Para os fundamentos dessa regulação, com alguns exemplos e sugestões retirados do direito alemão, cf. GLEIZER, MONTENEGRO, VIANA, *O direito de proteção...*, p. 105 e ss.

[102] Com mais profundidade, GLEIZER, MONTENEGRO, VIANA, *O direito de proteção...*, p. 107 e ss.

[103] Ibid., p. 112 e ss.

suspeita que recai sobre ele".[104] "Não por outra razão, é natural que também o nível das intervenções que o indivíduo deva suportar esteja em direta relação com esse grau de suspeita".[105]

Portanto, o grau de suspeita é um essencial contraponto ao grau interventivo de certas medidas. No direito alemão, por exemplo, que dá muita importância a esse equilíbrio, medidas mais invasivas estão limitadas a um rol específico de pessoas que podem ser afetadas. Por exemplo, para a infiltração online,[106] uma espécie de busca remota por infiltração em sistemas informáticos, que tem um alto caráter invasivo, há expressa determinação de que a medida, em princípio, só pode ser dirigida contra o suspeito (§100b, Abs. 3, S. 1, StPO). Isso significa que ela só pode se voltar contra insuspeitos caso seja possível assumir, com base em fatos concretos, que o suspeito utiliza sistemas informáticos de outra pessoa e que a realização da intervenção apenas nos sistemas informáticos do suspeito não possibilita a investigação dos fatos ou do local onde se encontra um coinvestigado (§100b, Abs. 3, S. 2, StPO). Mas isso não impede que insuspeitos possam, circunstancialmente, ser atingidos de forma mediata pela medida (100b, Abs. 3, S. 3, StPO) como, por exemplo, caso seus dados estejam no dispositivo informático do suspeito. No entanto, em regra, todas essas pessoas terão de ser notificadas, em um prazo legalmente estabelecido, de que foram afetadas pela medida (§101, Abs. 4, Nr. 4, StPO).

Também no direito brasileiro, bem como em todos os lugares onde valha o imperativo de proporcionalidade, é forçoso afirmar o mesmo: medidas devem, em princípio, dirigir-se somente contra suspeitos. E isso deve valer sobretudo para medidas altamente invasivas à privacidade como a requisição de dados de pesquisa, que permitem a obtenção de informações íntimas, que são produzidas por meio de atividades muito semelhantes ao pensamento.

---

[104] Ibid., idem.

[105] Ibid., idem.

[106] GRECO, GLEIZER, A infiltração online..., p. 1485 e ss. [1486].

Cahn/Humell dão nota dos mesmos incômodos no direito americano:

> "With a keyword search, police demand a list of every single user who has searched for a specific search term or 'keyword'. Rather than returning information for a single person suspected of a crime, *keyword warrants provide information on hundreds, thousands, or even millions of users, even though the vast majority of those identified will likely be completely innocent*. Even worse, the *judges who sign these orders do not know how many users* will be caught up in the search at the time they approve them. They cannot because it is the keyword search itself that tells police how many individuals searched for a specific name, address, or product. (…) Trial court magistrates have already approved these invasive searches, but many hope they will be found unconstitutional by higher courts. Notably, *keyword search warrants fail the particularity requirement found in the U.S. Constitution's Fourth Amendment*. This is because police cannot particularly describe probable cause for treating each google user who searched for an address as a suspect. Quite the opposite, *they know that the vast majority of people who make such searches will have no connection to the crime*".[107]

A medida, embora assuma aqui uma nova roupagem, continua sendo a boa e velha prática de *fishing expedition*, "que, em bom português, significa investigar jogando rede de arrastão, sem alvos definidos"[108] e, no Brasil, está vedada.[109] Ela seria comparável a eventual ordem judicial dirigida a instituição bancária com determinação para que esta identificasse, pelos extratos bancários, clientes que eventualmente tenham realizado certas compras ou feito certos pagamentos em determinados estabelecimentos;[110] ou ainda com um mandado de busca que autorizasse a entrada em

---

[107] CAHN, Albert Fox. HUMELL, Amanda. A Disturbing New Police Tactic Harnesses the Full Tracking Power of 'Big Tech'. Disponível em: https://verfassungsblog.de/keyword-warrants/. Acesso em: 12 jan. 2022.

[108] ESTELLITA, GLEIZER, A investigação penal de insuspeitos.

