V O T O

O Senhor Ministro Edson Fachin (Relator): Examino, inicialmente, as preliminares suscitadas nesta ação direta.

Alegações das Partes sobre as Preliminares

A Presidência da República alega que a ACEL não tem pertinência temática para propor a ação direta, porquanto "não foi comprovado pela requerente que a disponibilização de dados cadastrais e a manutenção de registros telefônicos de usuários do serviço de telefonia móvel são temas que afetam diretamente interesses jurídicos e econômicos" de seus associados. Aduz, ainda, que a associação também não poderia ser considerada entidade representativa de classe, na medida em que reúne apenas operadoras de telefonia celular.

A Advocacia-Geral da União sustenta não haver interesse jurídico no pedido de interpretação conforme, pois a norma apresenta apenas um sentido, qual seja, o de permitir a requisição apenas de "dados e informações cadastrais". Além disso, o sentido pleiteado pela requerente implicaria inovação legal, o que, em seu entender, também desautorizaria o conhecimento do pedido.

Análise dos Argumentos sobre as Preliminares

A Associação Nacional das Operadoras de Celulares – ACEL, como entidade de classe, teve sua legitimidade reconhecida por diversos precedentes desta Corte (*v.g.* ADI 5.521, Rel. Min. Gilmar Mendes, Pleno, DJe 22.05.2019).

Além disso, há, ao menos em tese, interesse na representação de seus associados a fim de que não sejam obrigados a cumprir dispositivo de lei que, em seu entender, seja inconstitucional. O dispositivo constante do art. 3º, I, II e III, de seu Estatuto, portanto, atesta a pertinência temática da requerente.

No que tange à preliminar suscitada pela Advocacia-Geral da União, é preciso observar, em primeiro lugar, que apenas quanto ao pedido

subsidiário são levantadas as dúvidas de interpretação do art. 11 da Lei 13.344/2016. Por isso, nesse ponto, nada obsta o conhecimento da ação quanto ao primeiro pedido, qual seja, o de se declarar *in totum* a inconstitucionalidade do dispositivo.

Também não merece prosperar a alegação de que há apenas um sentido ou de que o sentido pleiteado implicaria atuação legislativa por parte do Supremo Tribunal Federal. Embora seja no mérito da ação que esses argumentos devem ser mais bem examinados, cumpre registrar que há, ao menos em tese, polissemia no sintagma "dados e informações cadastrais", ora a configurar gênero de informações, ora espécie. A alegada polissemia e a eventual incompatibilidade com a constituição de algumas das acepções da expressão impugnada justificam o conhecimento integral da ação.

Por essas razões, rejeito as preliminares suscitadas.

Alegações das Partes sobre o Mérito

A requerente sustenta que os dispositivos impugnados permitem a requisição direta de dados e comunicações telefônicas, sem que haja ordem judicial específica. Defende que as comunicações telefônicas propriamente ditas e os dados inerentes à utilização dos serviços de telefonia têm proteção constitucional, consoante previsão expressa dos incisos X e XII do art. 5º da Constituição Federal. Esses dados, portanto, somente poderiam ser obtidos por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal. A proteção constitucional abrangeria, assim, não apenas as comunicações telefônicas propriamente ditas, mas também os dados inerentes à utilização dos serviços de telefonia.

A requerente questiona, em particular, a possibilidade de se franquear ao Ministério Público e à autoridade policial, sem controle judicial prévio, o acesso a dados de usuário referentes ao dia, à data, horário e ao fuso no qual se deu o acesso à internet. Defende, portanto, que seja dada interpretação conforme a fim de reconhecer a necessidade de autorização judicial para a requisição dos seguintes dados: (i) interceptação de voz; (ii) interceptação telemática; (iii) localização de terminal ou IMEI de cidadão em tempo real por meio de ERB; (iv) extrato de ERB; (v) 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; (vi) dados cadastrais dos terminais fixos não figurantes em lista telefônica

divulgável e de terminais móveis; (vii) extrato de chamadas telefônicas; (viii) extrato de mensagens de texto (SMS ou MMS); (ix) serviços de agenda virtual ofertados por empresas de telefonia; (x) dado cadastral de e-mail; (xi) extratos de conexão de internet a partir de linha ou IP.

