

**AÇÃO DECLARATÓRIA DE CONSTITUCIONALIDADE 91 DISTRITO
FEDERAL**

RELATOR	: MIN. CRISTIANO ZANIN
REQTE.(S)	: ASSOCIACAO BRASILEIRA DE PROVEDORES DE INTERNET E TELECOMUNICACOES
ADV.(A/S)	: GUSTAVO DE MELO FRANCO TORRES E GONCALVES E OUTRO(A/S)
INTDO.(A/S)	: PRESIDENTE DA REPÚBLICA
PROC.(A/S)(ES)	: ADVOGADO-GERAL DA UNIÃO
INTDO.(A/S)	: CONGRESSO NACIONAL
PROC.(A/S)(ES)	: ADVOGADO-GERAL DA UNIÃO
ADV.(A/S)	: GABRIELLE TATITH PEREIRA
ADV.(A/S)	: FERNANDO CESAR DE SOUZA CUNHA
ADV.(A/S)	: MATEUS FERNANDES VILELA LIMA
ADV.(A/S)	: RODRIGO PENNA COSTA E COSTA
ADV.(A/S)	: ANA CRISTINA DIOGENES REGO
AM. CURIAE.	: CONSELHO NACIONAL DE PROCURADORES- GERAIS DO MINISTÉRIO PÚBLICO DOS ESTADOS E DA UNIÃO - CNPG
PROC.(A/S)(ES)	: PROCURADOR-GERAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS

VOTO

O Senhor Ministro **CRISTIANO ZANIN** (Relator): Pretende-se, na presente ação, a declaração de constitucionalidade e a análise do alcance interpretativo do art. 10, § 1º, da Lei n. 12.965/2014 (Marco Civil da Internet — MCI) no que se refere à requisição de dados cadastrais e à exigência de ordem judicial prévia para acesso a registros de conexão.

I. Pressupostos de admissibilidade da ação declaratória de constitucionalidade

De início, reconheço a legitimidade ativa da requerente para a propositura da presente ação declaratória de constitucionalidade, nos termos do art. 103, IX, da Constituição da República, tendo em vista se

ADC 91 / DF

tratar de entidade de alcance nacional. A legitimidade *ad causam* da requerente para a propositura de ações de controle de constitucionalidade já foi reconhecida em outros julgados do Supremo Tribunal Federal (ADI 7.379, Rel. Min. Gilmar Mendes, Tribunal Pleno, DJe 1º/10/2025; ADI 7.211, Rel. Min. Alexandre de Moraes, Tribunal Pleno, DJe 10/10/2022).

Também estão presentes os demais pressupostos de admissibilidade: (i) foi demonstrada a existência de controvérsia judicial relevante; (ii) foram adequadamente definidos o ato questionado (art. 10, § 1º, da Lei n. 12.965/2014) e os fundamentos jurídicos do pedido veiculado na inicial; (iii) foi juntada a procuração com poderes específicos para propor a ação (doc. 3).

No que se refere à “controvérsia judicial relevante”, o Supremo Tribunal Federal já firmou entendimento de que é essencial dissídio jurisprudencial em proporções expressivas, isto é, divergência interpretativa de tal intensidade que produza insegurança jurídica (ADC 23 AgR, Rel. Min. Edson Fachin, Tribunal Pleno, DJe 1º/2/2016).

A requerente, por sua vez, demonstrou a existência de múltiplos pedidos expedidos por autoridades públicas requisitando "dados cadastrais de IP", inclusive com instauração de investigações contra os representantes de provedores que deixaram de atendê-las, sob a imputação do delito de desobediência (docs. 6-15).

Além disso, comprovou a ocorrência de julgados contraditórios de juízes e dos Tribunais dos Estados de Mato Grosso do Sul, do Paraná e de Santa Catarina, além de precedente do Tribunal Regional Federal da 5ª Região e do Superior Tribunal de Justiça (doc. 17-26). Os documentos apresentados demonstram, na minha compreensão, cenário de insegurança jurídica suficiente a justificar a propositura da presente ação declaratória de constitucionalidade.

Assim, pelos motivos acima expostos, conheço da presente ação declaratória de constitucionalidade e passo à análise do mérito.

II. Privacidade, proteção de dados e autodeterminação informacional

A questão ora em exame consiste em determinar se é constitucional a exigência de ordem judicial para disponibilização de registros de conexão pelo Marco Civil da Internet (art. 10, § 1º, da Lei n. 12.965/2014), assim como se a interpretação desse dispositivo permite concluir que o fornecimento de dados cadastrais vinculados a registros de conexão, para permitir a identificação de usuários, exige ordem judicial (§ 1º) ou pode ser requisitado diretamente pela autoridade policial ou Ministério Público (§ 3º).

Trata-se, portanto, de debate vinculado à proteção constitucional dos direitos fundamentais à **autodeterminação informacional**, à **privacidade** (art. 5º, X, da Constituição Federal – CF) e à **proteção de dados pessoais** (art. 5º, LXXIX, da CF).

O direito à privacidade garante aos indivíduos um espaço para o livre desenvolvimento da personalidade, no qual possam expressar convicções, “sentimentos, reflexões, visões de mundo e experiências pessoais sem medo de estar sendo observados por órgãos estatais” (GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, set./dez. 2019, p. 1495), o que abrange a autonomia individual sobre os próprios dados pessoais que, sobretudo se analisados em conjunto, expressam a individualidade do sujeito.

Esse direito, destarte, permite que o indivíduo aja com espontaneidade no seu âmbito privado, tendo a liberdade de ser quem ele

é, sabendo que, em circunstâncias normais, não será vigiado pelo Estado.

A respeito da privacidade, ensina Stefano Rodotà:

As discussões teóricas e as complexas experiências dos últimos anos demonstram que a privacidade se apresenta, enfim, como noção fortemente dinâmica e que se estabeleceu uma estreita e constante relação entre as mudanças determinadas pelas tecnologias da informação (mas também pelas tecnologias da reprodução, pela engenharia genética) e as mudanças em seu conceito. Uma definição da privacidade como “direito de ser deixado só” perdeu há muito tempo seu valor genérico, ainda que continue a abranger um aspecto essencial do problema e possa (deva) ser aplicada a situações específicas. Na sociedade da informação tendem a prevalecer definições funcionais da privacidade que, de diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas. Assim, a privacidade pode ser definida, mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações (RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008, p. 92).

Conforme ressaltou José Afonso da Silva, a privacidade abrange o conjunto de informações a respeito do indivíduo, de modo que apenas ele poderá decidir se deseja mantê-las “sob seu exclusivo controle” ou se prefere comunicá-las, “decidindo a quem, quando, onde e em que condições” quer fazê-lo (SILVA, José Afonso da. *Curso de direito constitucional positivo*. Rio de Janeiro: Malheiros, 2002. p. 205).

Nesse contexto, o Tribunal Federal Constitucional alemão, por ocasião da emblemática decisão do censo (BVerfGE 65, 1), a qual consagrou

de forma pioneira o direito à autodeterminação informacional, ressaltou que “o livre desenvolvimento da personalidade sob as condições modernas do processamento de dados, pressupõe a proteção do indivíduo contra irrestritas faculdades de obtenção, armazenamento, utilização e transferência de seus dados pessoais” (GRECO, Luís. Considerações introdutórias sobre o processo penal alemão. *In*: WOLTER, Jürgen. *O inviolável e o intocável no direito processual penal*. São Paulo: Marcial Pons, 2018. p. 43).

Assim, com a consagração do **direito amplo à proteção de dados pessoais**, deve-se assegurar, ao lado do sigilo das telecomunicações, outros âmbitos de proteção, como o direito à autodeterminação informacional (a respeito, cf. GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública*. São Paulo: Marcial Pons, 2021. p. 37).

Esse direito foi expressamente reconhecido pelo Supremo Tribunal Federal antes mesmo da Emenda Constitucional 115/2022, como se pode conferir também nos seguintes julgamentos: ADI 6.387 (Rel. Min. Rosa Weber, Tribunal Pleno, DJe 12/11/2020); ADI 6.529 (Rel. Min. Cármen Lúcia, Tribunal Pleno, DJe 22/10/2021); ADI 6.649 e da ADPF 695 (Rel. Min. Gilmar Mendes, Tribunal Pleno, DJe 19/6/2023).

Após a promulgação da referida Emenda Constitucional, que elencou expressamente o direito à proteção de dados pessoais (art. 5º, LXXIX, da CF), a reafirmação do direito à autodeterminação informacional tomou ainda maior importância (cito, por exemplo, ADI 6.561, Rel. Min. Edson Fachin, Tribunal Pleno, DJe 3/11/2023; ADI 5.642, Rel. Min. Edson Fachin, Tribunal Pleno, DJe 22/8/2024), como reiterou esta Suprema Corte em julgados recentes, que evidenciam a centralidade dessa garantia no contexto do tratamento de dados pessoais.