[109] STF, RE 1.055.941, Tribunal Pleno, Rel. Min. Dias Toffoli, DJe 18/03/2021, p. 41 do voto, proferido em 20/11/2019: "Não é possível a geração de RIF por encomenda - os chamados internacionalmente *fishing expeditions* - contra cidadãos relativamente aos quais não haja alerta emitido de ofício pela unidade de inteligência nem procedimento investigativo formal estabelecido pelas autoridades competentes".

[110] STF, Inq-AgR 2245/MG, Tribunal Pleno, Rel. Min. Joaquim Barbosa, Relatora do acórdão Min. Cármen Lúcia, DJe 09/11/2007: "2. Configura-se ilegítima a quebra de sigilo bancário de listagem genérica, com nomes de pessoas não relacionados diretamente com as investigações (art. 5º, inc. X, da Constituição da República). 3. Ressalva da possibilidade de o Ministério Público Federal formular pedido específico, sobre pessoas identificadas, definindo e justificando com exatidão a sua pretensão. 4. Agravo provido parcialmente".

qualquer casa de uma determinada favela em busca de um objeto.[111] Ou seja, uma medida de investigação que atinge necessária e predominantemente pessoas insuspeitas. Necessariamente, porque não se pode supor que, em extensas listas de usuários que pesquisaram pelos parâmetros oferecidos, todos seriam suspeitos do crime. Predominantemente, porque se pode supor que as mesmas extensas listas apresentarão (muito) mais resultados de pessoas insuspeitas do que de pessoas suspeitas. Vale mencionar que os parâmetros potencializam isso, pois incluem o nome de uma rua e o nome de uma personalidade política. Além disso, a janela temporal compreende algumas horas seguintes à morte da vítima, sendo de se esperar que nesse intervalo o interesse na busca de informação sobre a vereadora tenha aumentado exponencialmente.

b) O efeito inibitório da medida

Além da ampla afetação de insuspeitos, há uma última consideração, baseada no efeito inibitório da medida, que põe em questão a sua proporcionalidade. Embora a noção de efeito inibitório (ou *chilling effect*) tenha sua origem no direito norte-americano, sua importância na justificação de intervenções em direitos fundamentais, como se verá, tem sido reconhecida pelo Supremo Tribunal Federal e cumpre ser empregada para avaliar a proporcionalidade da medida em análise.

Nos EUA, o efeito inibitório é afirmado quando "indivíduos que procuram exercer uma atividade protegida pela Primeira Emenda [garantia da liberdade de expressão] são dissuadidos disso por força de uma regulamentação governamental não especificamente dirigida a essa atividade protegida", explica *Schauer*.[112] Isso pode ocorrer "sempre que qualquer atividade protegida pela Constituição é indevidamente

[111] STJ, AgRg no HC 435.934, Sexta Turma, Rel. Min. Sebastião Reis Jr., DJe 20/11/2019, caso da determinação de busca e apreensão coletiva.

[112] SCHAUER, Frederick. Fear, Risk and the First Amendment: Unraveling the Chilling Effect. *Boston University Law Review*, v. 58, p. 685–732, 1978, p. 693. A referência a não ser "diretamente exigida" deriva do fato de que, se for diretamente dirigida, basta arguir a violação direta do direito fundamental (idem).

desencorajada".[113] É o que sucede, por exemplo, quando uma lei, pretendendo coibir a publicação de notícias falsas difamatórias, acaba por inibir a expressão de verdades ou opiniões,[114] ou, como no presente caso, quando uma decisão, pretendendo investigar um crime, acaba por inibir o ato de informar-se com liberdade.[115]

O efeito inibitório pode se referir ao exercício de outros direitos fundamentais, mas no direito americano, ele é particularmente ligado à garantia da liberdade de expressão.[116] Com medo de serem investigados ou punidos, os indivíduos não só deixam de fazer aquilo que têm direito de fazer, mas também aquilo que *devem* (em um sentido político) fazer; ou seja, há, com isso, não só um dano de caráter individual decorrente do não exercício de um direito fundamental, mas também um de caráter social, uma vez que a proteção do direito à liberdade de expressão, na forma de liberdade de se informar, assenta-se na premissa de que a livre troca de informações e a crítica são virtudes positivas e peças fundamentais em sistemas democráticos.[117] Numa democracia, há um interesse geral em que os indivíduos se informem e "a falta de controles suficientes sobre a obtenção, por parte do governo, de extensos registros sobre como as pessoas navegam na web, os livros e revistas que leem e os vídeos ou canais de televisão que escutam pode comprometer esse interesse".[118]

O STF reconheceu, e em mais de uma oportunidade, que o *chilling effect* pode ocasionar grave restrição à liberdade de manifestação do pensamento (art. 5º, IV, e

---

[113] Ibid., p. 690.