A Presidência da República alega que a norma atacada promove restrição na esfera privada de forma razoável e proporcional, já que os crimes para os quais a expectativa de sigilo pode ser afastada são particularmente graves e se destinam a localizar as vítimas e suspeitos, além de obter provas para a instrução penal. Ademais, não haveria, segundo alegou o Presidente da República, outro meio menos invasivo para promover o mesmo fim. Ainda segundo a Presidência, não há acesso indiscriminado aos dados, uma vez que são requisitados apenas informações cadastrais.

A Advocacia-Geral da União, por sua vez, chama a atenção para a diferença de redação entre o art. 13-A e o art. 13-B do Código de Processo Penal, na redação introduzida pela norma objeto desta ação direta. Enquanto no art. 13-A, prevê-se apenas acesso às informações cadastrais, no art. 13-B, utiliza-se a expressão "meio técnicos adequados", que abrange sinais, informações e outros, que permitam localizar a vítima ou os suspeitos do delito em curso. Para a requisição de dados que permitam a localização, é preciso, segundo a AGU, autorização judicial, salvo se a demanda for urgente e não houver manifestação do juízo competente no prazo de 12 (doze) horas.

Para a Procuradoria-Geral da República, a necessidade de se submeter à autorização judicial o pedido para o compartilhamento de dados que não digam respeito ao conteúdo da comunicação seria inconstitucional. Em seu parecer, defende que a lei não cria novas restrições de acesso aos dados, para além daquelas já fixadas pela Constituição. Em analogia com a possibilidade de entrada forçada em domicílio nos casos de flagrante, alega que "não há razão que justifique a exigência de prévia autorização do juiz para requisição de meios necessários à obtenção da localização de vítima e/ou suspeito em tempo real no caso da prática de crimes relacionados ao tráfico de pessoas" (eDOC 37, p. 11).

Análise dos Argumentos sobre o Mérito da Ação

A presente ação direta desafia a atualização da cláusula constitucional de proteção à privacidade na era digital. Não obstante a relevância dessa

proteção, ante as limitações estabelecidas pela própria Lei, que restringe sua aplicação apenas a crimes especialmente graves como o cárcere privado, a redução a condição análoga à de escravo, o tráfico de pessoas, o sequestro relâmpago, a extorsão mediante sequestro e o envio ilegal de criança ao exterior, **é improcedente a presente ação direta.**

A Constituição assegura a todos a inviolabilidade do sigilo de correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, como reconhece a jurisprudência do Supremo Tribunal Federal, por ordem judicial e nas hipóteses em que a lei permitir para fins de investigação criminal ou instrução processual penal (art. 5º, XII, da CRFB).

Além disso, a Constituição também protege a casa, asilo inviolável do indivíduo, garantindo que ninguém possa nela penetrar sem consentimento do morador ou determinação de autoridade judicial (art. 5º, XI, da CRFB).

Essas disposições constitucionais corporificam no Brasil o direito à privacidade e à vida privada consagrado no art. 11 do Pacto de São José da Costa Rica, que prevê que "ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação".

Por expressa disposição constitucional, apenas a lei pode determinar as hipóteses de investigação criminal que autorizam, mediante ordem judicial, o afastamento do sigilo que se espera das comunicações.

O sigilo é necessário porque ele ampara uma legítima expectativa de privacidade não apenas no sentido de ser deixado a sós, como defendia o Justice Brandeis, mas sobretudo para proteger escolhas de vida contra o controle estatal e a estigmatização social (RODOTÀ, Stefano. General Presentation of Problems related to Transsexualism. In: Transsexualism, Medicine and Law: Proceedings of the XXIIIrd Colloquy on European Law. Strasbourg: Concil of Europe Publishing, 1995. p. 22-23).

O direito à proteção da privacidade não é absoluto, mas qualificado. A lei pode restringir esse direito ao prever as hipóteses em que o Poder Judiciário poderá afastá-lo e a finalidade para a qual a restrição é admitida é a de investigar as infrações à lei, pois as provas das infrações raramente ficam disponíveis publicamente.

No passado, o balanceamento desses interesses fez com que a prática jurídica nacional criasse uma divisão entre fatos que seriam publicamente

acessíveis e aqueles que estariam sob proteção judicial. Era comum, por exemplo, que os regulamentos da polícia judiciária atribuíssem aos delegados o poder de requisitar "informações cadastrais", ou seja, as informações que constam do registro geral de identificação, cujo cadastro é da competência da própria polícia (*v.g.* , art. 108, VIII, do Decreto n. 56.511, de 28 de junho de 1965). Assim, para o acesso a essas informações mais simplificadas que diziam respeito à identificação da pessoa – e que constavam de um banco de dados público –, a autorização judicial não seria necessária.