Nesse sentido, reconheceu-se que:

[...] A possibilidade de se acessar, por meio de aparelhos celulares, bem mais que metadados relativos à comunicação telefônica desloca a discussão travada nos autos para a questão da **inviolabilidade da intimidade, da vida privada, da honra e da imagem (CF/88, art. 5º, inciso X), do direito à proteção dos dados pessoais, inclusive nos meios digitais (CF/88, art. 5º, inciso LXXIX, introduzido pela Emenda Constitucional no 115, de 2022), e do direito à autodeterminação informacional, os quais conferem proteção jurídica especial e diferenciada aos dados pessoais armazenados e justificam a superação do entendimento firmado no HC no 91.867/PA para se construir uma solução mais condizente com a nova realidade [...]** (ARE 1.042.075, Rel. Min. Dias Toffoli, Tribunal Pleno, DJe 24/9/2025).

[...] O direito fundamental à proteção de dados e à autodeterminação informativa (CF, art. 5º, 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 4906, Rel. Min. Nunes Marques, Tribunal Pleno, DJe 24/10/2024).

No julgamento da ADI 4.906, inclusive, reconheci a aplicabilidade da Lei Geral de Proteção de Dados (Lei n. 13.709/2018) à matéria penal, no que for compatível e na pendência da promulgação de uma esperada LGPD Penal.

Com efeito, o **direito à autodeterminação informacional atribui ao titular dos dados a liberdade de (auto)determinar e, portanto, de controlar se e dentro de quais limites essas informações que revelam fatos de sua vida pessoal poderão ser objeto de intervenção. Como demonstrado, ele é um direito autônomo, que tem relação direta com o**

direito à privacidade (inciso X do art. 5º da CF) e está expressamente protegido pelo novo inciso LXXIX do art. 5º da Constituição, vinculando-se, em última instância, ao direito geral ao livre desenvolvimento da personalidade, inerente à dignidade humana.

Há que se superar, assim, a considerável diferenciação antes defendida entre a proteção constitucional atribuída a dados em fluxo e a dados armazenados, derivada da clássica distinção sustentada por Tércio Sampaio Ferraz Júnior (Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 88, 1993, p. 439-59) e incorporada em importantes precedentes desta Suprema Corte, como no RE 418.416, da relatoria do eminente Ministro Sepúlveda Pertence (Tribunal Pleno, DJ 19/12/2006), e no HC 91.867, da relatoria do eminente Ministro Gilmar Mendes (Segunda Turma, DJe 20/9/2012).

Isso, inclusive, já vem sendo reconhecido pelo Supremo Tribunal Federal:

EMENTA Recurso extraordinário com agravo. Julgamento sob a sistemática da repercussão geral. Constitucional. Processual penal. Aparelho celular encontrado fortuitamente no local do crime. Acesso à agenda telefônica, aos registros de chamadas e às fotografias arquivadas no aparelho sem prévia autorização judicial. (...) 4. Examinados em conjunto, dados e metadados revelam um espectro enorme de dados pessoais, o que torna possível uma investigação completa e – diga-se de passagem – muito eficiente acerca das preferências pessoais, das relações familiares e interpessoais, dos hábitos de vida, de trabalho e de consumo e, em última análise, da forma de pensar, de agir e de decidir de determinado indivíduo. Isso sem falar, obviamente, das facilidades que o acesso proporciona para a intrusão indevida e “para o futuro”, a partir da instalação de

softwares “espiões”. 5. A possibilidade de se acessar, por meio de aparelhos celulares, bem mais que metadados relativos à comunicação telefônica desloca a discussão travada nos autos para a questão da inviolabilidade da intimidade, da vida privada, da honra e da imagem (CF/88, art. 5º, inciso X), do direito à proteção dos dados pessoais, inclusive nos meios digitais (CF/88, art. 5º, inciso LXXIX, introduzido pela Emenda Constitucional nº 115, de 2022), e do direito à autodeterminação informacional, os quais conferem proteção jurídica especial e diferenciada aos dados pessoais armazenados e justificam a superação do entendimento firmado no HC nº 91.867/PA para se construir uma solução mais condizente com a nova realidade. 6. Após revisitar os precedentes sobre a matéria, verifica-se que a jurisprudência do Supremo Tribunal Federal acabou encampando, ao menos em parte, o texto seminal do Professor Tércio Sampaio Ferraz Júnior, para quem, “[o] sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade”. Isso não significa, contudo, que o texto constitucional asseguraria proteção jurídica apenas e tão somente à “comunicação de dados”, isto é, ao “fluxo comunicacional”, ou aos “dados em trânsito”. Como lembrou Ferraz Júnior, os “dados estáticos”, ou seja, os “dados armazenados” também são passíveis de proteção jurídica e, embora não se revistam sempre e incondicionalmente de caráter sigiloso, podem alcançar tal qualidade a depender das circunstâncias, encontrando guarida, por exemplo, no disposto no art. 5º, inciso X, do texto constitucional. 7. A Emenda Constitucional nº 115, de 2022, ao introduzir no art. 5º da Constituição o inciso LXXIX, segundo o qual “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” e, antes dela, as Leis nº 12.695/14 e nº 13.709/18, que instituíram no ordenamento jurídico brasileiro, respectivamente, o Marco Civil da Internet e a Lei Geral de Proteção de Dados, passaram a conferir proteção jurídica especial e autônoma aos dados pessoais. Assim, enquanto o

primeiro diploma legal elevou ao patamar de direito dos usuários de internet a inviolabilidade e o sigilo de suas comunicações privadas armazenadas e o não fornecimento de seus dados pessoais, a segunda lei alçou a proteção jurídica dos dados pessoais a uma categoria autônoma com relação aos direitos à privacidade e à intimidade (CF, art. 5º, inciso X). 8. Não se pode olvidar, ainda, que o direito à privacidade, apesar de relativamente recente, passou – e ainda passa – por considerável ressignificação. É dizer, no contexto da sociedade atual, a possibilidade de o indivíduo proceder ao controle dos dados que dizem respeito à própria pessoa – porque eles consistem em manifestação de sua personalidade – é *conditio sine qua non* para a preservação de sua personalidade e para o desenvolvimento pleno de sua autonomia. Isso porque é o direito à privacidade que assegura a cada indivíduo um espaço próprio de experimentação, no qual é possível a cada qual expressar “sentimentos, reflexões, visões de mundo e experiências pessoais sem medo de estar sendo observado por órgãos estatais” (GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. Revista Brasileira de Direito Processual Penal. Porto Alegre, v. 5, n. 3, set./dez. 2019, p. 1495). (ARE 1.042.075, Rel. Min. Dias Toffoli, Tribunal Pleno, DJe 24/9/2025).

Habeas corpus. 2. Acesso a aparelho celular por policiais sem autorização judicial. Verificação de conversas em aplicativo WhatsApp. Sigilo das comunicações e da proteção de dados. Direito fundamental à intimidade e à vida privada. Superação da jurisprudência firmada no HC 91.867/PA. Relevante modificação das circunstâncias fáticas e jurídicas. Mutações constitucionais. Necessidade de autorização judicial. 3. Violação ao domicílio do réu após apreensão ilegal do celular. 4. Alegação de fornecimento voluntário do acesso ao aparelho telefônico. 5. Necessidade de se estabelecer garantias para a efetivação do direito à não autoincriminação. 6. Ordem concedida para

declarar a ilicitude das provas ilícitas e de todas dela derivadas (HC 168.052, Rel. Min. Gilmar Mendes, Segunda Turma, DJe 2/12/2020).

Não há dúvida, portanto, que os chamados “dados estáticos” são também objeto de proteção pela Constituição da República de 1988.

O reconhecimento de direitos fundamentais impõe ao Estado um dever geral de abstenção. Considerando, contudo, que na persecução penal a intervenção em direitos fundamentais é necessária para fins investigativos, esse dever poderá ser afastado por meio de uma justificação especial fundada em lei proporcional.

Assim, a intervenção no direito fundamental à privacidade para fins de persecução penal é possível, mas depende da observância de determinados limites. O parâmetro de legitimação dessas intervenções vincula-se sobretudo a dois princípios da dogmática constitucional: o **princípio da reserva de lei** e o **princípio da proibição de excesso**, que exige a proporcionalidade da medida interventiva (A respeito, cf. GLEIZER; MONTENEGRO; VIANA. *O direito de proteção de dados no processo penal e na segurança pública*. p. 40).

A exigência de autorização legal deriva não apenas do art. 5º, II, da Constituição Federal (“II – ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”), como também do art. 11, 2, primeira parte, da Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), da qual o Brasil é signatário (Decreto 678/1992), que estabelece que “[ninguém] pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada”.