[114] Ibid., p. 693.

[115] "If anything has a chilling effect on people's exercise of their First Amendment rights, it is this provision: when we think that the government will invade our privacy just because we have spoken freely, or read a book that a government agent views as suspicious, then we will refrain from these activities. We will begin to fear our government-that it might misinterpret a book we have read and, like Orwell's Big Brother, punish us for exercising our constitutional right to ideological freedom. The missing probable cause standard allows searches that the Fourth Amendment is intended to prevent" (MARTIN, Kathryn. The USA Patriot Acts Application to library Patron Records. *Journal of Legislation,* vol. 29, n. 2, pp. 283-306, 2013, p. 297).

[116] SCHAUER, Fear, Risk…, p. 691.

[117] SCHAUER, Fear, Risk…, p. 693.

[118] SOLOVE, Daniel J. Digital Dossiers and the Dissipation of Fourth Amendment Privacy. *Southern California Law Review*. v. 75, pp. 1084–1167, 2002, p. 1104, tradução livre.

220, CF), à liberdade do direito de reunião (art. 5º, XVI) e à liberdade de ensinar e ao pluralismo de ideias (CF, art. 206, II e III, CF). Por seu Plenário, em duas oportunidades, a Corte afirmou a desproporcionalidade de lei que buscava limitar o conteúdo do ensino (Casos do Programa Escola Livre). Nestas oportunidades, foram justamente a incerteza (pela generalidade das normas) e a comparação entre os danos que motivaram as declarações de inconstitucionalidade. Em outro caso, o Plenário considerou o efeito inibitório sobre o exercício da liberdade de reunião, ponderando que "a mera insegurança decorrente da ameaça de sofrer sanções constitui, em si mesma, efeito inibitório (*chilling effect*) prejudicial ao pleno exercício legítimo do direito fundamental de livre reunião. É que a simples imposição de penalidades, tenham elas natureza civil, administrativa ou penal, em razão da participação ou organização de protestos tem um efeito deletério estrutural ao refrear, inibir o indivíduo de recorrer, no futuro, à liberdade a ele assegurada pela Constituição para reivindicar direitos e se fazer ouvir".[119]

Finalmente, também em mais de uma oportunidade, a Corte considerou o efeito inibitório no que tange ao exercício da liberdade de expressão. Assim, em seu voto na ADI 5.527 (Caso do Bloqueio do Whatsapp), a Min. Rosa Weber considerou que "integra o pleno exercício das liberdades de expressão e de comunicação a capacidade das pessoas de escolherem livremente as informações que pretendem compartilhar, as ideias que pretendem discutir, o estilo de linguagem empregado e o meio de comunicação. O conhecimento de que a comunicação é monitorada por terceiros interfere em todos esses elementos componentes da liberdade de informação: os cidadãos podem mudar o modo de se expressar ou até mesmo absterem-se de falar sobre certos assuntos, no que a doutrina designa por efeito inibitório (chilling effect) sobre a liberdade de expressão. (...) As consequências da ausência dessa precondição em uma sociedade vão desde a desconfiança em relação às instituições sociais, à apatia generalizada e a debilitação da vida intelectual, fazendo de um ambiente em que as

[119] STF, ADI 5.852, Tribunal Pleno, Min. Rel. Dias Toffoli, Min. Redator para o acórdão Min. Luiz Fux, DJe 26/11/2020, p. 87-88.

atividades de comunicação ocorrem de modo inibido ou tímido, por si só, uma grave restrição à liberdade de expressão".[120]

O caso mais recente, o Caso dos Dossiês (ADPF 722), nos remete, lamentavelmente, à confirmação da máxima de que autoridades públicas tendem ao abuso de poder, sendo uma forma de manifestação desse abuso a perniciosa reunião de informações sobre determinadas pessoas,[121] criando um efeito inibitório do engajamento social em atividades democráticas, como adverte Solove: "o perigo dessas iniciativas de coleta de informações não é apenas o de inibir a expressão ou ameaçar o protesto lícito, mas também o de tornar as pessoas mais vulneráveis, expondo-as a potenciais perigos futuros, tais como vazamentos, falhas de segurança e prisões indevidas".[122]