Em linha com essa orientação, a prática deste Tribunal em passado recente pode ser representada pela célebre colocação do e. Ministro Sepúlveda Pertence: "a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos dados em si mesmos" (RE 418.416, Rel. Min. Sepúlveda Pertence, Pleno, DJ 19.12.2006). No mesmo sentido, o e. Ministro Gilmar Mendes adverte que "não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta" (HC 91.867, Rel. Min. Gilmar Mendes, Segunda Turma, DJe 19.02.2012). Ou seja, de acordo com os precedentes do Supremo Tribunal Federal, tal como as informações de registros públicos, os dados cadastrais, de posse das empresas de telefonia, também poderiam ser requisitados, sem que se falasse em ofensa ao direito à privacidade.

A própria legislação passou a afastar a expectativa de privacidade que esses dados cadastrais teriam quando dispôs sobre a obrigatoriedade de seu fornecimento. O exemplo mais conhecido, porque longamente debatido neste Tribunal, foi o acesso às informações bancárias, previsto na Lei Complementar 105, de 2001, pela autoridade Fazendária (ADI 2.858, Rel. Min. Dias Toffoli, Pleno, DJe 20.10.2016), entendimento que, no âmbito do Superior Tribunal de Justiça, foi estendido à requisição pelo Ministério Público, eis que as informações dos correntistas bancários seriam apenas "dados cadastrais" (REsp 1.561.191, Rel. Min. Herman Benjamin, DJe 26.11.2018).

No mesmo sentido também não possuem expectativa de privacidade, por expressa disposição legal, os provedores de acesso à internet (art. 10, § 3º, da Lei 12.965, de 2014), entendidos esses dados como sendo a qualificação pessoal, a filiação e o endereço.

À semelhança do direito norte-americano, criou-se no Brasil uma espécie de doutrina de terceiros (*third-party doctrine*) que acaba por afastar a expectativa de privacidade dos dados guardados por terceiros, isto

é, agentes privados que tem a custódia de informações voluntariamente concedidas a bancos, provedores de internet e companhias telefônicas.

Essa orientação sobre o sentido da expressão "dados cadastrais" foi levada em conta pelo Poder Legislativo nas alterações feitas à lei processual penal, no que ampliaram os poderes de investigação das autoridades policiais e dos membros do Ministério Público, conforme se observa da leitura da Lei 9.613, de 1998, na redação dada pela Lei 12.683, de 2012, e da Lei 12.850, de 2013:

> Lei 9.613
> "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."
> Lei 12.850
> "Art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito."

A Lei 12.850, de 2013, na redação dada pela Lei 13.964, de 2019, conceitua dados cadastrais como sendo "informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão" e prevê constituir crime a recusa ou a omissão de dados cadastrais, quando requisitados pelo juiz, Ministério Público ou delegado de polícia.

A definição, no entanto, aparece no art. 10-A, que disciplina a técnica de infiltração de agentes e não encontra paralelo nos demais textos que preveem o acessos aos dados cadastrais.

Por isso, ante a ausência de uma definição precisa, não chega a surpreender que todas as disposições que autorizem o acesso aos dados tenham sido impugnadas no Tribunal.

O art. 17-B da Lei 9.613, de 1998, por exemplo, é questionado na ADI 4.906, de Relatoria do e. Min. Nunes Marques. A ação estava na pauta do plenário virtual que se iniciou no dia 28.05.2021, mas seu julgamento foi suspenso em virtude de pedido de vista do e. Min. Gilmar Mendes.

Já os dispositivos iniciais da Lei 12.850, de 2013, são impugnados na ADI 5.059 e na ADI 5.043, ambas de Relatoria do e. Min. Dias Toffoli, e os artigos que dispõem especificamente sobre o poder de requisição são atacados na ADI 5.063, de Rel. do e. Min. Gilmar Mendes, todas ainda pendentes de inclusão no calendário de julgamento.

Os argumentos pela inconstitucionalidade desses dispositivos são semelhantes aos que estão postos na presente ação direta: com a evolução tecnológica é possível utilizar dados simples, como os cadastrais, para obter informações sensíveis, o que, potencialmente, fragilizaria a proteção à privacidade, desvirtuando a finalidade da garantia constitucional. Dito de outro modo, a proposição segundo a qual os dados cadastrais não têm expectativa de privacidade seria, de acordo com as requerentes, mal adaptada para a era digital.

