AÇÃO DIRETA DE INCONSTITUCIONALIDADE 5.059 DISTRITO FEDERAL

RELATOR	**: MIN. DIAS TOFFOLI**
REQTE.(S)	: ASSOCIAÇÃO NACIONAL DAS OPERADORAS CELULARES - ACEL
ADV.(A/S)	: RODRIGO DE BITTENCOURT MUDROVITSCH E OUTRO(A/S)
INTDO.(A/S)	: PRESIDENTE DA REPÚBLICA
PROC.(A/S)(ES)	: ADVOGADO-GERAL DA UNIÃO
INTDO.(A/S)	: PRESIDENTE DO CONGRESSO NACIONAL
PROC.(A/S)(ES)	: ADVOGADO-GERAL DA UNIÃO
AM. CURIAE.	: ASSOCIAÇÃO DOS DELEGADOS DE POLÍCIA DO BRASIL - ADEPOL
ADV.(A/S)	: WLADIMIR SÉRGIO REALE
AM. CURIAE.	: ADPF - ASSOCIAÇÃO NACIONAL DOS DELEGADOS DE POLÍCIA FEDERAL
ADV.(A/S)	: ANTONIO TORREAO BRAZ FILHO E OUTRO(A/S)
AM. CURIAE.	: ASSOCIAÇÃO DOS DELEGADOS DE POLÍCIA DO ESTADO DE SÃO PAULO - ADPESP
ADV.(A/S)	: DENISE OZÓRIO FABENE RODRIGUES

VOTO

O SENHOR MINISTRO DIAS TOFFOLI (RELATOR):

Discute-se, na presente ação direta, **se é constitucional ou não** o disposto no **§ 2º do art. 2º da Lei nº 12.830/13**, no qual se preconiza que, "[d]urante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos".

Alega a requerente, em síntese, que esse **poder genérico de requisição** permitiria ao delegado de polícia acessar, **independentemente de ordem judicial**, quaisquer dados relativos às comunicações telefônicas, o que importaria, a seu ver, em violação do sigilo das comunicações e dos direitos fundamentais à vida privada e à intimidade (CRFB/88, art. 5º, incisos X e XII).

Subsidiariamente, sustenta a requerente que **dependeriam de prévia autorização judicial** **(i)** a interceptação de voz; **(ii)** a interceptação

telemática e o acesso a: **(iii)** a localização de terminal ou IMEI de cidadão em tempo real por meio de ERB; **(iv)** o extrato de ERB; **(v)** os dados cadastrais de usuários de IP (ou seja, dados de usuários que em determinados **dia, data, hora e fuso** fizeram uso de um IP para acessar a internet); **(vi)** os dados cadastrais dos terminais fixos não figurantes em lista telefônica divulgável e de terminais móveis; **(vii)** o extrato de chamadas telefônicas; **(viii)** o extrato de mensagens de texto (SMS ou MMS); **(ix)** os serviços de agenda virtual ofertados por empresas de telefonia; e **(x)** os dados cadastrais de correio eletrônico (**e-mail**).

1. DA PRELIMINAR DE ILEGITIMIDADE ATIVA *AD CAUSAM* DA ACEL.

O Procurador-Geral da República, em sua primeira manifestação nos autos (e-doc. 39), suscitou a ilegitimidade ativa **ad causam** da **Associação Nacional das Operadoras de Celulares (ACEL)**, argumentando que o requerente não representa toda a classe dos prestadores de serviços de telecomunicações, mas apenas as operadoras de telefonia celular, e que não haveria pertinência temática entre as respectivas finalidades institucionais e o teor da norma impugnada.

Não prospera, contudo, a preliminar.

Como decidido pelo Ministro **Luiz Fux**, à época Relator do feito, **o requerente enquadra-se no conceito de entidade de classe de âmbito nacional** previsto no art. 103, inciso IX, da Constituição de 1988, e, portanto, **está autorizado a deflagrar o processo de controle abstrato de normas**, visto que,

> "**[p]rimeiro**, a proponente representa categoria delimitada de pessoas jurídicas integrantes do mesmo ramo de atividade (Serviço de Telefonia Móvel), pelo que descabe caracterizá-la como de composição heterogênea.
>
> Além do mais, não parece razoável, para a configuração da legitimidade ativa da requerente, exigir a presença de

associadas do ramo de telefonia fixa, cujos serviços envolvem atividades bastante distintas que, por sua própria natureza, não estão abrangidas pelas controvérsias jurídicas atinentes à norma objeto desta Ação Direta.

Segundo, a entidade em destaque abrange pessoas jurídicas da área de telecomunicações localizadas não apenas em determinados Estados ou regiões, mas com atuação em todo o território nacional. Neste sentido, a aplicação analógica da Lei Orgânica dos Partidos Políticos (Lei nº 9.096/95, art. 7º, § 1º) mostra-se plenamente atendida.

Terceiro, há pertinência temática entre os objetivos institucionais da associação e a pretensão deduzida na demanda. Para efeito de comprovação desta afirmação, transcrevem-se trechos do Estatuto Social da ACEL.

> 'Art. 3º A Acel tem como objeto: I - A promoção, entre suas Associadas, do intercâmbio de informações que visem o aprimoramento dos serviços por elas prestados e a defesa de seus interesses comuns; II - A representação dos interesses coletivos de suas Associadas perante instituições públicas ou privadas, nacionais ou estrangeiras, bem como junto aos Poderes Executivo, Legislativo e Judiciário — da União, dos Estados e dos Municípios — e outras entidades de qualquer forma relacionadas com os objetivos sociais e com os interesses comuns das Associadas, dependendo de prévia autorização da Diretoria Executiva; [...] VII - A instituição e a defesa de normas éticas e regulamentares que deverão nortear as atividades de suas Associadas.'

Assim, ainda que a norma impugnada trate especificamente sobre os poderes conferidos ao Delegado de Polícia durante a investigação criminal, o pedido formulado na petição inicial desta Ação de Controle encontra correlação com os objetivos institucionais da Associação requerente" (e-doc.

65).

Reafirmo as razões acima transcritas, sobretudo por estarem em perfeita harmonia com a jurisprudência da Corte, que, ao definir as balizas para que determinada entidade seja enquadrada na categoria de "entidade de classe de âmbito nacional", para fins de propositura de ações de controle de constitucionalidade, estabeleceu como requisitos: **(i)** a **delimitação subjetiva da associação**, que deve representar categoria delimitada ou delimitável de pessoas físicas ou jurídicas, **vedada a heterogeneidade de sua composição**; **(ii)** o **caráter nacional**, configurado pela presença de associados em ao menos nove estados da Federação; e, por fim, **(iii)** a **correlação temática** entre os objetivos institucionais da postulante e a norma objeto de sindicância. **Todos eles estão satisfeitos na hipótese dos autos**.

Observo, por último, que a legitimidade ativa da **Associação Nacional das Operadoras de Celulares (ACEL)** foi reconhecida pelo Supremo Tribunal Federal em diversas ocasiões (**v.g.**, ADI nº 7.498, Rel. Min. **Gilmar Mendes**, Tribunal Pleno, DJe de 5/6/24; ADI nº 7.413, Rel. Min. **Edson Fachin**, Tribunal Pleno, DJe de 22/11/23; ADI nº 7.321 Rel. Min. **Gilmar Mendes**, Tribunal Pleno, DJe de 4/8/23; ADI nº 6.326, Rel. Min. **Cármen Lúcia**, Tribunal Pleno, DJe de 3/12/20; ADI nº 6.087, Rel. Min. **Marco Aurélio**, Tribunal Pleno, DJe de 23/9/19; ADI nº 5.575, Rel. Min. **Luiz Fux**, Tribunal Pleno, DJe de 7/11/18; ADI nº 4.15-MC, Rel. Min. **Marco Aurélio**, DJe de 7/2/13; e ADI nº 3.846, Rel. Min. **Gilmar Mendes**, Tribunal Pleno, DJe de 15/3/11).