Considerando que o compartilhamento de dados pessoais de usuários pelos provedores de conexão é uma intervenção no direito fundamental à autodeterminação informacional, há que se avaliar a extensão da

autorização contida no Marco Civil da Internet (infra III) e a proporcionalidade da proteção conferida pela lei (infra IV).

III. O plano da legalidade: a proteção dos dados cadastrais, dados de tráfego e dados de conteúdo no Marco Civil da Internet

O dispositivo ora questionado assim estabelece:

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .

São também relevantes para a análise do presente caso:

§ 2º O conteúdo das comunicações privadas 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 .

§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

Como se nota, o Marco Civil da Internet – assim como o direito europeu de proteção de dados (veja-se o recente Regulamento UE 2023/1543 do Parlamento Europeu e do Conselho de 12 de julho de 2023) e a Convenção de Budapeste sobre o Crime Cibernético – faz uma distinção entre **dados cadastrais**, **dados de tráfego** e **dados de conteúdo** e estipula diferentes padrões de proteção para cada um deles.

Os **dados cadastrais**, conforme definição do próprio Marco Civil da Internet (art. 10, § 3º, da Lei n. 12.965/2014), compreendem informações básicas de identificação, como a **qualificação pessoal, filiação e endereço** de uma pessoa determinada. O Decreto n. 8.771/2016, que regulamenta a referida lei, também consagra o mesmo conceito:

Da requisição de dados cadastrais

Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.

§ 1º O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados.

§ 2º **São considerados dados cadastrais:**

I - a filiação;

II - o endereço; e

III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

§ 3º Os pedidos de que trata o caput **devem especificar os indivíduos cujos dados estão sendo requeridos** e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.

Os dados cadastrais, que são armazenados nas bases de dados dos provedores de conexão, **podem ser requisitados diretamente pela**

autoridade policial e pelo Ministério Público (ou, a depender do caso, outra autoridade competente), conforme autorização prevista não apenas no art. 10, § 3º, da Lei n. 12.965/2014, mas também no art. 15 da Lei de Organizações Criminosas (Lei n. 12.850/2013), no art. 17-B da Lei de Lavagem de Capitais (Lei n. 9.613/1998) e no art. 13-A do Código de Processo Penal. Os dois últimos, inclusive, já tiveram a sua constitucionalidade reconhecida pelo Supremo Tribunal Federal, nas ADIs 5.642 e 4.906.

Nesse contexto, entendo que essa autorização instituída pelo Marco Civil da Internet está em consonância com as orientações da Convenção de Budapeste sobre o Crime Cibernético, promulgada no Brasil pelo Decreto n. 11.491/2023, que prevê no art. 18, item 3, que a possibilidade de que autoridades competentes ordenem o compartilhamento de “informações cadastrais do assinante” não abrange dados de tráfego e dados de conteúdo.

Ressalto que o Supremo Tribunal Federal vem interpretando o conceito de dados cadastrais tal como determinado no Marco Civil da Internet, elucidando, em diferentes julgados, que esse conceito abrange **apenas dados cadastrais básicos (a qualificação pessoal, a filiação e o endereço)** (ADI 5.642, Rel. Min. Edson Fachin, Tribunal Pleno, DJe 22/8/2024; ADI 4.906, Rel. Min. Nunes Marques, Tribunal Pleno, DJe 24/10/2024).

Os **dados de tráfego**, por sua vez, são metadados referentes à conexão ou ao acesso, que permitam a identificação do usuário. Eles abrangem os registros de conexão e os registros de acesso a aplicações de internet, também definidos no Marco Civil da Internet:

Art. 5º [...]

V - conexão à internet: a habilitação de um terminal para

envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à **data e hora de início e término de uma conexão à internet, sua duração e o endereço IP** utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à **data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP**.

Em síntese, os provedores de aplicações de internet disponibilizam aos usuários diversas funcionalidades – como redes sociais, serviços de mensagens e plataformas de compartilhamento de conteúdo. Tais aplicações são acessadas por meio de um terminal apto ao envio e recebimento de dados, conectado à rede de computadores mediante um endereço de Protocolo de Internet (IP). Os dados de tráfego abrangem os registros dessas conexões e do uso dessas aplicações.

Convém esclarecer que o endereço de IP é uma sequência numérica que identifica um dispositivo ou conexão na internet, possibilitando a troca de dados na rede entre sistemas que utilizam a mesma família de protocolos (a respeito, ver PECK, Patrícia. *Direito Digital*. 7. ed. São Paulo: Saraiva, 2021, p. 624). O art. 5º, VI e VIII, prevê expressamente que o endereço IP integra o conjunto de informações que constituem registros de conexão ou de acesso a aplicações de internet.

Em relação aos dados de tráfego, que são mais reveladores do que os cadastrais, a lei criou uma obrigação de retenção de informações e exige a guarda de registros de conexão por provedores de conexão à internet, que

fornece acesso à rede, pelo prazo de um ano (art. 13) e a guarda de registros de acesso a aplicações de internet pelo prazo de seis meses (art. 15).

O Marco Civil da Internet também prevê a possibilidade de requisição, pela autoridade policial ou administrativa ou o Ministério Público, de guarda cautelar dos dados de tráfego por prazo superior ao previsto na lei, para posterior análise judicial (art. 13, §§ 2º a 4º e art. 15, § 2º).

A exigência de retenção de dados de tráfego instituída pelo Marco Civil da Internet destina-se fundamentalmente à possibilidade de identificar os indivíduos que se prevalecem da anonimidade para praticar crimes por meio da internet (LIMA, Marcelo Chiavassa de Mello Paula; ANDRADE, Vitor Morais de. *Manual de Direito Digital*. 2. ed. São Paulo: Tirant lo blanch, 2023. p. 119).

Se esses dados não fossem retidos, seria consideravelmente mais difícil, por exemplo, identificar o endereço de IP de um sujeito que publica conteúdo calunioso em rede social, tendo em vista que a necessidade de acessar esses dados para identificar o criminoso somente surge após a realização da postagem.

Nos termos do art. 10, § 1º, do Marco Civil da Internet, “o provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, 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**”. Desse modo, o fornecimento desses registros de conexão e de acesso a aplicações, quando destinados à identificação do usuário ou do terminal, encontra-se submetido à reserva de jurisdição.

Já os **dados de conteúdo** correspondem às informações que permitem o acesso ao teor das interações digitais do usuário, como as comunicações privadas armazenadas. Diante da ausência de uma definição expressa no Marco Civil da Internet, pode-se recorrer à conceituação adotada no Regulamento UE 2023/1543 do Parlamento Europeu e do Conselho, que os concebem como “dados num formato digital, como texto, voz, vídeos, imagens e som”, que não sejam dados cadastrais ou de tráfego.

Tendo em vista que os dados de conteúdo são ainda mais relevantes que os de tráfego, o Marco Civil da Internet não exige que provedores armazenem o conteúdo das comunicações realizadas no âmbito dos acessos feitos pelos usuários. Porém, conforme entendo, a Lei n. 12.965/2014 permite, nos §§ 1º e 2º do art. 10, que esses dados sejam compartilhados pelos provedores, na eventualidade de estarem efetivamente guardados, contanto que haja determinação judicial.

IV. O plano da proporcionalidade

Na análise da proporcionalidade, há que se reconhecer que existem **diferentes graus de intervenção** no direito à autodeterminação informacional. Podemos recorrer, aqui, à **teoria das esferas**, que permite enxergar os distintos níveis de afetação do direito geral de personalidade.

De acordo com essa teoria, a compreensão da esfera privada deve ser analisada com base em três círculos concêntricos. Quanto mais próxima do núcleo estiver uma intervenção estatal, mais rigorosas deverão ser as exigências de proporcionalidade para que se admita o ingresso na esfera em questão (LANG, Heinrich; WILMS, Heinrich. *Staatsrecht II: Grundrechte*. 2. ed. Stuttgart: Kohlhammer, 2020, p. 126).

No círculo externo está a **esfera social ou pública**, que abrange informações sobre a profissão ou outros aspectos a respeito do indivíduo cujo conteúdo é público (o que ele posta em redes sociais abertas, por

exemplo) e na qual é possível intervir sem maiores exigências de justificação.

No círculo intermediário está a **esfera privada ou do sigilo**, e a intervenção nesse âmbito, que abrange informações sobre as contas bancárias, extratos telefônicos, a rotina, as compras ou o círculo de amizades do indivíduo, exige um grau mais intenso de justificação.

Por fim, no terceiro e mais restrito círculo está o **núcleo da esfera privada**, o qual expõe uma dimensão tão íntima do indivíduo que inviabiliza a justificação de intervenções (a respeito, ver GRECO, *Considerações introdutórias sobre o processo penal alemão*, p. 34).