Tome-se, por exemplo, a localização de uma estação radio base (ERB), comumente conhecida como "antena de celular". Ela serve para conectar a infraestrutura física de comunicação com o sinal de rádio captado pelos telefones celulares. Na ERB ficam armazenadas as informações de conexão de aparelhos de telefone, sem, porém, haver a interceptação do conteúdo da comunicação. A partir do cruzamento de dados entre a localização das ERBs e a conexão de um usuário é possível obter informações sobre a localização do aparelho em um determinado momento, ou mesmo o histórico de locais por onde transitou.

Como sabem as empresas que controlam os principais aplicativos de internet e as redes sociais utilizadas por bilhões de usuários, para saber muito sobre a vida das pessoas, o acesso aos metadados das comunicações é, muitas vezes, mais relevante do que saber o próprio conteúdo das conversas.

Por essa razão, no campo doutrinário, alguns autores passaram a utilizar a metáfora de um mosaico para redefinir o alcance do direito à privacidade: a era digital tornou possível que o acúmulo gradual de informações sobre a pessoa passasse a merecer tutela constitucional

(SLOBOGIN, Christopher. *Making the Most of United States v. Jones in a Surveillance Society: a Statutory Implementation of Mosaic Theory* . 8 Duke Journal of Constitutional Law & Public Policy, n. 1, 2012).

A dúvida trazida nesta ação direta é, portanto, a de saber se expressão "dados cadastrais" ampara a proteção constitucional da privacidade à luz das inovações trazidas pelo desenvolvimento tecnológico.

O debate não é inédito na experiência comparada. Como a evolução tecnológica é global e como a proteção da privacidade é um direito universal, outros países também têm passado por debates semelhantes.

Embora haja países em que se dispense o mandado judicial para o monitoramento dessas atividades (p.ex., na Holanda, na Itália e na Polônia, conforme relatam B.J. Koops, B.C. Newell, and I. Škorvánek, em *Location Tracking by Police: The Regulation of 'Tireless and Absolute Surveillance* , 9 UC Irvine L. Rev. n. 3, 2019), nos Estados Unidos, a Suprema Corte rejeitou a possibilidade de requisição, sem autorização judicial, do histórico de dados de uma ERB, já que a eles não se aplica a expectativa de privacidade, porque, desde que ligado o aparelho celular, as informações das estações são captadas o tempo todo, independentemente da vontade de quem porta o telefone. Admitir o acesso a esses dados, segundo afirmou o Justice Roberts ao redigir o texto da maioria, daria aos investigadores acesso à informação de "modo detalhado, enciclopédico e facilmente compilado" (Carpenter v. U.S., 585 U.S. 138 S. Ct. 2206; 201 L. Ed. 2D 507).

Na Alemanha, o Código de Processo Penal passou a admitir, mediante autorização judicial, a captura dos dados de localização apenas em relação aos dados de tráfego para evitar a prática ou para realizar o flagrante de crimes graves, desde que tais dados sejam necessários para determinar os fatos ou para identificar a localização do acusado (§ 100g, combinado com § 100a e § 100b, *Strafprozeßordnung*).

De modo semelhante, no Canadá, o Código Penal passou a exigir que os documentos contendo os dados de localização só podem ser entregues por meio de ordem judicial (§ 487.017).

Essas alterações legislativas e os debates judiciais demonstram que, na era digital, são no mínimo discutíveis a aplicação do conceito de "dados cadastrais" para definir o alcance dos poderes de requisição sem mandado judicial por parte das autoridades policiais e do Ministério Público. Por isso, apesar de a redação legislativa contida no art. 13-A do Código de Processo Penal limitar-se a "dados e informações cadastrais", expressão consagrada

na jurisprudência deste Tribunal, é preciso não colocá-la acima da própria proteção constitucional, isto é, não se deve interpretar a expressão de modo a tornar ineficaz a proteção constitucional.

Como advertem Dennys Antonialli e Jacqueline de Souza Abreu (*Brazil and the Treasure Trove's Tales: A Study on the Evolution and Popularization of Phones and Law Enforcement Access to Communications.* In: FELSBERGER, Stefanie; SUBRAMANIAN, Ramesh. *Mobile Technology and Social Transformation.* Abingdon: Routledge, 2021, *tradução livre*):

> "Na prática, essas autoridades [delegados de polícia e membros do Ministério Público] utilizam esses dispositivos legais [que lhes atribuem o poder de requisição de dados cadastrais] para justificar a requisição de dados a empresas de telefonia em todos os casos; e a questão só é levada às cortes para revisão se uma empresa se recusar a cumprir. A falta de qualquer critério formal ou material para o fornecimento de informações deixa esses procedimentos ainda mais discricionários".