2. DO MÉRITO.

2.1 Da necessária delimitação da controvérsia.

O requerente solicita **(i) que o Tribunal declare a inconstitucionalidade parcial da norma impugnada**, **afastando** o poder

requisitório do delegado de polícia relativamente a serviços telefônicos; ou, subsidiariamente, **(ii) que o Tribunal confira interpretação conforme à Constituição da República de 1988 à norma impugnada, explicitando** os contornos e os limites desse poder, com a exclusão da possibilidade de "quebra de sigilo" sem a prévia deliberação judicial, conforme expressamente indicado na petição inicial.

Esse recorte inicial será levado em consideração para viabilizar a apreciação da presente controvérsia, dada a abrangência semântica da norma impugnada.

2.2 - Da adequada contextualização da controvérsia constitucional.

Nos quase doze anos transcorridos desde o ajuizamento da presente ação direta, verificou-se a obsolescência de algumas tecnologias, bem como o surgimento e a rápida popularização de outras. Entre as novidades, merece destaque o uso – **hoje, quase universal** – dos **smartphones**. Esses aparelhos oferecem aos usuários inúmeras funcionalidades, do acesso à internet ao compartilhamento, em tempo real, de fotos, áudios e vídeos.

Paralelamente, nota-se uma significativa evolução legislativa, começando pela edição do **Marco Civil da Internet** (Lei nº 12.965/14) e, na sequência, da **Lei Geral de Proteção de Dados** (Lei nº 13.709/18), sendo esses dois diplomas legais vocacionados, desde a concepção, a disciplinar a adjudicação de direitos fundamentais na internet. Mais recentemente, promulgou-se a **Emenda Constitucional nº 115/22**, por meio da qual se inseriu no rol do art. 5º da Constituição Federal "o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Também não se poderia deixar de mencionar, ainda que rapidamente, as inúmeras inovações legislativas pontuais, inclusive em matéria penal e processual penal – **algumas delas mencionadas no decorrer deste voto** –, e as dezenas de projetos de lei em tramitação no Congresso Nacional com os quais se busca uma regulação mais eficiente

dos fenômenos relacionados às novas tecnologias e aos serviços digitais, como é o caso da inteligência artificial e das redes sociais.

É nesse contexto de constante efervescência tecnológica e normativa que se desenvolve a discussão da matéria de fundo acerca da garantia constitucional do sigilo das comunicações e, ainda, dos contornos e limites dos direitos fundamentais à intimidade e à vida privada, em face da necessidade de uma persecução penal mais ágil e efetiva para fazer frente a novos riscos e à crescente criminalidade organizada.

2.3 Dos paradigmas de controle aplicáveis à espécie.

Invoca-se, no caso em apreço, como paradigma de controle de constitucionalidade **a inviolabilidade da vida privada, da intimidade**, e **do sigilo das comunicações**, a qual é consagrada pela Constituição Federal de 1988, em seu art. 5º, nos seguintes termos:

> "Art. 5º (...)
> (...)
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> (...)
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal."

A esse respeito, ensina o Professor **Tércio Sampaio Ferraz Júnior**, em artigo seminal, que, enquanto "[a] **privacidade**, como direito, tem por conteúdo a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio" e "a **intimidade** é o âmbito exclusivo que alguém reserva para si, sem nenhuma repercussão social", o **sigilo**

constituiria "um direito fundamental de negação", cujo objeto é "a faculdade de resistir ao devassamento", não sendo, pois, "um fim em si mesmo (...), mas instrumento fundamental cuja essência é a assessoriedade" (JÚNIOR, Tércio Sampaio Ferraz. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo, v. 88, p. 439-459, 1993).

Por conseguinte, como ressalta referido autor,

> "[a] inviolabilidade do sigilo, não sendo faculdade *exclusiva* da privacidade (é também da segurança da sociedade e do Estado), é *conditio sine qua non* (condição), mas não é *conditio per quam* (causa) do direito fundamental à privacidade. Ou seja, se não houver inviolabilidade do sigilo não há privacidade, mas se houver inviolabilidade do sigilo isto não significa que haja privacidade (pode haver outra coisa, como a segurança do Estado ou da sociedade)" (JÚNIOR, Tércio Sampaio Ferraz. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo, v. 88, p. 439-459, 1993 – grifo nosso).

Ensina **René Ariel Dotti**, por sua vez, que o **direito à vida privada** (ou o **direito à privacidade**, como se fala comumente) e o **direito à intimidade** são diferentes, apesar de, em muitas ocasiões, serem utilizados indistintamente, como sinônimos (DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação: possibilidades e limites**. São Paulo: Editora Revista dos Tribunais, 1980, p. 71). Segundo o autor, o direito à vida privada abrangeria, em síntese, "todos os aspectos que por qualquer razão não gostaríamos de ver cair no domínio público", ou seja, "tudo aquilo que não deve ser objeto do direito à informação nem da curiosidade da sociedade moderna", desdobrando-se em outros tantos direitos, como o direito à imagem; o direito ao nome; o direito ao

domicílio e à correspondência, o direito à honra e à reputação, e o direito à integridade física e moral. Seu conteúdo é móvel, razão pela qual nem a legislação nem a jurisprudência conseguiriam fornecer uma delimitação precisa desse direito.

Já a expressão **"direito à intimidade"** designaria um "bem jurídico" que "não pode ser considerado isoladamente, mas em referência a algo" (DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação: possibilidades e limites.** São Paulo: Editora Revista dos Tribunais, 1980, p. 71). Nessa esteira, nas palavras do Professor **Tércio Sampaio Ferraz Júnior**, seriam exemplos de direito à intimidade "o diário íntimo, o segredo sob juramento, as próprias convicções, as situações indevassáveis de pudor pessoal, o segredo íntimo cuja mínima publicidade constrange" (JÚNIOR, Tércio Sampaio Ferraz. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo, v. 88, p. 439-459, 1993).

Em contrapartida, como sintetizam **Ana Paula Ávila** e **André Woloszyn**, o sigilo é "**o segredo que não pode nem deve ser relevado**", relacionando-se com os "deveres de preservação e proteção contra a inviolabilidade", de modo que, "[e]m princípio, terceiros (**nem mesmo o poder público**) não podem ter acesso a esses dados sem o consentimento do indivíduo, que tem a prerrogativa de decidir sobre a sua exibição e uso" (AVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**, v. 4, n. 3, p. 167-200, 2019).