Nesse caso, enfrentado no âmbito da decisão sobre a medida cautelar na ADPF 722, a Min. Rosa Weber tomou o efeito inibitório como base de sua argumentação: "a mera insegurança decorrente do conhecimento de que se está sendo monitorado, bem como a da ameaça de sofrer sanções, constitui, em si mesma, efeito inibitório (*chilling effect*) prejudicial ao pleno exercício legítimo dos direitos fundamentais de livre manifestação do pensamento, expressão, reunião e associação: os cidadãos podem mudar o modo de se expressar ou até mesmo absterem-se de falar sobre certos assuntos. É que a simples imposição de penalidades, tenham elas natureza civil, administrativa ou penal, em razão do exercício do direito tem um efeito deletério estrutural ao refrear, inibir o indivíduo de recorrer, no futuro à liberdade a ele assegurada pela Constituição para reivindicar direitos e se fazer ouvir".[123] O voto foi acompanhado pelo Min. Luiz Fux (p. 98 do acórdão) e pelo Min. Gilmar Mendes que, considerando a liberdade de expressão um

---

[120] STF, ADI 5527, Rel. Min. Rosa Weber, j. 27/05/2020, voto da Min. Relatora, p. 10. Cf. decisões no mesmo sentido nos USA em SOLOVE, Digital Dossiers…, p. 1103.

[121] Sobre esse tipo de abuso no ambiente do FBI, por mais de cinquenta anos, sob a direção de J. Edgar Hoover, cf. SOLOVE, Digital Dossiers..., p. 1084–1167, *passim,* valendo destacar esta afirmação: "Indeed, historically, totalitarian governments have developed elaborate systems for collecting data about people's private lives" (p. 1102).

[122] Ibid., p. 1108, tradução livre.

[123] STF, ADPF 722, Tribunal Pleno, Min. Rel. Cármen Lúcia, DJe 22/10/2020, voto Min. Rosa Weber, p. 93. A cautelar foi mantida no julgamento final da arguição em 16/05/2022, DJe 09/06/2022.

pilar do sistema democrático (art. 5º, IV e 220, CF; p. 110 do acórdão), observou que "essa atuação estatal indevida também tem um efeito pernicioso sobre a sociedade como um todo, a partir do momento em que gera desestímulos ao debate de ideais contrárias àquelas defendidas pelo governantes, caracterizando o denominado efeito dissuasório ou '*chilling effect*'" (p. 117 do acórdão). Rememorou, ainda, o voto do Min. Celso de Mello na ADPF 187 (Caso da Marcha da Maconha), quem, citando memoriais do IBCCRIM, ressaltou que esse efeito gera um "comportamento obsequioso", "um pernicioso efeito dissuasório" que culmina, "progressivamente, com a aniquilação do próprio ato individual de reflexão".[124]

Aplicadas à requisição de dados de pesquisa, as considerações sobre efeito inibitório levantam sérias dúvidas sobre a constitucionalidade da medida. Como visto, as aplicações de busca (Pesquisa do Google, Yahoo, Bing, Ask, Wikipedia, DuckDuckGo etc.) podem revelar tanto ou mais sobre a privacidade e mesmo a intimidade de seus usuários do que as telecomunicações.[125] Em primeiro lugar, porque as buscas, em geral, são atividades que não envolvem terceiros. Em segundo, porque, por sua própria natureza, as buscas representam, atualmente, quase uma extensão do pensamento humano: na era da informação, o indivíduo dificilmente memoriza todo o conhecimento produzido e passa a utilizar-se das informações disponíveis na internet para se orientar em diversas situações do seu cotidiano. Isso significa que as pessoas não apenas usam com maior frequência aplicações de busca, mas também que as usam sem qualquer restrição temática e sem maiores reflexões. Como disse *Kerr*: "*In the digital age, we think*

[124] STF, ADPF 187, Tribunal Pleno, Min. Rel. Celso de Mello, DJe 29/05/2014, p. 83.