Por tudo isso, este Tribunal não pode aceitar acriticamente a utilização da expressão "dados e informações cadastrais" para reconhecer como legítima toda e qualquer interferência no direito à privacidade, já que a atual capacidade de produção e análise de dados, ainda que mais simples e públicos, pode trazer significativos impactos.

O texto normativo impugnado acrescentou dois artigos ao Código de Processo Penal:

> " 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."

"Art. 13-B. Se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso.

§ 1º Para os efeitos deste artigo, sinal significa posicionamento da estação de cobertura, setorização e intensidade de radiofrequência.

§ 2º Na hipótese de que trata o caput, o sinal:

I - não permitirá acesso ao conteúdo da comunicação de qualquer natureza, que dependerá de autorização judicial, conforme disposto em lei;

II - deverá ser fornecido pela prestadora de telefonia móvel celular por período não superior a 30 (trinta) dias, renovável por uma única vez, por igual período;

III - para períodos superiores àquele de que trata o inciso II, será necessária a apresentação de ordem judicial.

§ 3º Na hipótese prevista neste artigo, o inquérito policial deverá ser instaurado no prazo máximo de 72 (setenta e duas) horas, contado do registro da respectiva ocorrência policial.

§ 4º Não havendo manifestação judicial no prazo de 12 (doze) horas, a autoridade competente requisitará às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz."

Como se depreende da leitura do texto atacado, a tentativa de proteção dos dados pessoais é feita pela distinção contida nas cabeças dos artigos 13-A e 13-B. Enquanto no art. 13-A é possível a requisição apenas de dados cadastrais, no art. 13-B, a requisição é a "dos meios técnicos adequados que permitam a localização da vítima ou dos suspeitos", ou seja, trata-se de espécie de requisição administrativa e não de garantia de restrição a dados.

Além disso, ainda de acordo com o *caput* do art. 13-B, que deve orientar a interpretação dos seus respectivos parágrafos, a requisição exige ordem judicial, mesmo ser for inferior a trinta dias.

Não há como negar a gravidade dos delitos que ensejam a adoção dessas medidas, como são o cárcere privado, a redução a condição análoga à de escravo, o tráfico de pessoas, o sequestro relâmpago, a extorsão mediante sequestro e o envio ilegal de criança ao exterior. Também não há

como deixar de reconhecer os esforços envidados pelo legislador para restringir esse poder de requisição apenas aos casos em que tiver sido instaurado o inquérito penal, ou seja, apenas no casos em que houver elementos mínimos da prática de um delito grave.

A doutrina tem sustentado que sem a restrição de quais aparelhos podem ser usados, sem indicação dos dados a serem mapeados, sem a determinação da intensidade, da profundidade, da continuidade e da duração da requisição, o mero recurso à expressão "dados cadastrais" é insuficiente para a promoção da privacidade na era digital (*Código de processo penal comentado* [livro eletrônico]/ coordenação Antonio Magalhães Gomes Filho, Alberto Zacharias Toron, Gustavo Henrique Badaró. 3ª ed. São Paulo: Thomson Reuters Brasil, 2020):

> "O disposto no art. 13-A do CPP, porém, é muito amplo, porque não delimita o que seriam tais dados cadastrais, se apenas de elementos identificadores, mas também não só do suspeito, e sim da vítima, esvaziando-se, assim, a proteção constitucional da privacidade."

Ademais, também não passou despercebido da doutrina um possível problema na interpretação do art. 13-B que admite a requisição de meios técnicos sem autorização judicial (*Código de processo penal comentado* [livro eletrônico]/ coordenação Antonio Magalhães Gomes Filho, Alberto Zacharias Toron, Gustavo Henrique Badaró. 3ª ed. São Paulo: Thomson Reuters Brasil, 2020):

> "O disposto no art. 13-A, § 2º, inc. III, prevê que, "para períodos superiores àquele de que trata o inciso II, será necessária a apresentação de ordem judicial", o que permite interpretação segundo a qual as informações de localização de um cidadão por período inferior a 30 dias dispensariam prévia autorização judicial, hipótese que configura afronta ao art. 5º, inc. X, da Constituição da República."