Feitos esses esclarecimentos indispensáveis, e considerando que nas ações de controle concentrado a causa de pedir é aberta, o que possibilita, segundo a jurisprudência da Corte, o confronto da norma contestada com dispositivo(s) constitucional(is) não mencionado(s) na petição inicial, **acrescento a esse rol o direito à proteção de dados pessoais, incluído no art. 5º, inciso LXXIX, pela Emenda Constitucional nº 115, de 2022**. De

acordo com esse preceito, "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

É certo que essa proteção sempre esteve implícita na Constituição Federal de 1988, mas não se pode olvidar que sua consagração expressa no catálogo de direitos fundamentais, como um direito autônomo, **reforça a relevância da adequada proteção dos dados pessoais na sociedade contemporânea**, se não como resultado de um processo gradual de reconhecimento, ao menos como uma releitura autêntica – porque empreendida pelo Poder Constituinte Derivado Reformador – dos direitos fundamentais.

Nesse sentido, cito **Ingo W. Sarlet**, que, em meados de 2020 – ou seja, dois anos antes da promulgação da EC nº 115/22 –, já preconizava a necessidade de se construir uma **dogmática constitucionalmente adequada do direito à proteção de dados no Brasil**, ocasião na qual esclareceu o seguinte:

> "À míngua, portanto, de expressa previsão de tal direito, pelo menos na condição de direito fundamental explicitamente autônomo, no texto da CF, e a exemplo do que ocorreu em outras ordens constitucionais, o direito à proteção dos dados pessoais pode (**e mesmo deve!**) ser associado e reconduzido a alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam — aqui nos termos da CF — os direitos à privacidade e à intimidade, no sentido que alguns também chamam de intimidade informática.
>
> Mas, possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade

> da pessoa humana e no direito geral de liberdade, o qual também assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana, que, de acordo com tradição jurídica já consolidada no direito constitucional estrangeiro e no direito internacional (universal e regional) dos direitos humanos, inclui o (**mas não se limita ao!**) direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa" (SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988. **Direitos Fundamentais & Justiça**, 2020).

Para referido autor,

> "na condição de direito implicitamente positivado e enquanto não aprovada e promulgada emenda constitucional (...) não se cuida de direito submetido (como no caso do sigilo das comunicações) à expressa reserva legal, mas a sua vinculação — ainda que não superposição integral — com os direitos à privacidade e intimidade sugere que se lhe dê proteção em princípio equivalente" (SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988. **Direitos Fundamentais & Justiça**, 2020).

No mesmo sentido vai o entendimento de **Danilo Doneda**, que, desde longa data, chama a atenção para "a dificuldade em tratar do tema da informação pessoal de forma diversa daquela binária – sigilo/abertura, público/privado – de forma que reflita a complexidade da matéria". Como explica esse autor,

> "[a] leitura das garantias constitucionais para os dados somente sob o prisma de sua comunicação e de sua eventual interceptação lastreia-se em uma interpretação que não chega

> abranger a complexidade do fenômeno da informação ao qual fizemos referência. Há um hiato que segrega a tutela da privacidade, esta constitucionalmente protegida, da tutela das informações pessoais em si – que, para corrente mencionada, gozaria de uma proteção mais tênue. E este hiato possibilita a perigosa interpretação que pode eximir o aplicador de considerar os casos nos quais uma pessoa é ofendida em sua privacidade – ou tem outros direitos fundamentais desrespeitados – não de forma direta, porém por meio da utilização abusiva de suas informações pessoais em bancos de dados" (DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico: Journal of Law**, v. 12, n. 2, p. 91-108, 2011).

Nessa linha, a inserção de um **direto à proteção de dados pessoais**, inclusive nos meios digitais, no rol dos direitos fundamentais, não deixa dúvidas a respeito da existência

> "[d]os assim chamados **limites aos limites à proteção de dados, entre os quais desponta a necessária observância dos critérios da proporcionalidade e da salvaguarda do núcleo essencial, o que se aplica seja qual for a origem e natureza da intervenção estatal (judiciária, administrativa e legislativa) na esfera de proteção do direito à proteção de dados**" (SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988. **Direitos Fundamentais & Justiça**, 2020 – grifo nosso).

Desse modo, a discussão delineada nos autos não está centrada na inviolabilidade do sigilo das comunicações (CF/88, art. 5º, inciso XII). Ela compreende também a inviolabilidade da vida privada e da intimidade (CF/88, art. 5º, inciso X) e, ainda, o novel "direito à proteção dos dados pessoais, inclusive nos meios digitais" (CF/88, art. 5º, inciso LXXIX, incluído pela EC nº 115, de 10/2/22).

2.4 Redefinindo a controvérsia constitucional.

Convém ressaltar, por último, que não se discute, nos autos, se o direito fundamental à inviolabilidade da vida privada, da intimidade, do sigilo das comunicações e dos dados pessoais digitais (CF/88, art. 5º, incisos X, XII e LXXIX) seria passível de limitação.

De acordo com a jurisprudência do Supremo Tribunal Federal, os direitos fundamentais não salvaguardam práticas ilícitas, inexistindo, portanto, direitos absolutos. Ademais, **o debate delineado na inicial parte exatamente dessas premissas**, concentrando-se, pois, na **averiguação de quais seriam os limites e os critérios necessários para a fiel observância dos preceitos constitucionais desafiados**.

Em outras palavras, questiona-se nos autos, especificamente, **se** e **em quais casos** seria indispensável a autorização judicial para se ter acesso a dados e metadados decorrentes das comunicações telefônica, informática e telemática, ou se, **ao revés**, tais dados poderiam ser acessados diretamente por autoridade policial, com fundamento em um poder genérico de requisição dos delegados de polícia.

2.5 Do poder requisitório do delegado de polícia quanto a dados produzidos por comunicação telefônica, informática ou telemática (ou relacionados a ela)

O poder requisitório do delegado de polícia, previsto no **art. 2º, § 2º, da Lei nº 12.830/13**, surge como **decorrência lógica das atribuições legais dessa autoridade** para instruir as investigações criminais e, ao fim e ao cabo, para conduzir o inquérito policial.

A propósito, dispõem os arts. 6º e 7º do Código de Processo Penal, **in verbis**:

"Art. 6º. Logo que tiver conhecimento da prática da

infração penal, a autoridade policial deverá:

I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais; (Redação dada pela Lei nº 8.862, de 28.3.1994)

II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; (Redação dada pela Lei nº 8.862, de 28.3.1994)

III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;

IV - ouvir o ofendido;

V - ouvir o indiciado, com observância, no que for aplicável, do disposto no Capítulo III do Título VII, deste Livro, devendo o respectivo termo ser assinado por duas testemunhas que lhe tenham ouvido a leitura;

VI - proceder a reconhecimento de pessoas e coisas e a acareações;

VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;

VIII - ordenar a identificação do indiciado pelo processo datiloscópico, se possível, e fazer juntar aos autos sua folha de antecedentes;

IX - averiguar a vida pregressa do indiciado, sob o ponto de vista individual, familiar e social, sua condição econômica, sua atitude e estado de ânimo antes e depois do crime e durante ele, e quaisquer outros elementos que contribuírem para a apreciação do seu temperamento e caráter.

X - colher informações sobre a existência de filhos, respectivas idades e se possuem alguma deficiência e o nome e o contato de eventual responsável pelos cuidados dos filhos, indicado pela pessoa presa. (Incluído pela Lei nº 13.257, de 2016).

Art. 7º. Para verificar a possibilidade de haver a infração sido praticada de determinado modo, a autoridade policial poderá proceder à reprodução simulada dos fatos, desde que esta não contrarie a moralidade ou a ordem pública."