[125] Um "banco de dados de intenções", nas palavras de John Battelle, *apud*: TENE, Omer, What Google Knows: Privacy and Internet Search Engines, Utah Law Review, v. 4, 2008, p. 1435. "One's search history eerily resembles a metaphorical X-ray photo of one's thoughts, beliefs, fears, and hopes. It is ripe with information that is financial, professional, political, sexual, and medical in nature. (…) Data contained search-query logs may be far more embarrassing and privacy intrusive than that of the contents of e-mail correspondences or telephone calls", ibid., p. 1442-1443. Muito embora esse artigo tenha sido escrito num ambiente diverso de proteção de privacidade e de dados pessoais e sob uma outra política de proteção de dados por parte da Consulente, suas conclusões gerais sobre retenção de dados de conteúdo permanecem válidas.

and therefore we Google".[126] Aplicações de busca na internet são usadas, hoje, inclusive para consultas a temas sexuais, religiosos, existenciais, étnicos etc., consultas essas que, aliás, podem produzir dados pessoais considerados sensíveis pela LGPD (art. 5º, II, LGPD).[127]

A decisão analisada neste Parecer dá bom testemunho disso, pois tem potencial para atingir dados sensíveis referentes à opinião política dos alvos da medida (termos: VEREADORA MARIELE [sic] e AGENDA VEREADORA MARIELE [sic]), bem como sobre sua possível origem racial e étnica (CASA DAS PRETAS). As pessoas que utilizaram a Pesquisa do Google com a combinação de palavras VEREADORA MARIELE, por exemplo, poderiam estar fazendo uma pesquisa para um trabalho escolar, querendo saber mais sobre o partido da vereadora, reunindo material para uma matéria jornalística, ou buscando mais informações sobre sua atuação política, seja por interesses eleitorais ou mesmo por reprovação ao seu trabalho; elas poderiam estar, também, em busca de informações sobre o Carnaval de rua no Rio de Janeiro, sobre a localização geográfica de um endereço (Rua dos Inválidos) ou interessadas em um movimento social (Casa das Pretas). Acessadas por essas razões, a ninguém interessa o conteúdo de todas essas buscas, mas elas poderão servir como fundamento de uma suspeita penal. Da mesma forma, uma pessoa interessada nos crimes nazistas pode, por exemplo, deparar-se com a obra *Mein Kampf* e consultá-la e, embora isso nada diga sobre suas preferências políticas, essa informação pode ser mal interpretada a ponto de ser usada como prova de afinidade com a ideologia nazista, pondera *Martin*.[128]

Como todas essas pessoas veem-se, agora, na iminência de serem investigadas como possíveis mandantes de um homicídio que chocou o país, decisões como a analisada neste Parecer têm um elevado e perigoso potencial inibitório, pois as

---

[126] KERR, Orin. Implementing Carpenter. In: The Digital Fourth Amendment. Oxford University Press, (forthcoming), p. 46 (Disponível em: https://ssrn.com/abstract=3301257). Cf. TENE, What Google Knows…, p. 1433.

[127] Sobre as espécies de dados retidos por aplicativos das mais diversas naturezas e o caráter particularmente íntimo de vários deles, cf. TOKSON, Matthew, The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, Harvard Law Review, v. 135, p. 1790–1852, 2022, p. 1849.

[128] MARTIN, The USA Patriot Acts…, p. 290.

pessoas que hoje usam maciçamente a Pesquisa do Google (ou mesmo outras aplicações de busca) como porta de entrada para suas pesquisas poderão ver-se desestimuladas a fazê-lo e terão, no mínimo, que refletir detidamente antes de suas buscas.[129] Por isso, as aplicações de busca demandam uma alta expectativa de proteção constitucional, de forma que o indivíduo não tenha receios de buscar por informações das mais diversas naturezas.

A decisão deliberada de não respeitar os pressupostos estritos para intervenção em direitos informacionais significará que muitas pessoas passarão a sentir-se forçadas a refletir sobre atividades que, por decisão firmada no pacto constitucional, deveriam praticar sem receios: pesquisas, pagamentos, leituras ou pedidos online. Se qualquer informação puder ser obtida processualmente por meio de uma medida tão simples como a requisição dirigida contra à Consulente, que não se submete a pressupostos rigorosos, que contorna a lei e que ainda pode alcançar pessoas insuspeitas, quem poderia, conscientemente, viver sem receios?

Pense-se, apenas para arrematar, que afirmada a legalidade da medida, ela poderá ser utilizada em outros casos, com muito menos visibilidade e controle público ou por parte dos titulares de dados afetados. Isso aumentaria exponencialmente o risco de monitoramento de cidadãos pelo Estado, especialmente em face de instituições de controle fragilizadas e tendências políticas autoritárias, basta lembrar as práticas denunciadas no âmbito da ADPF 722 (Caso dos Dossiês), apreciada pelo Supremo Tribunal Federal.