Nem tampouco, ainda de acordo com os mesmo autores, a possibilidade de se obter os dados sem autorização judicial, simplesmente pelo término do prazo de doze horas:

> "A previsão do § 4º do art. 13-B do CPP tem sua constitucionalidade questionada, porque prevê que, se não houver

> manifestação judicial no prazo exíguo de 12 horas, a Autoridade Policial ou o membro do Ministério Público poderá "requisitar" diretamente às empresas prestadoras de serviço de telecomunicações e /ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso, com imediata comunicação ao juiz.
>
> O dispositivo, sob argumento de urgência, dispensa autorização judicial, o que constitui afronta ao disposto no art. 5º, incs. X e XII, da Constituição da República."

Em que pese as manifestações trazidas pelos judiciosos autores, a norma impugnada não confere um 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.

Há, com efeito, cuidados precisos para restringir o poder de requisição apenas aos crimes listados no *caput* do art. 13-A. Além disso, a norma prevê a indicação do número de inquérito instaurado, o que, a um só tempo, denota que há indícios de autoria e materialidade, assim como supervisão judicial. Finalmente, a norma foi produzida pelo Congresso Nacional após longas investigações no âmbito da Comissão Parlamentar de Inquérito que investigava graves denúncias de tráfico de pessoas. A proposta, objeto de um longo processo de negociação, buscou dar ampla efetividade aos mecanismos de combate a essa modalidade de crime, cuja gravidade não apenas é reconhecida pela legislação brasileira, como também por diversos tratados internacionais de que o país é parte.

Os pedidos deduzidos pela requerente, no sentido de restringir os dados que podem ser requisitados, conquanto possam comportar discussões mais aprofundas em outras ações diretas, não merecem trânsito relativamente aos poderes de requisição para os crimes que atentam contra a liberdade pessoal, tal como os disciplinados pela redação do art. 13-A do Código de Processo Penal, quer por sua notável gravidade, quer porque foram objeto de especial seleção por parte do legislador, o que permitiu restringir tanto as autoridades públicas que têm poder de requisição, quanto as hipóteses em que esse poder se manifesta. Por isso, não há inconstitucionalidade na disposição normativa atacada.

Pleiteia a Associação Autora que seja dada interpretação conforme aos arts. 13-A e 13-B do Código de Processo Penal para se reconhecer a impossibilidade de requisição dos seguintes dados:

> (i) interceptação de voz;
> (ii) interceptação telemática;
> (iii) localização de terminal ou IMEI de cidadão em tempo real por meio de ERB;
> (iv) extrato de ERB;
> (v) 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;
> (vi) dados cadastrais dos terminais fixos não figurantes em lista telefônica divulgável e de terminais móveis;
> (vii) extrato de chamadas telefônicas;
> (viii) extrato de mensagens de texto (SMS ou MMS);
> (ix) serviços de agenda virtual ofertados por empresas de telefonia;
> (x) dado cadastral de e-mail;
> (xi) extratos de conexão de internet a partir de linha ou IP.

Sem embargo das considerações trazidas pela requerente, em relação aos delitos indicados no *caput* do art. 13-A do Código de Processo Penal, não há dúvida interpretativa sobre o alcance da expressão "dados cadastrais".

O texto constitucional e o próprio Pacto de São José da Costa Rica exigem lei para a requisição de dados em investigações criminais. É preciso, portanto, que haja uma investigação em curso, isto é, que indícios de autoria e materialidade tenham justificado a abertura de um procedimento investigatório, e que a lei atribua às autoridades competentes para a investigação o poder de requisição.

Não pode haver dúvidas de que as comunicações em si mesmas não podem ser interceptadas sem autorização judicial. Além da nitidez do texto constitucional, os precedentes desta Suprema Corte são fortes no sentido de que a diligência probatória é admissível apenas com a devida autorização (*v.g.* , HC 81.260, Rel. Min. Sepúlveda Pertence, Pleno, DJ 19.04.2002).

Ainda nessa mesma ordem de argumentação, exigem autorização judicial a interceptação de dados telemáticos e do conteúdo das mensagens de texto.

Isso não significa que o Estado deva deixar de dar respostas céleres e efetivas aos graves crimes que são objeto da lei impugnada e que foram bem retratadas na CPI dos tráfico de pessoas. Para isso é indispensável não apenas que preparar os órgãos de persecução para cumprirem sua função, como também o próprio Poder Judiciário, que deve manter uma estrutura de plantão permanente para autorizar as medidas mais restritivas à privacidade. Em nenhuma hipótese pode-se permitir que cumprimento integral das garantias constitucionais sejam empecilho à efetividade da repressão de crimes que configuram graves violações de direitos humanos.