Todavia, **não se pode admitir que o delegado de polícia tenha acesso irrestrito, ilimitado e/ou independentemente de prévia autorização judicial a toda e qualquer espécie de dados, sob pena de se franquear a essa autoridade acesso indiscriminado a dados sigilosos, ou a dados que, mesmo não revestidos desse atributo, devam gozar de uma proteção jurídica especial, seja porque consistem em dados pessoais cuja proteção deve obedecer ao disposto em lei específica, seja porque sua proteção é consectário lógico (e direto) da garantia da inviolabilidade da vida privada e da intimidade**.

Nesse sentir, ao comentar o dispositivo impugnado nestes autos, **Renato Brasileiro de Lima** ressalta que "o inquérito policial é conduzido de maneira discricionária pela autoridade policial, que deve determinar o rumo das diligências de acordo com as peculiaridades do caso concreto" (LIMA, Renato Brasileiro de. **Legislação criminal especial comentada**. 6. ed.rev., atual. e ampl., Salvador: Editora JusPodivm, 2018. p. 372). Porém, a esse respeito, explica o referido autor o seguinte:

> "**Discricionariedade implica liberdade de atuação nos limites traçados pela lei. Se a autoridade policial ultrapassa esses limites, sua atuação passa a ser arbitrária, ou seja, contrária à lei. Logo, não se permite ao Delegado de Polícia a adoção de diligências investigatórias contrárias à Constituição Federal e à legislação infraconstitucional**. Portanto, quando o art. 2º, § 2º, da Lei nº 12.830/13 dispõe que cabe ao delegado de polícia a requisição de perícia, informações documentos e dados que interessem à apuração dos fatos, há de se lembrar que certas diligências investigatórias demandam prévia autorização judicial, sujeitas que estão à denominada cláusula de reserva de jurisdição (**v.g.**, prisão temporária, mandado de busca domiciliar). Assim, apesar de o delegado de polícia ter discricionariedade para avaliar a necessidade de interceptação telefônica não poder fazê-lo sem autorização judicial. Nos

> mesmos moldes, por ocasião do interrogatório policial do investigado, deverá adverti-lo quanto ao direito ao silêncio (CF, art. 5º, LXIII)" (**ibidem**).

Ora, é fato notório que os serviços telefônicos, assim como os serviços informáticos e telemáticos, produzem (**ou possibilitam acesso a**) uma multiplicidade de dados (**inclusive a dados pessoais**) e, por isso, penso **não ser possível endossar a tese** de que o dispositivo legal em apreço franquearia aos delegados de polícia um poder genérico de requisição relativamente à integralidade desses dados e metadados.

Como já vimos, a norma em apreço atribui ao delegado de polícia um poder de requisitar perícias, documentos, dados e informações, de que essa autoridade pode lançar mão, **com discricionariedade**, para operacionalizar as investigações criminais e instruir os inquéritos policiais. Mas, repita-se, **conferir aos delegados o poder de, discricionariamente, requisitar perícias, documentos, dados e informações de interesse das investigações não significa autorizá-los a atuar de forma contrária à lei e ao direito para alcançar o fim pretendido**.

Assim, a meu ver, **a tese de que o delegado de polícia está autorizado pelo art. 2º, § 2º, da Lei nº 12.830/13 a acessar todo e qualquer tipo de dado relacionado às comunicações telefônicas ou de sistemas de informática ou telemática é tão equivocada quanto a tese de que o delegado de polícia estaria impedido, de modo absoluto, de acessar quaisquer desses dados e metadados discricionariamente**.

A seguir, examinarei separadamente as inúmeras formas de se acessarem dados e metadados produzidos por (ou decorrentes de) serviços telefônicos, informáticos e telemáticos, no intuito de averiguar, em cada caso, se seriam ou não passíveis de requisição direta pelo delegado de polícia.

(a) Interceptação das comunicações telefônicas (ou interceptação de voz).

Mesmo nestes autos, **há consenso quanto à necessidade de autorização judicial prévia para a interceptação das comunicações telefônicas** (também chamada de **interceptação de voz**), não só em razão do que preceitua expressamente o inciso XII do art. 5º da Constituição Federal, regulado pela Lei nº 9.296, de 1996, como também por força de jurisprudência consolidada sobre a matéria no âmbito do Supremo Tribunal Federal.

Apenas a título ilustrativo, recordo que o Supremo Tribunal Federal reafirmou, recentemente, o entendimento de que **a interceptação das comunicações telefônicas está condicionada à preexistência de uma ordem judicial específica, "expedida pelo juiz competente para a ação principal (...) que demonstre a conveniência e a indispensabilidade desse meio de prova**" (RE nº 625.263, Rel. Min. **Gilmar Mendes**, red. do ac. Min. **Alexandre de Moraes**, Tribunal Pleno, DJe de 3/6/22). A matéria se sujeita, assim, **a reserva jurisdicional**.

Por conseguinte, como ficou decidido na mesma ocasião, **são lícitas as sucessivas prorrogações das interceptações, desde que verificados os requisitos legais (art. 2º da Lei nº 9.296/96) e demonstradas, com elementos concretos, a necessidade de cada prorrogação e a complexidade da investigação**. Nesse sentido, **vide** o teor da tese de repercussão geral fixada no caso (Tema nº 661):

> "São lícitas as sucessivas renovações de interceptação telefônica, desde que, verificados os requisitos do artigo 2º da Lei nº 9.296/1996 e demonstrada a necessidade da medida diante de elementos concretos e a complexidade da investigação, **a decisão judicial inicial e as prorrogações sejam devidamente motivadas, com justificativa legítima, ainda que sucinta, a embasar a continuidade das investigações.** São ilegais as motivações padronizadas ou reproduções de modelos genéricos sem relação com o caso concreto" (RE nº 625.263, Rel. Min. **Gilmar Mendes**, red. do ac. Min. **Alexandre de Moraes**,

Tribunal Pleno, DJe de 3/6/22).

(b) Extratos de chamadas telefônicas

Especificamente quanto aos **extratos de chamadas telefônicas** (também denominados de **extratos de registros telefônicos**) – abrangendo dados sobre os **terminais de destino**, assim como **data, hora e duração das chamadas** realizadas a partir de certo terminal telefônico de origem –, a jurisprudência mais recente do Supremo Tribunal Federal vai no sentido de que

> "**o afastamento do sigilo de dados telefônicos somente poderá ser decretado, da mesma maneira que no tocante às comunicações telefônicas, nos termos da Lei nº 9.296/96 e sempre em caráter de absoluta excepcionalidade, quando o fato investigado constituir infração penal punida com reclusão e presente a imprescindibilidade desse meio de prova**, pois a citada lei vedou o afastamento da inviolabilidade constitucional quando não houver indícios razoáveis da autoria ou participação em infração penal ou a prova puder ser feita por outros meios disponíveis, **não podendo, em regra, ser a primeira providência investigatória realizada pela autoridade policial**" (RE nº 625.263, Rel. Min. **Gilmar Mendes**, red. do ac. Min. **Alexandre de Moraes**, Tribunal Pleno, DJe de 3/6/22).