A aplicação da lógica da teoria das esferas explicita que nem toda intervenção deve depender de autorização judicial, sobretudo se estiver no âmbito mais externo da sua esfera de proteção, como os dados cadastrais.

Assim, a proteção conferida aos dados pessoais pelo Marco Civil da Internet é, a meu ver, proporcional.

Como já me manifestei por ocasião do julgamento da ADI 4.906 (Rel. Min. Nunes Marques, Tribunal Pleno, DJe 24/10/2024), **não se pode excluir os dados cadastrais do âmbito de proteção do direito à autodeterminação informacional**. Conforme frisou a eminente Ministra Rosa Weber no julgamento da ADI 6.387 MC-Ref (Rel. Min. Rosa Weber, Tribunal Pleno, DJe 12/11/2020), na mesma linha do que havia sido reconhecido pelo Tribunal Federal Constitucional alemão na decisão do censo (BVerfGE 65, 1 [p. 45]), **não há dados insignificantes ou irrelevantes** no contexto hodierno, considerando as condições do processamento automático de dados, que permite a formação de perfis informacionais de muita relevância para o Estado e para o mercado.

Assim, o fato de que se trata de dados menos reveladores não os exclui

do âmbito de proteção dos direitos à privacidade e à autodeterminação informacional, tampouco dispensa a exigência de reserva legal e proporcionalidade para autorizar eventual tratamento desses dados.

Embora os dados cadastrais integrem o âmbito de proteção do direito fundamental à autodeterminação informacional, há lei que autoriza a requisição direta desses dados (art. 10, § 3º, da Lei n. 12.965/2014), e a dispensa da ordem judicial para requisitá-los é proporcional, porquanto esses dados se encontram no estrato mais externo da esfera de proteção. É razoável, portanto, o seu compartilhamento mediante requisição direta de autoridades públicas.

Por sua vez, apesar da obrigação de guarda dos **dados de tráfego**, de acordo com as regras estipuladas pelo Marco Civil da Internet – o que já é, em si, um tratamento de dados, mostra-se proporcional que o acesso a eles dependa de ordem judicial específica e fundamentada, nos termos do art. 22 do Marco Civil da Internet:

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

- I - fundados indícios da ocorrência do ilícito;
- II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
- III - período ao qual se referem os registros.

Com efeito, o acesso a metadados permite traçar perfis comportamentais, como com qual frequência e em que momentos a pessoa se comunica; a reconstrução de rotinas diárias e redes de contato físico.

Trata-se, outrossim, de dados que podem ser reveladores e que potencialmente se aproximam mais da esfera íntima do que da esfera pública, sendo proporcional a exigência legal de ordem judicial para acessá-los.

Por fim, os **dados de conteúdo**, que se aproximam ainda mais do núcleo da esfera privada, devem ser protegidos com maior intensidade. Em relação a eles, o Marco Civil da Internet não institui uma obrigação de guarda e é proporcional que o seu compartilhamento somente possa ser realizado mediante ordem judicial que fundamente os critérios adotados.

De todo o exposto, considero que o modelo formulado no Marco Civil da Internet é constitucional e assegura, nesse ponto, salvaguarda proporcional à privacidade e à autodeterminação informacional dos usuários.

Impõe-se, assim, **reconhecer a constitucionalidade do art. 10, § 1º, da Lei n. 12.965/2014**, que condiciona ao crivo judicial o acesso a dados de tráfego – “de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal” –, preservando a reserva de jurisdição como garantia essencial contra ingerências indevidas na esfera privada.

V. Compartilhamento de dados cadastrais vinculados a registros de conexão

A requerente demonstrou que os provedores de conexão à internet têm sido recorrentemente confrontados com requisições do que se convencionou denominar de “dados cadastrais de IP”. Essas solicitações referem-se ao compartilhamento de dados cadastrais de pessoa ainda não identificada, a partir do fornecimento, pela autoridade requisitante, dos registros de conexão (IP, data, hora e fuso horário). Solicita-se, assim, que

o provedor de conexão proceda à vinculação entre os dados de conexão fornecidos pela autoridade requisitante e os dados cadastrais, permitindo, assim, a identificação do usuário.

Contudo, como já ressaltai, as decisões proferidas nas ADIs 5.642 e 4.906 foram categóricas em determinar que a autorização legal para requisição direta **se limita ao acesso a dados cadastrais básicos** — qualificação pessoal, filiação e endereço.

Assim, a autorização para requisição direta **não abrange** outras informações como **os dados cadastrais de usuários de IP, os quais abarcam dados de usuário que, em determinado dia, data, hora e fuso, utilizou um IP para acessar a 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.

Nesse sentido:

Ementa: AÇÃO DIRETA DE INCONSTITUCIONALIDADE DIREITO CONSTITUCIONAL. AÇÃO DIRETA DE INCONSTITUCIONALIDADE. DADOS CADASTRAIS DE VÍTIMAS E SUSPEITOS. ACESSO. REQUISIÇÃO DO MINISTÉRIO PÚBLICO E AUTORIDADE POLICIAL. POSSIBILIDADE. DISPONIBILIZAÇÃO MEIOS TÉCNICOS PARA LOCALIZAÇÃO DE VÍTIMAS E SUSPEITOS. ORDEM JUDICIAL. CONSTITUCIONALIDADE. IMPROCEDÊNCIA DOS PEDIDOS CONTIDAS NA AÇÃO DIRETA.

I. CASO EM EXAME

1. A ação direta questiona a constitucionalidade dos artigos 13-A e 13-B do Código de Processo Penal (CPP), incluídos pela Lei nº 13.344/2016, os quais preveem que os membros do Ministério Público e os Delegados de Polícia que investiguem

crimes previstos nos arts. 148, 149 e 149-A, no §3º do art. 158 e no art. 159 do Código Penal e no art. 239 do Estatuto da Criança e do Adolescente, podem requisitar dados e informações cadastrais sobre vítimas ou suspeitos diretamente aos órgãos do poder público e às empresas privadas (art. 13-A). Assim como, se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, 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 (art. 13-B).

II. QUESTÃO EM DISCUSSÃO

2. Saber se a requisição direta pelo Ministério Público ou pela autoridade policial dos dados cadastrais de vítimas e suspeitos, para apurar a prática dos crimes previstos no art. 13-A e a disponibilização de meios técnicos, com autorização judicial, para a localização de vítimas e suspeitos no contexto da prática do crime disposto no art. 13-B, violam a proteção constitucional da privacidade.

III. RAZÕES DE DECIDIR

1. As 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.

2. A requisição apresentada 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, do citado dispositivo.

3. 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.

4. Da leitura do art. 13-B, caput, não é possível depreender interpretação que admita a requisição de meios técnicos sem autorização judicial.

5. 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.

6. O disposto no art. 13-B é aplicável aos delitos previstos no art. 13-A, de acordo com decisão da maioria do Tribunal.

IV. DISPOSITIVO E TESE 1. Reconhecida a constitucionalidade do diploma impugnado e não vislumbrando dúvida sobre a interpretação constitucionalmente adequada da norma, pedidos contidos na presente ação direta julgados improcedentes. 2. 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; 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” (ADI 5.642, Rel. Min. Edson Fachin, Tribunal Pleno, DJe 22/8/2024).

EMENTA AÇÃO DIRETA DE INCONSTITUCIONALIDADE. LEI N. 9.613/1998, ART. 17-B. COMPARTILHAMENTO DE DADOS CADASTRAIS COM ÓRGÃOS DE PERSECUÇÃO CRIMINAL. DESNECESSIDADE DE AUTORIZAÇÃO JUDICIAL. 1. A Associação Brasileira de

Concessionárias de Serviço Telefônico Fixo Comutado (Abrafix) não tem legitimidade para impugnar inteiro teor de dispositivo quando impactadas entidades por ela não representadas. Preliminar da Advocacia-Geral da União acolhida, conhecendo-se parcialmente da ação, somente no que diz respeito à expressão “empresas telefônicas”. 2. Conforme entendimento do Supremo, a proteção versada no art. 5º, XII, da Constituição Federal refere-se à comunicação de dados, e não aos dados em si mesmos. 3. O direito à privacidade, entre os instrumentos de tutela jurisdicional, se consubstancia no sigilo, que consiste na faculdade de resistir ao devassamento de informações cujo acesso e divulgação podem ocasionar dano irreparável à integridade moral do indivíduo. O acesso ao conteúdo de certos objetos é medida excepcional que depende de autorização judicial e somente se justifica para efeito de investigação criminal ou instrução processual penal. 4. O objeto de tutela mediante a imposição de sigilo não alcança os dados cadastrais. Isso não significa que essas informações dispensem tutela jurisdicional, mas apenas que a tutela em virtude do direito à privacidade não se concretiza via sigilo. 5. O direito fundamental à proteção de dados e à autodeterminação informativa (CF, art. 5º, LXXIX) impõe a adoção de mecanismos capazes de assegurar a proteção e a segurança dos dados pessoais manipulados pelo poder público e por terceiros. 6. É compatível com a Constituição de 1988 o compartilhamento direto de dados cadastrais genéricos com os órgãos de persecução penal, para fins de investigação criminal, mesmo sem autorização da Justiça. 7. Ação direta de inconstitucionalidade de que se conhece em parte, e, nessa extensão, pedido julgado improcedente (ADI 4.906, Rel. Min. Nunes Marques, Tribunal Pleno, DJe 24/10/2024).