Nada disso, porém, indica inconstitucionalidade no texto impugnado. À luz de todo o histórico da jurisprudência deste Tribunal, assim como do próprio teor do art. 5º, XII, da Constituição Federal, é inequívoca a interpretação segundo a qual na expressão "dados cadastrais" não estão incluídas a interceptação de comunicação ou de dados telemáticos.

Mesmo em relação à possibilidade de requisição de meios, como prevista no art. 13-B, não há que se falar em violação à reserva de jurisdição, eis que a possibilidade de requisição visa a identificação e localização imediata da vítima. O crime, portanto, está em evidente situação de flagrância, caso em que a própria norma constitucional admite a restrição à privacidade de forma mais aguda. Caso se tenha conta que essa previsão restringe-se apenas às hipótese dos crimes contra a liberdade pessoal, não há óbices para que o controle judicial possa ser feito posteriormente à realização da diligência, caso se demonstre sua imprescindibilidade.

No mesmo sentido, a possibilidade de requisição de informações contida no § 2º do art. 13-B não pode ser vista como impondo uma limitação ao que dispõe o próprio *caput* do mesmo artigo. Isto é, da leitura do art. 13-B, *caput*, não é possível depreender interpretação que admita a requisição de meios técnicos sem autorização judicial.

Inexistindo inconstitucionalidade ou dúvida interpretativa, não há como se declarar a inconstitucionalidade da interpretação.

Em relação ao pedido de restrição ao extrato de chamadas telefônicas e de mensagens de texto, assim como dos dados cadastrais dos terminais fixos, a solução consiste em reconhecer que não cuidam propriamente do

conteúdo das comunicações, mas apenas dos dados de registro. Diferentemente dos dados de acesso à internet, que são protegidos pelo Marco Civil da Internet, o extrato dos números contactados, que constam da própria conta detalhada de telefonia, não gozam da mesma proteção que se concede ao conteúdo da comunicação, conforme a jurisprudência já indicada deste Tribunal, mas também do Superior Tribunal de Justiça, representada neste preciso julgado de Relatoria do e. Ministro Gilson Dipp:

> "A quebra do sigilo dos dados telefônicos contendo os dias, os horários, a duração e os números das linhas chamadas e recebidas, não se submete à disciplina das interceptações telefônicas regidas pela Lei 9.296/96 (que regulamentou o inciso XII do art. 5º da Constituição Federal) e ressalvadas constitucionalmente tão somente na investigação criminal ou instrução processual penal."
>
> (STJ. EDcl no RMS 17732/MT. Quinta Turma. Ministro Gilson Dipp. Julgamento: 23.08.2005).

Por isso, não é possível equiparar, como defende a requerente, a proteção do conteúdo das comunicações telefônicas com o seu registro (itens "vi", "vii" e "viii", do pedido deduzido) a justificar, portanto, o indeferimento do pedido.

Com relação aos dados de conexão, como o número de IP e o endereço de e-mail, é preciso ter em conta que o Marco Civil da Internet, em seu art. 10, § 3º, restringe o alcance da expressão "dados cadastrais" apenas aos dados que informem "qualificação pessoal, filiação e endereço". Além disso, estabelece também que o fluxo das comunicações pela internet assim como as comunicações privadas armazenadas têm inviolabilidade e sigilo, somente podendo ser relativizado por ordem judicial. Finalmente, estabelece o Marco Civil a previsão de guarda das informações relativas aos registros de acesso à aplicação de internet, prevendo o sigilo a essas aplicações, que só poderá ser afastado, nos termos do art. 15, § 3º, por autorização judicial.

A previsão genérica de fornecimento de informações cadastrais, não pode prevalecer sobre a regra específica de sigilo constante do Marco Civil da Internet. Ainda que assim não fosse, é preciso reconhecer que a proteção por ele conferida se amolda à necessidade constitucional de ampliar o sentido da proteção à privacidade.

Em um precedente histórico, a Corte Europeia de Direitos, no caso *Benedik v. Slovenia* (Caso n. 62.357/14, de 24.07.2018), reconheceu que o número de IP é um dado pessoal e que a previsão genérica de entrega do número de IP à autoridade policial, conforme previsão constante do Código de Processo Criminal da Eslovênia, era insuficiente para resguardar a privacidade. O argumento central foi o de que a interação de usuário na internet pressupõe o anonimato como direito integrante da livre determinação informacional.