Esse entendimento tem sido reafirmado pelas Turmas do STF, como se verifica no julgamento da **Pet nº 11.840-AgR-segundo**, Rel. Min. **Alexandre de Moraes**, cuja ementa transcrevo:

> "PENAL E PROCESSUAL PENAL. MEDIDAS CAUTELARES PREPARATÓRIAS. QUEBRA DE SIGILO DE DADOS E INTERCEPTAÇÃO DE COMUNICAÇÕES POSSÍVEL UTILIZAÇÃO IRREGULAR DO SISTEMA DE

> INTELIGÊNCIA DA ABIN PARA MONITORAMENTO DE DISPOSITIVOS MÓVEIS. EXCEPCIONALIDADE E IMPRESCINDIBILIDADE. REQUISITOS LEGAIS OBSERVADOS. AGRAVO REGIMENTAL A QUE SE NEGA PROVIMENTO. 1. **O afastamento do sigilo de dados telefônicos somente poderá ser decretado, da mesma maneira que no tocante às comunicações telefônicas, nos termos da Lei nº 9.296/96 e sempre em caráter de absoluta excepcionalidade, quando o fato investigado constituir infração penal punida com reclusão e presente a imprescindibilidade desse meio de prova.** 2. Inconsistências indicadas pela autoridade policial nos dados fornecidos e a real possibilidade de monitoramento indevido de autoridades públicas e outras pessoas de interesse. Necessidade de aprofundamento da investigação. 3. **Demonstração, mínima e razoável, de que a medida era imprescindível para a elucidação dos fatos.** 4. Presentes os requisitos legais e situação extraordinária verificada. 5. Inexistência de argumento minimamente apto a desconstituir os óbices apontados. 6. Agravo regimental a que se nega provimento" (Pet nº 11.840-AgR-segundo, Rel. Min. **Alexandre de Moraes**, Primeira Turma, julgado em 14/10/24, DJe de 18/10/24).

(c) Interceptação telemática

Também **depende de prévia autorização judicial a interceptação do fluxo de dados em sistemas de informática e telemática**. É o que se infere do disposto no art. 1º, parágrafo único, c/c o art. 2º da Lei nº 9.296/96:

> "Art. 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob

> segredo de justiça.
>
> **Parágrafo único. O disposto nesta lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática**.
>
> Art. 2º. Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
>
> I - não houver indícios razoáveis da autoria ou participação em infração penal;
>
> II - a prova puder ser feita por outros meios disponíveis;
>
> III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.
>
> Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada."

Nesse quadro, é possível concluir que **a lei brasileira admite a interceptação do fluxo de dados em sistemas informáticos e telemáticos, condicionando-a, porém, aos mesmos requisitos previstos para a interceptação da comunicação telefônica**, quais sejam: **(i)** ordem judicial expedida pelo juiz competente para a ação principal (ou **cláusula de reserva jurisdicional**); **(ii)** decisão devidamente fundamentada em que se demonstre, por meio de elementos concretos, a conveniência e a indispensabilidade desse meio de prova; **(iii)** finalidade exclusiva de produzir prova em investigação criminal ou instrução processual penal; e, por último, que **(vi)** apuração de crime a que se atribua pena de reclusão.

Como leciona **Guilherme de Souza Nucci**,

> "a comunicação estabelecida por meios ligados à informática **(computador)** e à telemática **(misto de computador com meios de comunicação)** não deixa de ser uma forma

> atualizada e moderna de comunicação telefônica. Por isso, se houver finalidade de apuração de crime, com autorização judicial, pensamos ser válida a interceptação da comunicação efetuada por esses meios (ex.: conversação captada através de **modem** ou em determinados sites próprios para isso)" (NUCCI, Guilherme de Souza. **Leis penais processuais penais comentadas**. 6. ed. São Paulo: RT, 2012. p. 372).

Luiz Flávio Gomes, por sua vez, acrescenta o seguinte:

> "[O] texto legal é legítimo, integralmente legítimo, e vale pelo que nele está escrito. Como vimos no número anterior (26), a Lei 9.296/96 tem incidência em qualquer forma de comunicação telefônica, assim como nas comunicações telemáticas (independentes do uso da telefonia). **A CF só exigiu (explicitamente) lei regulamentadora no que concerne às comunicações telefônicas, é verdade, mas isso não exprimia impedimento para que o legislador disciplinasse outras formas de comunicação. Cuidando-se de direito fundamental (sigilo das comunicações, intimidade), aliás, somente o legislador é que podia (e pode) restringi-lo**. (...) **uma inovação da Constituição foi estender a inviolabilidade aos 'dados'"** (GOMES, Luiz Flávio. **Interceptação telefônica:** Lei 9.296, de 24.07.96. São Paulo: RT, 1997. p. 173-174 – grifo nosso)**.**

Arremata o autor com o seguinte:

> "**Não vale, em suma, o argumento de que a CF só permitiu a restrição da comunicação telefônica. Quanto a ela, na verdade, existe autorização restritiva expressa. Quanto às comunicações telemáticas (independentes da telefonia), essa permissão é implícita ou imanente. Logo, podia o legislador discipliná-las. A rigor, devia mesmo discipliná-las.**
>
> Comunicações telefônicas, hoje, não podem significar só

> 'conversação' ou comunicação de voz. Isso valia para o tempo em que Graham Bell inventou o telefone (1876) ou para o tempo em que foi elaborado o Código Brasileiro de Telecomunicações (art. 4.°), em 1962. Não tem sentido nos dias atuais (v. supra itens 8 e 13)" (GOMES, Luiz Flávio. **Interceptação telefônica:** Lei 9.296, de 24.07.96. São Paulo: RT, 1997. p. 173-174 – grifo nosso).

A mesma linha de raciocínio é defendida por **Fernando Capez**. **Vide**:

> "**A Carta Magna, quando excepciona o princípio do sigilo na hipótese de 'comunicações telefônicas', não cometeria o descuido de permitir a interceptação somente no caso de conversação verbal por esse meio, isto é, quando usados dois aparelhos telefônicos, proibindo-a, quando pretendida com finalidade de investigação criminal e prova em processo penal, nas hipóteses mais modernas.** A exceção, quando menciona 'comunicações telefônicas', estende-se a qualquer forma de comunicação que empregue a via telefônica como meio, ainda que haja transferência de 'dados'. É o caso do uso do modem. **Se assim não fosse, bastaria, para burlar a permissão constitucional, 'digitar' e não falar'. (...) A circunstância de a CF expressamente só abrir exceção no caso da comunicação telefônica não significa que o legislador ordinário não possa permitir a interceptação na hipótese de transmissão de dados. Não há garantias constitucionais absolutas.** Se assim não fosse, o CP não poderia admitir a prática de homicídio em legítima defesa (arts. 23, II, e 25), uma vez que a Carta Magna garante a 'inviolabilidade do direito à vida' sem ressalva (art. 5 º , caput)' (...)" (CAPEZ, Fernando. **Curso de direito penal**: legislação penal especial. 9. ed. São Paulo: Saraiva, 2014. v. p. 471-472 – grifo nosso).

Para finalizar esse tópico, cito, em caráter exemplificativo, o **RHC nº**

132.115, **de minha relatoria**, em cujo julgamento a Segunda Turma do STF decidiu que

> "**a exceção constitucional ao sigilo alcança as comunicações de dados telemáticos**, não havendo que se cogitar de incompatibilidade do parágrafo único do art. 1º da Lei nº 9.296/96 com o art. 5º, inciso XII, da Constituição Federal" (RHC nº 132.115, **de minha relatoria**, Segunda Turma, julgado em 6/2/18, DJe de 19/10/18 – grifo nosso).