---

[129] "All of us have surely searched for something on the Internet. And we take our phones wherever we go. But doing these everyday activities can put us under suspicion by law enforcement officers using specific types of digital dragnet warrants known as reverse warrants." Dragnet Warrants are Trapping Innocent People, New York Civil Liberties Union, Disponível em: https://www.nyclu.org/en/news/dragnet-warrants-are-trapping-innocent-people. Acesso em: 10 dez. 2021 (itálico nosso). E nem todos o farão: "Technologies that are avoidable for most people are often unavoidable for others, including the disabled, the poor, and other disadvantaged populations"(TOKSON, The Aftermath of Carpenter…, p. 1849), especialmente em países como o nosso, com disparidades grotescas de acesso à educação e tecnologia entre as diversas camadas sociais.

Portanto, se "os direitos que as pessoas têm off-line devem também ser protegidos online",[130] há que se dar a máxima expressão à liberdade de informar-se, garantindo sua prática de forma desinibida também no ambiente online.

D. RESPOSTA ANALÍTICA AOS QUESITOS

Às indagações feitas pela Consulente devem ser dadas as seguintes respostas:

Quesito 1: A requisição de dados do Google Busca acima referida está autorizada por lei?

Premissa fundamental e incontornável para que se possa responder adequadamente ao primeiro quesito é reconhecer a reserva de lei como uma limitação a restrições de direitos individuais. Afinal, o direito de proteção de dados adquiriu status constitucional no Brasil, primeiro por força da jurisprudência constitucional e, mais recentemente, em razão da EC n. 115/2022. Estando os dados pessoais protegidos por cláusulas de direitos individuais (autodeterminação informacional, sigilo postal, sigilo das telecomunicações etc.), seu tratamento, especialmente para fins de persecução penal, exige fundamento em lei que determine com clareza os pressupostos e o alcance das medidas (arts. 5º, II, e 68, § 1º, II, CF). Em outras palavras, medidas de tratamento de dados estão submetidas à reserva de lei. Disso decorrem duas implicações importantes. A primeira delas é o rigoroso limite imposto à possibilidade de interpretação analógica; do contrário, a própria noção de reserva de lei perderia o sentido, já que a inexistência de lei sempre poderia ser substituída por uma interpretação analógica. A segunda implicação é a de que a diferença entre "dados estáticos" e "dados dinâmicos" não serve para justificar um tratamento de dados sem base legal, pois o regime de proteção de dados de base constitucional abrange todo e qualquer dado pessoal.

[130] STF, ADPF 403, voto Min. Edson Fachin, p. 59.

Uma vez que a LGPD exclui a persecução penal de seu âmbito de aplicação (art. 4º, III, d), a requisição de dados utilizados na Pesquisa do Google teria de ter fundamento legal em outras normas que autorizem medidas de investigação de natureza penal. Possíveis candidatos seriam os arts. 22 e 23, c.c. o art. 10, § 1º, do MCI, bem como a Lei 9.296/96 ou as normas do CPP que autorizam a busca e apreensão (arts. 240 ss.). Nenhuma dessas normas, contudo, autoriza a requisição de dados sob análise.

O MCI parte de uma importante distinção, cujas origens podem ser reconduzidas ao direito europeu, entre dados cadastrais, registro de conexão/registros de acesso a aplicações de internet e dados de conteúdo. Os arts. 22 e 23, c.c. o art. 10, § 1º, autorizam a retenção e o compartilhamento apenas dos registros de conexão e registros de acesso a aplicações de internet. O diploma legal também autoriza a possibilidade de requisição dos dados cadastrais (art. 10, § 3º). Não há autorização, contudo, para a requisição de dados de conteúdo. Isso é compatível com o sentido que orienta a regulação da requisição judicial de registros MCI. Afinal, o objetivo dessas normas é evitar que a internet, em razão da anonimidade que propicia, se transforme em um "espaço livre de direito", permitindo identificar autores de ilícitos – p. ex. uma injúria praticada no Facebook – praticados no ambiente virtual. A requisição dos dados de busca, no entanto, não se amolda às exigências legais, pois não se restringe a metadados, senão que alcança dados de conteúdo, a saber, as próprias pesquisas. A bem dizer, ela desvirtua o sentido das normas de requisição judicial, pois transforma normas que servem precipuamente para identificar autores de conteúdos ilícitos publicados na internet em um instrumento geral de investigação com imenso potencial invasivo.