Em linha com essa diretriz, David Kaye, Relator Especial para a liberdade de expressão na internet, afirmou que o anonimato visa proteger os indivíduos dos poderes dos "metadados", isto é, da coleta em massa de dados, porquanto eles podem especificar o comportamento individual, as relações sociais, as preferências privadas e até mesmo a identidade das pessoas, como o próprio Conselho de Direitos Humanos já teve oportunidade de reconhecer (A/HRC/27/37, par. 19).

Quando do julgamento da ADPF 403, sobre a criptografia em comunicações na internet, asseverei que, na internet, a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações online como o e-mail, mensagens de texto e outras interações. Assim, se a proteção a liberdade de expressão *online* deve ter a mesma proteção que tem *offline* , não há como deixar de reconhecer que é legítima a expectativa de privacidade em relação as informações relativas aos dados de conexão por e-mail e por IP.

Por tudo isso, é também inequívoca a interpretação segundo a qual na expressão "dados cadastrais" não se incluem os dados de IP, que envolvam os dados de acesso em determinado dia, data, hora e fuso, assim como o próprio extrato de conexão protegidos pelo sigilo legal e o cadastro de e-mail (itens "v", "x" e "xi" do pedido deduzido), nos termos do art. 15 do Marco Civil da Internet. Inexistindo dúvida acerca da interpretação legal, não há como se conferir interpretação conforme.

Por fim, a requisição de dados que dizem respeito a um longo período de tempo, como, por exemplo, a coleta de informações sobre a localização por GPS de um suspeito podem representar ofensa ao direito à privacidade, caso não tenham sido autorizadas por um juiz, como decidiu a Corte Europeia de Direitos Humanos nos casos Uzun v. Alemanha (Caso n. 35.623 /05, de 02.10.2010) e Ben Faiza v. França (Caso n. 31.446/12, de 08.05.2018).

Imaginar possível uma expectativa de monitoramento ou vigilância contínua impediria o livre exercício da autodeterminação das pessoas.

De fato, há um problema em relação ao período em que se pretende ter acesso a essas informações. Como os metadados, se recolhidos de forma sistemática e duradoura, podem trazer mais informações do que o próprio conteúdo de uma única comunicação, é preciso restringir o alcance temporal dessas requisições. Essa restrição é justificada ainda pela própria exigência de uma causa provável para a requisição, ou seja, é preciso que haja indícios da prática de um crime e de sua autoria, devendo ser minimamente possível determinar um período de tempo em que a infração tenha potencialmente ocorrido. À exceção dos crimes praticados pela internet, a investigação policial não deve, como regra, principiar pela pesquisa genérica de informações cadastrais dos usuários de internet.

No âmbito do Marco Civil da Internet, essa proteção é determinada pela obrigação de guarda de informações relativamente a um período curto, conforme a previsão constante do art. 13 da Lei. No entanto, os dados relativos aos extratos de ERB e aos telefones conectados a respectiva estação não estão a rigor disciplinados pelo Marco Civil.

Por isso, a requisição feita pela autoridade policial, exclusivamente para o crimes previstos no art. 13-A do Código de Processo Penal, conquanto possível, deve se restringir apenas à finalidade a que foi fixada, qual seja, a de reprimir e impedir a ocorrência dos delitos descritos no *caput* .

A restrição à privacidade imposta por essa medida é potencialmente grave, no entanto, não deve haver expectativa de privacidade para quem está em situação de flagrante delito de crime grave com vítimas submetidas à restrição de liberdade.

Em suma, na expressão "dados cadastrais" não estão abrangidas 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. Para esses dados, como não poderia deixar de ser, remanesce a necessidade de autorização judicial.

Continuam sendo 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; o extrato de ERB; os dados cadastrais dos terminais fixos não figurantes em lista telefônica divulgável e de terminais móveis; o extrato de chamadas telefônicas; o extrato de mensagens de texto (SMS ou MMS); e os sinais para localização de vítimas ou suspeitos, após o decurso do prazo de 12 horas constante do § 4º do art. 13-B do Código de Processo Penal.

Nada obstante, porque não há dúvida sobre a interpretação constitucionalmente adequada desse dispositivo, é desnecessário que este Supremo Tribunal Federal dê a ele interpretação conforme.

Ante o exposto, reconhecendo constitucional o diploma impugnado e não vislumbrando dúvida sobre a interpretação constitucionalmente adequada da norma, julgo improcedente a presente ação direta.

É como voto.