É verdade que o endereço de IP, em si, não revela as informações de navegação daquele indivíduo na rede. No entanto, ainda assim não pode ser compartilhado diretamente aos órgãos de persecução penal,

individualmente ou associado às demais informações que integram os dados de tráfego. **Isso em razão da expressa previsão da lei (art. 5º, VI, do Marco Civil da Internet), que o vincula o endereço de IP aos registros de conexão e o submete à reserva de jurisdição (art. 10, § 1º, da referida lei).**

Com efeito, a possibilidade de requisição direta de dados cadastrais **não abrange metadados referentes a registros de conexão e de acesso a aplicações de internet**, nem mesmo na hipótese de compartilhamento de dados cadastrais vinculados a eles.

Isso porque, para fornecer os dados cadastrais nesses casos, o **provedor deve proceder à identificação do usuário** – isto é, deve realizar a vinculação entre os dados de tráfego e os dados de cadastro da pessoa possivelmente vinculada ao IP. Assim, **não é possível obter os dados cadastrais sem, antes, acessar os dados de tráfego dos usuários** – tanto é que, ao requisitar as informações, as autoridades fornecem não apenas o endereço de IP, mas também as informações relativas a data, hora e fuso horário do acesso.

O art. 10, § 1º, do Marco Civil da Internet é explícito ao dispor que “o provedor responsável pela guarda somente será obrigado a disponibilizar **os registros mencionados no caput, 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**”. Ou seja, o exame e compartilhamento de informações que envolvam dados de tráfego – estejam ou não associados a elementos que permitam identificar o usuário – está condicionada à prévia autorização judicial.

Nesses casos de requisição de “dados cadastrais de IP”, o risco de intervenção indevida no direito à autodeterminação informacional é ainda maior quando se trata de IP dinâmico ou de conexões operadas por NAT (*Network Address Translation*) – especialmente quando diferentes usuários

ADC 91 / DF

compartilham um mesmo IP público –, situação em que a identificação pretendida pode resultar na divulgação de dados relativos a várias pessoas.

Com efeito, a requisição de “dados cadastrais de IP” nada mais é do que uma forma de tentar se sobrepor à necessidade de ordem judicial para acessar dados de tráfego e ao regime delineado pelo Marco Civil da Internet, devendo-se elucidar que a requisição direta de dados cadastrais básicos pressupõe a identificação prévia do usuário.

Não desconheço que a legislação de diferentes países consagra disciplina diversa sobre a requisição de dados cadastrais.

Na Alemanha, por exemplo, a requisição de dados cadastrais está disciplinada no Código de Processo Penal (§ 100j, StPO), distinguindo situações que exigem ou não autorização judicial. Apesar de considerar o que o endereço de IP, isoladamente, constitui dado cadastral, o Tribunal Federal Constitucional alemão decidiu que isso abrange apenas o endereço de IP estático, mas não o IP dinâmico, porquanto a determinação do usuário nesses casos exige que os provedores acessem e examinem dados de tráfego, que estão protegidos pelo sigilo (BVerfGE 130, 151; HENRICH, Simon; WEINGAST, Karin. § 100j. In: *Karlsruher Kommentar zur Strafprozessordnung*. 9. ed. Munique: C.H. Beck, 2023. nm. 2).

Além disso, o recente Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho, de 12 de julho de 2023 – que será aplicável a partir de agosto de 2026 e tem força de lei nos Estados-Membros da União Europeia –, introduziu uma nova categoria, distinta das noções tradicionais de dados de assinantes, dados de tráfego e dados de conteúdo, que são os “dados solicitados com o único objetivo de identificar o utilizador”. Isso justamente para facilitar as investigações nos casos em que a vinculação de dados de tráfego a dados de assinantes for necessária para

a identificação do usuário, como as que aqui se debate:

Art. 3 [...]

9) «Dados de assinantes», dados na posse de um prestador de serviços relacionados com a adesão aos seus serviços, relativos: a) À identidade de um assinante ou cliente, tais como o nome fornecido, a data de nascimento, o endereço postal ou geográfico, os dados de faturação e pagamento, o número de telefone ou o endereço de correio eletrónico; b) Ao tipo de serviço e respetiva duração, incluindo dados técnicos e dados que identifiquem medidas técnicas associadas ou interfaces fornecidas ao assinante ou cliente ou por ele utilizadas no momento do registo inicial ou da ativação, e dados relacionados com a validação da utilização do serviço, com exceção de palavras-passe ou outros meios de identificação utilizados em vez de uma palavra-passe que sejam fornecidos por um utilizador, ou criados a pedido do mesmo;

10) «Dados solicitados com o único objetivo de identificar o utilizador», os endereços IP e, se necessário, as portas de origem e o carimbo temporal pertinentes, nomeadamente a data e a hora, ou os equivalentes técnicos desses identificadores e informações conexas, quando solicitados pelas autoridades responsáveis pela aplicação da lei ou pelas autoridades judiciais com o único objetivo de identificar o utilizador numa investigação criminal específica;

11) «Dados de tráfego», dados relacionados com a prestação de um serviço por um prestador de serviços que servem para fornecer contexto ou informações adicionais sobre esse serviço e que são gerados ou tratados por um sistema de informação do prestador de serviços, tais como o remetente e o destinatário de uma mensagem ou de outro tipo de interação, sobre a localização do dispositivo, a data, a hora, a duração, o tamanho, a via, o formato, o protocolo utilizado e o tipo de

compressão, e outros metadados das comunicações eletrônicas e dados, com exceção dos dados de assinantes, relacionados com o início e o fim da sessão de acesso de um utilizador a um serviço, tais como a data e a hora da utilização, o início («log-in») e o fim («log-off») da ligação ao serviço;

12) «Dados de conteúdo», dados num formato digital, como texto, voz, vídeos, imagens e som, que não sejam dados de assinantes ou de tráfego;

Desse panorama, extraio duas conclusões.

Primeiro, a possibilidade restrita de compartilhamento de dados cadastrais vinculados a dados de tráfego, com o objetivo exclusivo de identificar um usuário em investigações criminais, parece ser uma alternativa proporcional para equilibrar o interesse estatal na persecução penal e a necessária proteção de dados pessoais, em situações específicas.

Segundo, para que tal solução seja juridicamente viável no Brasil, é indispensável uma alteração do modelo instituído pelo Marco Civil da Internet, para que seja respeitada a reserva de lei. **Não por acaso, nos exemplos estrangeiros mencionados, tais medidas somente se tornam legítimas após a edição de bases legais correspondentes.**

Reitero que, na minha compreensão, o Marco Civil da Internet é, quanto ao ponto aqui debatido, compatível com as obrigações assumidas pelo Estado brasileiro ao aderir à Convenção de Budapeste.

O art. 18 da Convenção assim dispõe:

Artigo 18 - Ordem de exibição

1. Cada Parte adotará as medidas legislativas e outras

providências necessárias para dar poderes a autoridades competentes para ordenar: [...]

b. a qualquer provedor de serviço que atue no território da Parte a entregar informações cadastrais de assinantes de tais serviços, que estejam sob a detenção ou controle do provedor.

[...] 3. Paras os fins deste Artigo, o termo “informações cadastrais do assinante” indica qualquer informação mantida em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a assinantes de seus serviços, com exceção dos dados de tráfego e do conteúdo da comunicação, e por meio da qual se possa determinar:

a. o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas para esse fim e a época do serviço;

b. a identidade do assinante, o domicílio ou o endereço postal, o telefone e outros números de contato e informações sobre pagamento e cobrança, que estejam disponíveis de acordo com o contrato de prestação de serviço.

c. quaisquer outras informações sobre o local da instalação do equipamento de comunicação disponível com base no contrato de prestação de serviço.

De qualquer forma, ainda que essa Convenção adote uma compreensão um pouco mais ampla de dados cadastrais – e que não inclua dados de tráfego –, a modificação do conceito instituído expressamente pelo Marco Civil da Internet, com repercussões sobre a disciplina jurídica interna, requer prévia alteração legislativa.