Também a LIT não oferece um fundamento legal para a medida. Os dados de busca não são oriundos de processo de telecomunicação, tampouco estão em fluxo. E a LIT autoriza expressamente uma medida de interceptação telefônica, que pressupõe, pelo menos, duas pessoas naturais se comunicando à distância.

Por fim, o fundamento para a requisição não pode ser encontrado nas normas referentes à busca e apreensão (arts. 240 ss., CPP). Essas normas não criam um dever de colaboração, mas apenas um dever de tolerar as buscas. Requisições coercitivas por força

de multa, no entanto, baseiam-se em deveres de colaboração inexistentes na lei, já que a obrigação de execução da medida é transferida àquele a quem se endereça a requisição. Em suma, a aplicação tanto da LIT quanto dos arts. 240 ss., CPP, configuraria uma analogia que contraria a reserva de lei.

A resposta a esse quesito, portanto, é negativa. Ela é uma decorrência de princípios básicos da teoria jurídica dos direitos fundamentais e de sua aplicação às normas que autorizam medidas investigativas no processo penal brasileiro, que não preveem a possibilidade de requisição de dados da Pesquisa do Google.

Quesito 2: A medida conforma-se aos requisitos constitucionais de proporcionalidade aplicáveis às intervenções em direitos fundamentais?

Se uma medida de tratamento de dados não está autorizada por lei, a questão em torno de sua proporcionalidade está prejudicada. Toda ação estatal de intervenção deve ser proporcional, mas isso não significa que uma ação interventiva proporcional possa superar a exigência de lei. A proporcionalidade pressupõe a reserva de lei, nunca a substitui.

No entanto, a resposta a esse quesito se afigura necessária por razões de cautela, uma vez que, no caso analisado, em inobservância à exigência de reserva de lei, a medida foi "fundamentada" em argumentos de natureza subsidiária, como a proporcionalidade. Por essa razão, é conveniente também apresentar argumentos de forma hipotética, a fim de evidenciar que, mesmo que a medida estivesse autorizada em nosso ordenamento, ela seria desproporcional no caso concreto.

A medida foi autorizada sem motivação, nem fundamentação judicial. A ausência de fundamentação judicial é um argumento em si. Mas, neste caso, também gera problemas de desproporcionalidade, já que os alvos da intervenção sofrem-na sem qualquer justificativa.

Além disso, a medida encerra sérios problemas quanto à sua *idoneidade* e *necessidade*. Ela não tem a capacidade de auxiliar, de fato, a investigação e é provável que termine afetando apenas pessoas sem qualquer envolvimento no crime.

Quanto à *idoneidade*, pode ser que os autores (executores ou mandantes) do crime nem sequer tenham realizado pesquisas no Google com as palavras indicadas na decisão combatida. Se isso ocorreu, não se tem notícia nos autos. Além disso, se, porventura, realizaram tais pesquisas, podem ter excluído esses dados posteriormente. A empresa não tem obrigação legal de armazenar essa espécie de dados e deve eliminá-los, caso os usuários optem por excluí-los (art. 7°, I, LGPD). Não bastasse, a entrega dos dados como requisitados na ordem judicial recorrida não representaria muito em termos investigativos, porque seria necessário revelar a identidade física de cada usuário por trás de cada um dos endereços de IP contidos em uma extensa lista, para dar o próximo passo: separar os suspeitos dos insuspeitos. Também é importante relembrar que o nome da vítima tem grafia incorreta no mandado, não sendo possível saber se essa foi uma estratégia deliberada dos investigadores – por exemplo, caso tenham tido informações de que os autores do crime redigiam de forma errada o nome da vereadora –, ou se foi uma falha. De qualquer forma, deve-se considerar que a busca por palavras com grafias incorretas apresentará resultados diferentes, o que poderia impactar na efetividade da medida.

A medida também não passa no crivo rigoroso da *subsidiariedade*, pois a decisão autoriza ao todo mais de 40 medidas, não sendo razoável que todas essas medidas tivessem que ser autorizadas ao mesmo tempo, e não de forma escalonada, tentando-se avançar paulatinamente pelas medidas menos graves até as mais graves. As medidas mais severas devem ser utilizadas por último. Essa é uma determinação lógica do imperativo constitucional de proporcionalidade.

A medida também é *desproporcional* por outras duas razões.