(d) Localização de terminal ou IMEI de um cidadão em tempo real e extrato de ERB

A Estação Rádio-Base (ou ERB) – comumente denominada **"antena de celular"** – permite a conexão da infraestrutura de telecomunicações com os telefones celulares existentes em sua área de cobertura, armazenando informações acerca da conexão desses aparelhos com a rede que a eles dá suporte, **sem registrar, contudo, o conteúdo da comunicação**.

A partir do cruzamento dessas informações, é possível obter **a geolocalização, em tempo real, de determinado aparelho/terminal/IMEI – e, por conseguinte, de determinada pessoa –, ou traçar o trajeto por ela percorrido durante certo período**. No caso, não há acesso, propriamente, aos "**dados**" produzidos pelo ato comunicativo (ou seja, aos dados recebidos e enviados pelos interlocutores, ou ao teor das conversas ou mensagens transmitidas). Obtêm-se apenas os **"metadados"** gerados pela interação técnica entre os aparelhos celulares e a infraestrutura de telecomunicações.

O Supremo Tribunal Federal já se pronunciou a respeito dessa espécie de dados – **metadados** – por ocasião do julgamento da **ADI nº 5.642**, Rel. Min. **Edson Fachin**, na qual se questionava a constitucionalidade dos **arts. 13-A e 13-B do Código de Processo Penal,**

incluídos pela Lei nº 13.344/16, ocasião em que se fixou, por maioria, a seguinte tese:

> "**São passíveis de requisição sem controle judicial prévio, mas sempre sujeito ao controle judicial posterior, a localização de terminal ou IMEI de cidadão em tempo real por meio de ERB por um período determinado e desde que necessário para os fins de reprimir os crimes contra a liberdade pessoal descritos no art. 13-A do Código de Processo Penal; extrato de ERB**; (...), após o decurso do prazo de 12 horas constante do § 4º do art. 13-B do Código de Processo Penal."

Naquela oportunidade, o Supremo Tribunal explicou que

> "[a]s normas impugnadas **não conferem amplo poder de requisição, mas um que é instrumentalmente necessário para reprimir as violações de crimes graves que atentam contra a liberdade pessoal e que se destinam a permitir o resgate das vítimas dessas infrações enquanto elas ainda estão em curso**" (ADI nº 5.642, Rel. Min. **Edson Fachin**, Tribunal Pleno, julgado em 18/4/24, DJe de 22/8/24).

Como se observa, a possibilidade de requisição direta de tais dados pelo delegado de polícia **é excepcional**, dada **a gravidade das infrações** penais estabelecidas em **rol taxativo** e, sobretudo, a finalidade de se proceder ao **resgate das vítimas em tempo hábil** e com **a integridade física preservada**. Daí decorre, portanto, **a inviabilidade de se estender a possibilidade de requisição direta desses metadados pelo delegado de polícia à totalidade dos crimes**, uma vez que isso poderia acarretar a devassa injustificada ou desproporcional da privacidade e/ou da intimidade dos eventuais investigados, ou, ainda, o monitoramento ativo de um número indeterminado de pessoas, inclusive para fins ilegais ou

moralmente ilegítimos, se não observada a proteção legal que deve recair sobre os respectivos dados pessoais e adotadas as devidas cautelas na coleta, no armazenamento, no tratamento e, posteriormente, no descarte desses dados.

Especificamente quanto à obtenção de extrato de ERB por autoridades administrativas, independentemente de autorização judicial, recordo que, ao referendar, por maioria dos votos, a medida cautelar deferida na **ADI nº 6.387**, Rel. Min. **Rosa Weber**, o Plenário do Supremo Tribunal Federal entendeu pela **necessidade de se suspender a eficácia da Medida Provisória nº 954, de 2020, para "prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel"**. O julgado foi ementado nos seguintes termos:

> "MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. **REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA.** FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. **Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das**

cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. **O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam 'adequados, relevantes e não excessivos em relação a esse propósito' e 'conservados apenas pelo tempo necessário.' (artigo 45, § 2º, alíneas 'b' e 'd')**. 4. **Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia**. 5. **Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades**. 6. **Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros**. 7. **Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público,**

> **por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada**. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. **Fumus boni juris** e **periculum in mora** demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada" (ADI nº 6.387-MC-Ref, Rel. Min. **Rosa Weber**, Tribunal Pleno, julgado em 7/5/20, DJe de 12/11/20).

Anote-se, por fim, que o referido precedente é anterior à promulgação da **EC nº 115, de 2022**, pela qual se incluiu a proteção dos dados pessoais como direito autônomo no rol de direitos fundamentais. Se, à época, esse entendimento reconhecia o monitoramento por geolocalização por meio de ERB como **medida invasiva e potencialmente lesiva a direitos fundamentais**, preconizando, por isso, seu uso adequado, pertinente e proporcional, agora, com maior razão, **não há**

como se refutar que medida tão drástica deve observar, rigorosamente, os critérios e as finalidades estabelecidas em lei específica. Nesse sentido, na ausência dessa, **a medida pressupõe autorização judicial prévia**, a fim de se resguardar a inviolabilidade dos direitos à vida privada e à intimidade e, ainda, o direito à proteção de dados pessoais, **cabendo ao juiz verificar, em cada caso concreto, a proporcionalidade da medida e fixar as cautelas devidas para a coleta, o tratamento, o armazenamento e o descarte dos dados obtidos**.

(e) Extrato de mensagens de texto (SMS ou MMS) e serviços de agenda virtual ofertados por empresas de telefonia

Por tudo o que já foi exposto até aqui, penso que **a inviolabilidade do sigilo das comunicações telefônicas e telemáticas estende-se aos extratos de mensagens de textos (SMS ou MMS)**, bem como **aos serviços de agenda virtual oferecidos pelas empresas de telefonia**, razão pela qual **o acesso a tais dados, a meu ver, também depende de prévia autorização judicial**.

Com efeito, não é crível que a Constituição de 1988 tenha estabelecido, por exemplo, a inviolabilidade da correspondência ou das comunicações telefônicas e do fluxo de dados informáticos e telemáticos e não resguarde, por exemplo, o sigilo de dados transmitidos por outros meios tecnológicos similares – ou nele armazenados. Embora esses recursos/serviços não existissem à época da promulgação da Constituição de 1988, eles parecem se amoldar perfeitamente às expressões mais abertas de que o Poder Constituinte originário se valeu no texto de 1988.

Nessa linha, ao comentar o já citado art. 1º, parágrafo único, da Lei nº 9.296/92, **Lenio Streck** ensina o seguinte:

> "[A]o estender a possibilidade de interceptação também ao fluxo de comunicações em sistemas de informática e telemática, apenas especificou que **a lei também atingirá toda e**

qualquer variante de informações que utilizem a modalidade 'comunicações telefônicas'. Ou seja, objetivou a lei estender a aplicação das hipóteses de interceptação de comunicações telefônicas *a qualquer espécie de comunicação*, ainda que realizada mediante sistemas de informática, existentes ou que venham a ser criados, desde que tal comunicação utilize a modalidade 'comunicações telefônicas'. Isto porque o constituinte, ao utilizar a expressão 'comunicações telefônicas', deixou patente que abarcava a possibilidade de o Estado interceptar 'informes em tráfego', conforme muito bem lembra o Juiz Federal Ivan de Lira Carvalho. Quisesse o constituinte limitar à interceptação simplesmente aos telefonemas entre pessoas, não teria usado 'comunicações' *lato sensu*. Sabe-se que, com o avanço da informática, permite-se a prática de comunicações via computador, por exemplo, a Internet, cujo veículo é o telefone. Já a telemática vem a ser a ciência que trata da manipulação e utilização da informação através do uso combinado do computador e meios de telecomunicação. Citando a obra de Sérgio Charlab — Você e a Internet no Brasil — Lira Carvalho esclarece que as comunicações implementadas por meio de fax modem, sendo este um dispositivo que permite a transmissão e a recepção de informações digitais de um computador para outro, através de linha telefônica, podem ser encartadas na previsão de telemática, prevista no parágrafo único do art. 1º da Lei 9.296. Por isso, com acerto, assinala Parizatto: 'qualquer, pois, que seja o meio utilizado para a comunicação, será possível a interceptação para prova em investigação criminal e em instrução processual penal, sendo o caso'. Não se discute se a expressão contida no inciso XII 'no último caso' se refere somente às comunicações telefônicas ou também aos 'dados'" (STRECK, Lenio. **As Interceptações Telefônicas e os Direitos Fundamentais**: Constituição, Cidadania, Violência: Lei 9.296/96 e seus reflexos penais e processuais. Porto Alegre: Livraria do Advogado, 1997. p. 42-44).

Ademais, ainda que se entenda não haver, no caso de serviços de agenda eletrônica, propriamente a transmissão de dados entre dois ou mais interlocutores (ou entre dois ou mais terminais de informática ou telemática), não estando caracterizada, por isso, tecnicamente, a "comunicação de dados" de que trata o inciso XII do art. 5º, **há, no caso, pelo menos o uso de serviço digital de armazenamento de dados em nuvem, oferecido pelas empresas de telefonia muitas vezes de forma gratuita. Sendo assim, não se pode deixar de reconhecer que esses dados – mesmo que não se revelem, por natureza, dados sigilosos – desfrutam de proteção jurídica especial, por força dos incisos X e LXXIX do art. 5º da Constituição de 1988, impondo-se, pois, a prévia autorização judicial para acessá-los**.

(f) Dados cadastrais de usuários de IP (ou seja, dados de usuários que, em determinado dia, data e hora e fuso, fizeram uso de um IP para acessar a internet); dados cadastrais de ***e-mail****; e, por último, dados cadastrais dos terminais fixos não figurantes em lista telefônica divulgável e dos terminais móveis*

A Lei nº 12.965, de 2014, ao instituir o **Marco Civil da Internet**, assegurou aos usuários de internet no país, em seu art. 7º; o direito à inviolabilidade da intimidade e da vida privada; o direito à inviolabilidade e ao sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; o direito à inviolabilidade e ao sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; e o direito ao não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (incisos I, II, III e VII), entre outros.

Além disso, referido diploma legal estabeleceu, em seu art. 10, que a guarda e a disponibilização de registros de conexão e de acesso a

aplicações, bem como dos dados pessoais e do conteúdo das comunicações privadas, "devem atender à preservação da intimidade, da privada privada, da honra e da imagem das partes direta ou indiretamente envolvidas". Logo, o provedor responsável pela guarda somente será obrigado a disponibilizar **registros de conexão** e de **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 Sessão IV" (art. 10, § 1º).

Especificamente quanto a esses dados, impõe-se observar que a **autoridade policial, administrativa e o Ministério Público** podem até requerer cautelarmente ao provedor de internet **a guarda** de tais dados por período superior ao previamente estabelecido em lei, **mas o acesso a aos registros depende sempre de autorização judicial (arts. 13 e 15)**.

Quanto ao **conteúdo das comunicações privadas**, diz a lei, no art. 10, § 2º, que "somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º", enquanto o § 3º do referido dispositivo legal preconiza que a preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas "**não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas**" (grifo nosso).

Registre-se, ainda, a existência de leis esparsas autorizando que o delegado de polícia (ou membro do Ministério Público que conduzir a investigação criminal) requisite diretamente dados cadastrais a órgãos públicos e a empresas privadas para fins de investigação criminal. Nesse sentido, destaco o **art. 17-B da Lei nº nº 9.613/98, inserido pela Lei nº 12.683/12,** e o **art. 13-A do CPP, incluído pela Lei nº 13.344/16**. Eis o que prescrevem referidos dispositivos:

Lei nº 9.613/98

> **"Art. 17-B.** A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito."
>
> **CPP**
>
> **"Art. 13-A.** Nos crimes previstos nos arts. 148 , 149 e 149-A , no § 3º do art. 158 e no art. 159 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal) , e no art. 239 da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente) , o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos.
>
> Parágrafo único. A requisição, que será atendida no prazo de 24 (vinte e quatro) horas, conterá:
>
> I - o nome da autoridade requisitante;
>
> II - o número do inquérito policial; e
>
> III - a identificação da unidade de polícia judiciária responsável pela investigação."

Pela legislação atual, portanto, **os dados cadastrais armazenados pelas empresas de telefonia podem ser requisitados diretamente pelo delegado de polícia (ou por membro do Ministério Público)**.

Ressalto, outrossim, que o Supremo Tribunal Federal, ao julgar a **ADI nº 4.924**, Rel. Min. **Gilmar Mendes**, reconheceu **a constitucionalidade de lei paranaense que fixa para as prestadoras de serviço telefônico a obrigação de fornecer os dados pessoais de usuários de terminais utilizados para passar "trotes" aos serviços de emergência**. Eis a ementa do julgado:

"Ação direta de inconstitucionalidade. Constitucional. Administrativo. Direitos fundamentais. Lei 17.107/12, do Estado do Paraná, que dispõe sobre penalidades ao responsável pelo acionamento indevido dos serviços telefônicos de atendimento a emergências envolvendo remoções ou resgates, combate a incêndios, ocorrências policiais ou atendimento de desastres (trote telefônico). 2. Inépcia da petição inicial. Falta de causa de pedir. Apenas o art. 2º, caput, e § 1º, se relacionam com as causas de pedir da ação – invasão da competência da União para legislar sobre telecomunicações e violação à vida privada e à proteção de dados. Demais dispositivos que tratam das sanções a serem aplicadas ao usuário da linha telefônica da qual se origina o trote a serviços de emergência. Ação conhecida apenas quanto aos dispositivos mencionados. 3. **Dispositivos que determinam que as prestadoras de serviço telefônico são obrigadas a fornecer, sob pena de multa, os dados pessoais dos usuários de terminais utilizados para passar trotes aos serviços de emergência.** 4. Alegação de inconstitucionalidade formal, por invasão da competência da União para legislar sobre serviços de telecomunicações – art. 22, IV, da CF. A norma trata do relacionamento entre as prestadoras e a administração pública, em uma relação diversa daquela decorrente da outorga da prestação do serviço – prestação de informações para processo administrativo. **Norma compatível com a legislação federal, que não estabelece um direito ao sigilo absoluto dos dados pessoais, sendo perfeitamente compatível com a requisição de dados no curso de um procedimento de apuração de infração administrativa.** 5. Alegação de inconstitucionalidade material, por suposta violação ao direito à privacidade, pela quebra do sigilo de dados sem ordem judicial e em situação desproporcional – art. 5º, X e XII, da CF. **Proporcionalidade da medida, desde que observadas as exigências que decorrem dos dispositivos constitucionais indicados. Quebra de sigilo limitada aos dados pessoais. Exigência de um procedimento**

> **administrativo em curso. Infração administrativa grave, com possíveis repercussões criminais e potencial de produzir considerável risco à comunidade.** 6. Conhecimento parcial da ação, apenas em relação ao art. 2º, caput, e § 1º. Quanto a estes, pedido julgado improcedente" (ADI nº 4.924, Rel. Min. **Gilmar Mendes**, Tribunal Pleno, julgado em 4/11/21, DJe de 28/3/22).