A Convenção de Budapeste não confere, de modo imediato, ao Estado poderes investigativos adicionais, nem autoriza diretamente intervenções em direitos fundamentais. É a própria Convenção, na verdade, que imputa aos Estados o dever de legislar sobre a matéria.

Como observa Lagodny, tratados de cooperação penal internacional são destinados a reger obrigações entre Estados, e o indivíduo não é seu destinatário direto (LAGODNY, Otto. *The Individual as Subject of International Cooperation in Criminal Matters: A Comparative Study*. Freiburg: Max-Planck-Institut für ausländisches und internationales Strafrecht, 2002, p. 3 e 6).

Da mesma forma, cada compromisso internacional há de ser implementado em leis nacionais, o que confirma que a Convenção não tem eficácia normativa imediata nem pode dispensar a necessidade de lei proporcional para restringir direitos fundamentais.

Não por outra razão, o art. 18 da Convenção não dispõe que as autoridades competentes poderão ordenar diretamente a exibição dos dados ali referidos. O que o dispositivo prevê é que os Estados-partes deverão adotar as medidas legislativas necessárias para conferir tal poder às autoridades nacionais.

Portanto, a norma internacional invocada não é completa nem suficiente o bastante para aplicação imediata — vale dizer, o art. 18 da Convenção de Budapeste manifestamente não resolve o problema em exame, porque manda o Estado *legislar*.

De todo o exposto, impõe-se a interpretação conforme à Constituição do art. 10, § 1º, do Marco Civil da Internet, a fim de elucidar que a identificação do usuário pelo provedor, por meio do compartilhamento da informação que permite o vínculo entre os dados cadastrais e os registros de conexão ou de acesso a aplicações de internet, está submetida à reserva de jurisdição.

VI. As exceções da legítima defesa e do estado de necessidade

Antes de concluir, faz-se necessário ressaltar que, em situações de extrema urgência, entendo ser possível autorizar a superação da exigência de ordem judicial para obtenção de dados cadastrais vinculados a dados de tráfego, **sem afastar a premissa, acima explicitada, da exigência de lei para justificar a intervenção.**

Com efeito, deve-se admitir, em caráter absolutamente excepcional e com fundamento nas causas de justificação penais (arts. 24 e 25 do Código Penal), a requisição direta nas situações em que o acesso imediato aos dados for comprovadamente imprescindível, por exemplo, para localizar uma pessoa sequestrada, evitar um ataque terrorista iminente ou impedir a consumação de um crime cibernético que está acontecendo naquele momento.

A possibilidade de recorrer a esta figura vincula-se, especificamente, à proteção de bens jurídicos de alto valor – como a vida e a liberdade de locomoção – diante de perigo atual e involuntário, preenchidos os demais pressupostos de justificação, além de depender de posterior controle judicial.

Para delinear melhor essa possibilidade, entendo serem necessárias algumas explicações.

É comum que direitos fundamentais sejam protegidos por meio do Direito Penal, apesar de isso não ser uma regra, em razão do princípio da *ultima ratio*. Assim, a prática de medidas investigativas, que caracterizam intervenções em direitos fundamentais, pode se subsumir a diferentes tipos penais, como invasão de dispositivo informático (art. 154-A, CP), violação de correspondência ou de comunicação (art. 151, CP), interceptação telefônica ilegal (art. 10 da Lei n. 9.296/1996), violação de sigilo funcional (art. 325, CP), divulgação de informações sigilosas (art. 153,

CP), além dos crimes de abuso de autoridade previstos na Lei n. 13.869/2019.

Desse modo, a realização de intervenções investigativas segundo os parâmetros legais pode afastar a própria tipicidade desses delitos, a depender da estrutura típica, ou ser justificadas pelo **estrito cumprimento de dever legal** ou **exercício regular de direito** (art. 23, III, CP), preenchidos os critérios de legitimidade da medida previstos em lei. Aplica-se, aqui, a mesma lógica da intervenção em direitos fundamentais, acima exposta, que exige lei formal para a justificação.

As normas permissivas, que afastam a ilicitude de uma conduta, não se restringem ao campo penal, podendo estar previstas em qualquer ramo do ordenamento jurídico, seja no Direito Processual Penal, no Direito Civil, no Direito Administrativo ou em outras esferas normativas (HUNGRIA, Nelson. *Comentários ao Código Penal*. vol. 1, Tomo II. 4. ed. Rio de Janeiro: Forense, 1958, p. 310). Isso decorre do **princípio da unidade do ordenamento jurídico**: seria logicamente contraditório que a ordem jurídica, considerada em seu conjunto, simultaneamente proibisse e autorizasse a mesma conduta.

Sob a perspectiva penal, há, ademais, **outras causas de exclusão da antijuridicidade** que podem ser relevantes, como o **estado de necessidade** (art. 24, CP) e a **legítima defesa** (art. 25, CP).

É só pensar, por exemplo, na filmagem não consentida de alguém que está a praticar um crime contra outra pessoa em um local privado. Apesar de poder caracterizar captação ambiental óptica sem ordem judicial (art. 10-A da Lei n. 9.296/96), o injusto pode ser afastado pela legítima defesa (art. 25, CP), própria ou de terceiros, desde que a gravação constitua meio para repelir a injusta agressão, ou pelo estado de necessidade (art. 24, CP). E isso faz com que a gravação, inicialmente oriunda de fato típico, seja

lícita, não apenas no direito penal, mas também no processo penal, pelo mesmo fundamento da unidade do ordenamento jurídico.

O Supremo Tribunal Federal já assentou esse entendimento ao reconhecer que, afastada a ilicitude da conduta pela legítima defesa, a gravação não pode ser tida como prova ilícita para os fins do art. 5º, LVI, da Constituição Federal (HC 74.678, Rel. Min. Moreira Alves, Primeira Turma, DJ 15/8/1997).

Isso ocorre, por exemplo, nos casos em que o próprio réu realiza uma gravação *prima facie* ilícita para provar sua inocência, agindo em legítima defesa ou estado de necessidade (a respeito, LOPES JR., Aury. *Direito Processual Penal*. São Paulo: Saraiva, 2022, p. 461). A licitude dessa prova se depreende da própria Lei n. 9.296/1996 (art. 8º-A, § 4º, “A captação ambiental feita por um dos interlocutores sem o prévio conhecimento da autoridade policial ou do Ministério Público poderá ser utilizada, em matéria de defesa, quando demonstrada a integridade da gravação”). Contudo, como eu já ressaltai em meu voto no ARE 1493134 AgR (Rel. Min. Luiz Fux, Primeira Turma, DJe 20/10/2025), esse dispositivo “não exclui outras possibilidades de justificação mais genéricas, como a legítima defesa probatória em casos de crimes registrados pela vítima”. Isso confirma que as causas gerais de exclusão da ilicitude continuam operando como válvulas residuais do sistema.

Tome-se, como hipótese ilustrativa, a situação em que a autoridade policial, no curso de investigação em andamento, obtém informação confiável de que um agente está, naquele exato momento, praticando um crime pela internet – como um ataque de *ransomware* contra a infraestrutura de um hospital (modalidade de ataque cibernético que cifra os dados e sistemas da vítima, tornando-os inacessíveis até o pagamento de resgate) ou a exploração sexual de criança por meio de plataforma digital – e que a identificação imediata do autor, por meio do acesso a

dados cadastrais vinculados a dados de tráfego, é a única medida capaz de interromper a conduta e evitar a consumação ou o agravamento do dano.

Não há, como já exposto acima, lei que autorize a requisição direta, de modo que a autoridade policial não poderá recorrer ao exercício regular de direito ou estrito cumprimento de dever legal. Isso porque essas duas figuras constituem, na expressão da doutrina, "causas de justificação em branco": são apenas enunciadas no art. 23, III, do Código Penal, mas seus fundamentos e limites dependem da especificação de outra norma permissiva que autorize o exercício do direito ou determine o cumprimento do dever (GRECO, Luís; HORTA, Frederico; LEITE, Alaor; TEIXEIRA, Adriano; QUANDT, Gustavo. *Reforma da parte geral do Código Penal: uma proposta alternativa para debate*. São Paulo: Marcial Pons, 2018, p. 30). Ausente essa norma permissiva específica – e inexistente, no ordenamento brasileiro, lei que discipline o acesso direto a dados cadastrais vinculados a dados de tráfego em situações de urgência –, essas justificantes não podem ser invocadas.

Após o início deste julgamento, a Lei n. 15.487/2026 alterou o Estatuto da Criança e do Adolescente e incluiu previsão específica de requisição direta de registros de conexão:

Art. 190-F. É lícita a ronda virtual realizada por órgão de persecução penal mediante utilização de software estritamente destinado à identificação e à coleta de arquivos disponibilizados em ambientes digitais públicos e relacionados a crimes de violência sexual contra criança ou adolescente.

(...)