Em primeiro lugar, autorizar levantamento de dados pessoais por meio de simples requisições de compartilhamento de dados dirigido a empresas privadas seria uma forma de burlar – ou, como escrevemos anteriormente, de contornar – os

pressupostos e limites estabelecidos pelas normas autorizativas de intervenção em direitos fundamentais. Já não seria necessário que estivessem presentes os requisitos autorizadores da interceptação telefônica, por exemplo, caso fosse possível simplesmente obrigar, por meio de uma requisição *sui generis*, empresas prestadoras de serviços de telecomunicação a compartilharem os dados desejados.

Em segundo, medida atingiria – prática, predominante e massivamente – pessoas insuspeitas. *O grau de afetação de insuspeitos, aqui, é dificilmente comparável às outras desproporções apontadas. Ele atinge níveis preocupantes de invasão à privacidade, que, em última instância, podem abalar significativamente a sensação dos cidadãos de estarem protegidos da vigilância estatal, que é pressuposto básico para um desenvolvimento livre da personalidade humana*. Disso pode decorrer um efeito inibitório nefasto na utilização da internet pelas pessoas. E não é possível dizer que esse efeito atingiria apenas os malfeitores, porque, como melhor parafraseou Snowden:

> "Dizer que você não se importa com o direito à privacidade porque não tem nada a esconder equivale a afirmar que você não se importa com a liberdade de expressão porque não tem nada a dizer."[131]

A resposta a esse quesito, portanto, também é negativa. Ela decorre de critérios de proporcionalidade básicos e amplamente aceitos pela doutrina. A medida burlaria a sistemática processual penal, para autorizar artifício que, sobretudo por ser altamente invasivo à privacidade, demandaria autorização parlamentar. Ela estimularia *fishing expeditions* e afetaria a confiança geral na privacidade, com riscos reais de prejuízo ao Estado de Direito.

[131] Em tradução livre do original: "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say"(Edward Snowden, The Guardian, Inglaterra, 15.5.2015, acessível em: https://www.theguardian.com/us-news/video/2015/may/22/edward-snowden-rights-to-privacy-video).

Esse o nosso Parecer, salvo melhor juízo e nos limites da consulta e das informações que nos foram fornecidas.

São Paulo/Halle (Saale)/Zurique, 5 de dezembro de 2022.

Heloisa Estellita
OAB/SP n. 125.447

Lucas Montenegro
OAB/CE n. 44.334

Orlandino Gleizer
OAB/RJ n. 175.710

Sobre os autores:

HELOISA ESTELLITA

Professora da Escola de Direito de São Paulo da Fundação Getúlio Vargas. Doutora em Direito pela Faculdade de Direito da Universidade de São Paulo. Mestre em Direito pela Universidade Estadual Paulista. Estágios de pós-doutorado nas Faculdades de Direito da Ludwig-Maximilians-Universität München, Augsburg Universität e Humboldt Universität zu Berlin. Bolsista da Alexander von Humboldt Stiftung.

LUCAS MONTENEGRO

Docente-assistente na cátedra de Direito Penal, Filosofia e Teoria do Direito da Martin-Luther-Universität de Halle-Wittenberg. Doutorando em Direito pela Humboldt-Universität zu Berlin. LL.M. pela Georg-August-Universität de Göttingen.

ORLANDINO GLEIZER

Doutorando em Ciência do Direito na Universidade Humboldt de Berlim. LL.M pela Universität Augsburg. Mestre em Direito Penal pela Universidade do Estado do Rio de Janeiro (UERJ). Foi assistente de cátedra na Universidade Julius Maximiliam de Würzburg de 2016 a 2021.

** Os comentários e avaliações jurídicas expostas neste parecer são baseadas e se limitam às informações fornecidas pelos patronos da Consulente e/ou aos documentos por eles exibidos sob compromisso de veracidade. Qualquer discrepância entre essas informações e a realidade dos fatos torna imprestável este parecer e as consequências legais daí advindas são de exclusiva responsabilidade da Consulente. Os comentários apresentados neste documento não consideram ou preveem alterações futuras na legislação ou jurisprudência, nem mesmo alterações relevantes para o caso decorrentes de políticas administrativas ou normativas. O entendimento jurídico aqui imparcialmente exposto não vincula qualquer autoridade brasileira, de persecução penal, administrativa ou mesmo judicial, não havendo qualquer garantia de que haverá concordância com seu conteúdo.*