Mas o que se deve entender por "dados cadastrais"? A ausência de consenso normativo a respeito do que se deva entender por "**dados cadastrais**" levou a **Associação Nacional das Operadoras de Celulares (ACEL)** – ora requerente – a questionar a constitucionalidade do disposto no **art. 17-B da Lei nº nº 9.613/98, inserido pela Lei nº 12.683/12**, e no **art. 13-A do CPP, incluído pela Lei nº 13.344/16**, dando origem à **ADI nº 4.906** e à **ADI nº 5.642**, ambas julgadas recentemente.

No julgamento da **ADI nº 4.906**, Rel. Min. **Nunes Marques**, o Supremo Tribunal Federal entendeu que "**a imposição de sigilo não alcança os dados cadastrais**", o que "**não significa que essas informações dispensem tutela jurisdicional, mas apenas que a tutela em virtude do direito à privacidade não se concretiza via sigilo**" (ADI nº 4.906, Rel. Min. **Nunes Marques**, julgado em 11/9/24, DJe de 24/10/24). Ressaltou, outrossim, o Tribunal que

> "[o] direito fundamental à proteção de dados e à autodeterminação informativa (CF, art. LXXIX) impõe a adoção de mecanismos capazes de assegurar a proteção e a segurança dos dados pessoais manipulados pelo poder público e por terceiros" (ADI nº 4.906, rel. Min. **Nunes Marques**, julgado em 11/9/24, DJe de 24/10/24).

No voto condutor do acórdão, o Ministro **Nunes Marques** esclarece que "**dados cadastrais são informações objetivas, fornecidas, não raro, pelo próprio usuário ou consumidor para registro da sua identificação nos bancos de dados de pessoas jurídicas públicas e privadas**" e

conclui, ao final, que "**seu compartilhamento com os órgãos de persecução penal para efeito de investigação criminal independe de autorização da Justiça**". Isso porque, de acordo com Sua Excelência,

> "a tutela do direito à privacidade, em sua dimensão estática, atinente ao poder do indivíduo de excluir certas informações do âmbito público, não alcança informações cadastrais, as quais, em regra, não são hábeis a ferir a integridade moral do indivíduo.
>
> Por sua vez, na dimensão dinâmica, concernente ao poder de controle e circulação das informações, essa tutela exige muito mais a consolidação de mecanismos capazes de reduzir os danos inerentes ao tratamento das informações, independentemente do conteúdo que veiculem, o que impede o fluxo delas mediante o sigilo" (ADI nº 4.906, Rel. Min. **Nunes Marques**, Tribunal Pleno, julgado em 11/9/24, DJe de 24/10/24).

Complementarmente, no julgamento da **ADI nº 5.642**, Rel. Min. **Edson Fachin**, o Supremo Tribunal Federal afirmou que a expressão "dados cadastrais"

> "**não abrange** a interceptação de voz; a interceptação telemática; os dados cadastrais de usuários de IP, os quais abarcam dados de usuário que em determinado dia, data, hora e fuso fizeram uso de um IP para acessar à internet; os serviços de agenda virtual ofertados por empresas de telefonia; o dado cadastral de **e-mail** e os extratos de conexão a partir de linha ou IP" (ADI nº 5.642, Rel. Min. **Edson Fachin**, Tribunal Pleno, julgado em 18/4/24, DJe de 22/8/24).

Desse modo, depende de autorização judicial prévia o acesso a i) dados cadastrais de usuários de IP (o que inclui dados de usuários que, em determinado dia, data e hora e fuso, fizeram uso de um IP para

acessar a internet) e ii) dado cadastral de **e-mail**. Já os dados cadastrais relativos a terminais (fixos ou móveis) de telefonia não constantes de listas telefônicas divulgáveis podem ser obtidos pela autoridade policial independentemente de ordem judicial, com fundamento no art. 2º, § 2º, da Lei nº 13.830/13, ora impugnado, **ficando as concessionárias de telefonia obrigadas a informar tão somente o nome completo, a filiação e o endereço do titular da(s) linha(s) ou do(s) terminal(is) indicado(s)**.

2.6 Considerações finais.

Para finalizar, observo que, conquanto se tenha tratado, neste voto, **unicamente da possibilidade de requisição direta de dados e metadados relativos a serviços de telefonia por autoridade policial** – até porque a norma contestada está inserida em diploma legal destinado a disciplinar a atividade de investigação criminal conduzida por delegado de polícia –, convém deixar claro que **as conclusões acima são aplicáveis, *mutatis mutandis*, às requisições feitas pelo Ministério Público**, porquanto, conforme decidido na **ADI nº 5.043**, de **minha relatoria**, julgada em sessão virtual do Plenário realizada entre 21 e 28 de março de 2025 (acórdão pendente de publicação), **"a atividade de investigação criminal não é exclusiva ou privativa da polícia, sob direção dos delegados de polícia**".

3. DISPOSITIVO.

Ante todo o exposto, **julgo procedente**, **em parte, o pedido** formulado na presente ação direta para se **conferir interpretação conforme à Constituição de 1988 ao § 2º do art. 2º da Lei nº 12.830, de 2013**, a fim de esclarecer que

(i) o poder genérico de requisição, contido na referida norma, atribui ao delegado de polícia o poder de atuar conforme a lei e o direito e, assim, **não dispensa a prévia autorização judicial nas hipóteses**

constitucionais e legais submetidas à reserva jurisdicional;

(ii) nas investigações criminais que conduzir, o delegado de polícia (**ou o membro do Ministério Público**) pode requisitar **diretamente** às concessionárias de telefonia **somente** "dados cadastrais", assim considerados **o nome completo, a filiação e o endereço** do titular da linha ou terminal (fixo ou móvel) em relevo; quando configurada qualquer das hipóteses do art. 13-A do CPP, incluído pela Lei nº 13.344/16, também será possível, **excepcionalmente**, a requisição **direta** por delegado de polícia (ou por membro do Ministério Público) de a) dados pertinentes à localização de terminal ou IMEI de cidadão em tempo real por meio de ERB e b) fornecimento de extrato de ERB (**cf**. art. 13-B do CPP, inserido pela Lei nº 13.344/16, e ADI nº 5.642, Rel. Min. **Edson Fachin**, Tribunal Pleno, julgado em 18/4/24, DJe de 22/8/24);

(iii) a expressão "dados cadastrais" **não abrange** a) a interceptação de voz; b) a interceptação telemática; c) o extrato de chamadas telefônicas (ou extrato de registros telefônicos); d) a localização de terminal ou IMEI de cidadão em tempo real por meio de ERB e o extrato de ERB; e) os extratos de mensagens de texto (SMS ou MMS); f) os serviços de agenda virtual ofertados por empresas de telefonia; g) os registros de conexão e de acesso a aplicações de internet, a partir de determinada linha ou IP; h) o conteúdo das comunicações privadas armazenadas; i) os dados cadastrais de usuários de IP, os quais abarcam dados de usuários que, em determinado dia, data, hora e fuso, fizeram uso de um IP para acessar a internet; e j) os dados cadastrais de correio eletrônico (**e-mail**).

É como voto.