§ 2º Nos casos de flagrante, de risco à vida ou de risco à integridade física de criança ou adolescente identificados durante a ronda virtual, a autoridade policial ou o Ministério Público poderão requisitar diretamente ao provedor de conexão

ou ao provedor de aplicação, respectivamente, os registros de conexão ou os dados cadastrais de que disponham, sem necessidade de ordem judicial prévia, nos termos da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

Trata-se de dispositivo que **soluciona apenas parcialmente** o problema aqui colocado, pois fundamenta o exercício regular de direito nas hipóteses específicas de flagrante e de risco à vida ou à integridade física de crianças e adolescentes, identificadas a partir da ronda virtual. Em relação aos demais crimes, contudo, os casos de urgência permanecem sem previsão legal específica.

Resta, portanto, a análise da legítima defesa e do estado de necessidade.

A **legítima defesa** (art. 25, CP) exige, quanto à situação justificante, uma **agressão injusta, atual ou iminente**, a direito próprio ou alheio (SANTOS, Juarez Cirino dos. *Direito Penal: parte geral*. Curitiba: ICPD, 2014, p. 226-229). Nos exemplos hipotéticos, o crime em andamento constitui conduta humana dolosa e objetivamente antijurídica, de modo que esse requisito está preenchido.

Quanto à ação justificada, a requisição dos dados é o meio pelo qual se identifica e, conseqüentemente, se interrompe a agressão em curso em favor de terceiros – as vítimas do ataque de *ransomware* ou da exploração sexual. A depender das circunstâncias do caso concreto, portanto, é possível afirmar a legítima defesa de terceiro. A circunstância de que a reação não se dirige diretamente contra o agressor, mas em relação ao provedor que detém os dados necessários à sua identificação, não afasta essa qualificação, pois o que importa é que a medida é o meio pelo qual a agressão injusta em curso é interrompida, e não que ela recaia fisicamente sobre o próprio agressor, até porque os dados que serão acessados são de sua titularidade. A requisição direta de dados nessas circunstâncias

caracteriza uso moderado dos meios necessários.

Não se exclui, ademais, a aplicação alternativa do estado de necessidade justificante (art. 24, CP), caso não preenchidos os pressupostos da legítima defesa no caso concreto. A diferença entre as duas justificantes, neste contexto, é de enquadramento dogmático, pois, em ambos os casos, a requisição direta dos dados pela autoridade policial, sem prévia autorização judicial, estaria justificada.

O estado de necessidade está previsto no art. 24 do CP, que assim dispõe: “considera-se em estado de necessidade quem pratica o fato para salvar de perigo atual, que não provocou por sua vontade, nem podia de outro modo evitar, direito próprio ou alheio, cujo sacrifício, nas circunstâncias, não era razoável exigir-se.”

Quanto à situação justificante, a lei exige, em juízo objetivo *ex ante*, **perigo atual e involuntário** a direito próprio ou alheio (SANTOS, *Direito Penal*, p. 238-240). No caso em exame, o perigo é **atual**, pois o crime está se consumando no momento da decisão da autoridade policial, não se tratando de risco futuro ou já exaurido; é **involuntário**, porquanto não foi criado nem potencializado pela própria autoridade; e recai sobre **bem jurídico alheio**, o patrimônio, a autodeterminação informacional e a proteção de dados sensíveis dos pacientes do hospital ou, conforme o caso, a liberdade sexual das vítimas.

Já a ação justificada pressupõe, em primeiro lugar, a **necessidade** (isto é, que a lesão ao bem jurídico alheio seja inevitável por outro meio), o que implica verificar se a conduta era idônea a afastar o perigo e representava o meio menos gravoso disponível. No caso concreto, a requisição direta dos dados preenche ambos os critérios: é idônea, pois a identificação imediata do autor é a única medida capaz de interromper o ataque em curso; e é o meio menos gravoso, pois o tempo exigido para a obtenção de

autorização judicial, ainda que via plantão, pode ser objetivamente incompatível com a janela disponível para evitar a consumação ou o agravamento do dano, inexistindo, nas circunstâncias, alternativa igualmente eficaz e menos invasiva.

E, em segundo lugar, a **razoabilidade**, que, a despeito da controvérsia doutrinária a respeito da amplitude da justificante (SANTOS, *Direito Penal: parte geral*, p. 242-247), compreendo assentada em uma ponderação de interesses, que não se reduz à comparação abstrata entre os bens nominalmente envolvidos, mas deve contemplar também a extensão dos danos decorrentes do perigo originário e da ação salvadora, a intensidade do perigo, a reparabilidade do dano e a idoneidade *ex ante* da medida para afastá-lo (QUANDT, Gustavo de Oliveira. O estado de necessidade no Código Penal brasileiro: uma proposta de modelo diferenciador. *Revista do Instituto de Ciências Penais*, v. 6, n. 2, 2021, p. 459-460).

Presentes, portanto, os pressupostos do estado de necessidade justificante, a requisição direta dos dados pela autoridade policial, sem prévia autorização judicial, não configura, na minha compreensão, ilícito penal nem processual penal, ressalvada a necessidade de submissão da medida a controle judicial *a posteriori*, ocasião em que se verificará, com base na documentação contemporânea aos fatos, se os elementos fáticos invocados eram reais, objetivos e suficientes para caracterizar a justificante.

Para fins comparativos, ressalto que a possibilidade de recorrer à justificação penal nesses casos, com consequências para a admissibilidade das provas no processo, é amplamente debatida na Alemanha.

Apesar de limitar seu objeto de análise a casos de busca privada por meios de prova, Samuel Strauß, ao tratar sobre a “necessidade probatória”, explora a possibilidade de justificar, por meio do estado de necessidade, a prática de fatos típicos – sobretudo de gravações não autorizadas – para

fins probatórios. Elucida, contudo, que o mero interesse em uma conservação preventiva de provas, sem motivo concreto, não pode ser justificada pelo estado de necessidade (STRAUSS, Samuel. *Rechtfertigung und Beweisverbot*. Duncker & Humblot: Berlin, 2023, p. 238). Como exemplo dessa possibilidade, Neumann menciona a justificação da violação de segredos privados pelo estado de necessidade, quando, de outro modo, o acusado não puder exercer adequadamente sua defesa (NEUMANN, NK-StGB, 6. ed. 2023, StGB § 34 Rn. 22-31g.).

Há, no entanto, alguns pontos que devem ser sublinhados.

Inicialmente, deve-se registrar que há relevante controvérsia, na doutrina alemã, a respeito da possibilidade de agentes públicos recorrerem às causas justificação da legítima defesa ou do estado de necessidade.

Como ensinam Claus Roxin e Luís Greco, ao comentar sobre o estado de necessidade previsto no § 34 StGB alemão, "se autoridades estatais podem recorrer a um estado de necessidade justificante (...) é uma questão tão controversa quanto se suas atuações podem ser justificadas pela legítima defesa", concluindo, porém, que isso deve ser admitido em princípio, desde que limitado a "casos raros e extremos" e sujeito a "rígido controle judicial" – pois "a possibilidade de justificação pelo § 34 StGB nunca pode entrar em consideração em situações normais" (ROXIN, Claus; GRECO, Luís. *Direito Penal: parte geral*. São Paulo: Marcial Pons, p. 1050).

Os autores complementam:

(...) uma justificação de atos estatais por meio do preceito do § 34 StGB entra em consideração apenas em hipóteses excepcionais, pois em casos como a prisão, a busca, a apreensão, as interceptações telefônicas e muitos outros, o conflito entre o interesse público na intervenção e o interesse privado na

proteção é regulado por disposições especiais, de modo que essa ponderação realizada pelo legislador não pode ser eludida por meio da realização de uma ponderação judicial distinta, com auxílio do § 34 StGB. Assim, **a aplicação do § 34 StGB somente pode ser considerada: quando um conflito de interesses, em razão de sua excepcionalidade, não foi previsto pelo legislador (o que, em razão da diversidade dos acontecimentos da vida, sempre acaba por ocorrer); quando um certo caso de estado de necessidade está fora do âmbito de aplicação de uma regra geral prevista em lei (como, p.ex., a hipótese de exigência de libertação de presos por meio da captura de reféns); ou quando o legislador, em razão da novidade e da falta de clareza de um problema, ainda quer aguardar um pouco antes de legislar a respeito de uma concretização do § 34 StGB.** Por isso, gravações secretas de som por parte da polícia só podem ser justificadas pelas regras dos §§ 100a ss. StPO (vigilância de telecomunicação, vigilância domiciliar, uso de aparelhos técnicos etc.), mas normalmente não pelo § 34 StGB. “No âmbito de regulamentação dos §§ 100a ss. StPO, só caberá uma legítima defesa ou um estado de necessidade justificante para os órgãos de persecução penal, no melhor dos casos, em hipóteses muito extraordinárias” (BGHSt 31, 304 [307]). “Caso contrário, seriam afastados os bem ponderados regramentos legais acerca das faculdades de intervenção processuais-penais” (BGHSt 34, 39 [51 s.]) (ROXIN; GRECO. *Direito Penal*: parte geral, p. 1050-1051).

Esse entendimento encontra respaldo no próprio desenvolvimento histórico da jurisprudência do BGH. Em BGHSt 27, 260, decisão proferida no contexto de um sequestro realizado por uma organização terrorista, o Tribunal Federal de Justiça alemão (equivalente ao nosso STJ) admitiu, em caráter absolutamente excepcional, que a violação do § 148 Abs. 1 StPO, que assegura ao preso o contato com seu defensor, poderia ser justificada pelo estado de necessidade (§ 34 StGB), tendo em vista que os acusados, se

mantido o contato com seus defensores, poderiam elevar o perigo à vida do sequestrado (p. 262-263).

O BGH sublinhou, contudo, dois balizamentos essenciais: a medida não poderia privar o acusado de toda assistência jurídica, devendo ser-lhe designado novo defensor impedido de tratar do caso em questão; e a restrição estaria sujeita a revisão judicial, cessando tão logo deixasse de ser indispensável. A decisão ilustra, assim, que o recurso ao estado de necessidade justificante para atuação de agentes públicos não dispensa o controle judicial posterior e pressupõe proporcionalidade estrita.

No Brasil, por sua vez, não há qualquer dificuldade em aplicar as causas de justificação para ações de agentes públicos, tendo em vista que não temos uma legislação própria que discipline especificamente sobre o direito de polícia, ao contrário da Alemanha. É, comum, portanto, que agentes de segurança pública, em situações extremas, atuem em legítima defesa de terceiros, e em regra não há quem sustente que o resgate da vítima nesse contexto seja ilícito, com consequências inclusive probatórias.

De qualquer forma, as ressalvas de Roxin e Greco são úteis também no contexto brasileiro. Os autores indicam que a aplicação do estado de necessidade justificante para atuação de agentes públicos somente pode ser considerada em três hipóteses: (i) quando o conflito de interesses, em razão de sua excepcionalidade, não foi previsto pelo legislador; (ii) quando o caso concreto está fora do âmbito de aplicação de uma regra geral prevista em lei; (iii) ou quando o legislador, diante da novidade e da falta de clareza de um problema, ainda não legislou sobre sua concretização.

Todas essas premissas convergem para o caso ora em análise.

O acesso a dados cadastrais vinculados a dados de tráfego por requisição direta da autoridade policial, em situações de urgência extrema,

é precisamente o tipo de conflito de interesses que o legislador brasileiro não antecipou. O acesso direto a determinadas informações em situações de urgência foi inserido em nossa legislação apenas em 2016, com a inserção dos arts. 13-A e 13-B no Código de Processo Penal. Esses dispositivos, inclusive, foram considerados constitucionais pelo Supremo Tribunal Federal (ADI 5.642, Rel. Min. Edson Fachin, Tribunal Pleno, DJe 22/8/2024).

Embora o STF tenha assinalado, na ADI 5.642, que o Poder Judiciário deve manter estrutura de plantão permanente para autorizar medidas mais restritivas, isso não afasta a possibilidade de justificação nos casos em que o intervalo de tempo para obtenção da ordem – ainda que via plantão – seja objetivamente incompatível com a janela disponível para evitar o dano irreversível. A existência abstrata do plantão não equivale à disponibilidade concreta e tempestiva de autorização em toda e qualquer situação de urgência extrema.

A isso se acrescenta uma última distinção estrutural relevante. O Direito Penal liberal erige garantias processuais em favor do suspeito/imputado precisamente porque ele é o sujeito vulnerável perante o poder punitivo estatal, aquele a quem o ordenamento deve assegurar a proteção contra a instrumentalização.

Essa posição jurídica não se confunde com a daquele que, no momento da intervenção, é a própria fonte do perigo: o agente cuja conduta ilícita em curso ameaça direitos de terceiros e que, a qualquer momento, pode fazer cessar essa ameaça simplesmente interrompendo sua ação. No direito alemão, essa distinção se expressa na diferença entre o **suspeito**, sobre o qual recai o processo penal repressivo, e o **perturbador** (*Störer*), afetado pelo direito de polícia ou de proteção contra perigos, assim definido como “aquele a cujo comportamento ou a cuja esfera o perigo pode ser reconduzido” (GRECO, Luís. Considerações introdutórias sobre

o processo penal alemão, p. 52).

Como observa Luís Greco, a fraqueza e a vulnerabilidade que justificam a proteção reforçada do suspeito no processo penal simplesmente não se encontram naquele que expande unilateralmente sua esfera de liberdade à custa de terceiros, pois a ele está sempre aberta a alternativa de cessar a conduta e retornar aos limites do seu direito (GRECO, Luís. Kernbereichsschutz als Ausbeutungsschutz. In: KUSCHE, Carsten; STEFANOPOULOU, Georgia (Hrsg.). *Digitalisierung als total social fact der Kriminalwissenschaften*. Baden-Baden: Nomos, 2024, p. 170). Nos casos hipotéticos examinados, o agente que pratica o *ransomware* ou a exploração sexual de criança não é o suspeito que o processo penal protege. A requisição de seus dados cadastrais, nesses casos, dirige-se a quem, por sua própria conduta, é a fonte do perigo que a justificante visa neutralizar.

VII. Modulação de efeitos

Considerando a necessidade de conciliar a tese ora proposta com a preservação da segurança jurídica, entendo que a modulação de efeitos é necessária no presente caso.

Propus, inicialmente, que a interpretação aqui firmada produzisse efeitos apenas prospectivos, resguardando-se a licitude das investigações realizadas com base em interpretação diversa e ressalvados os pedidos formulados pelas defesas até a data de publicação da ata deste julgamento. Sugeri a seguinte redação de tese: “atribuem-se efeitos prospectivos à presente decisão, ressalvados os pedidos formulados até a data de publicação da ata do presente julgamento”.

Em seu voto-vista, contudo, o eminente Ministro Dias Toffoli propôs que se atribuisse efeitos *ex nunc*, considerando que se trata de ação declaratória de constitucionalidade, sugerindo a seguinte redação: “Para

privilegiar a segurança jurídica, conferem-se efeitos *ex nunc* à interpretação conforme conferida ao art. 10, § 1º, da Lei nº 12.965/14 (Marco Civil da Internet), ficando ressalvadas dessa modulação apenas as investigações ou ações penais em curso nas quais a defesa tenha levantado a controvérsia até a conclusão deste julgamento”.

Acolho a proposta do eminente Ministro Dias Toffoli, para substituir os efeitos prospectivos por efeitos *ex nunc*.

Importa precisar, contudo, o alcance concreto dessa modulação. Os efeitos *ex nunc* significam que a interpretação conforme ora estabelecida, vincula apenas as investigações e ações penais iniciadas ou em curso nas quais a defesa tenha suscitado a controvérsia até a conclusão deste julgamento. Em consequência, preserva-se a higidez das provas obtidas mediante requisição direta nas investigações e processos em que tal ilicitude não foi alegada, não sendo cabível sua arguição em momento posterior com fundamento nesta decisão.

VIII. Dispositivo

Posto isso, julgo procedente o pedido para declarar a constitucionalidade do art. 10, § 1º, da Lei n. 12.965/2014 (Marco Civil da Internet) e atribuir-lhe interpretação conforme à Constituição a fim de elucidar que a identificação do usuário pelo provedor, por meio do compartilhamento da informação que permite o vínculo entre os dados cadastrais e os registros de conexão ou de acesso a aplicações de internet, depende de autorização judicial.

Proponho a seguinte tese de julgamento:

1. É constitucional o art. 10, § 1º, da Lei n. 12.965/2014 (Marco Civil da Internet), que condiciona o compartilhamento,

por provedores, de dados de tráfego – de forma autônoma ou associados a outros dados pessoais – à obtenção de prévia autorização judicial. Consequentemente, a identificação do usuário mediante a correlação, pelo provedor, entre os dados cadastrais e os registros de conexão ou de acesso a aplicações de internet, exige autorização judicial específica.

2. Em situações excepcionais, caracterizadas pelo perigo iminente para bens jurídicos de alto valor e que configurem estado de necessidade, é permitido que a autoridade policial ou o Ministério Público requisitem diretamente o compartilhamento de dados cadastrais associados a dados de tráfego para a identificação imediata do usuário. Nesses casos, o ato deverá ser documentado e submetido a posterior apreciação judicial.

3. Atribuem-se efeitos prospectivos à presente decisão, ressalvados os pedidos formulados até a data de publicação da ata do presente julgamento.

É como voto.