

**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-VISTA

O SENHOR MINISTRO DIAS TOFFOLI:

Trata-se de ação declaratória de constitucionalidade ajuizada pela **Associação Brasileira de Provedores de Internet e Telecomunicações (ABRINT)**, com pedido de medida liminar, mediante a qual se postula a declaração da constitucionalidade do art. 10, § 1º, da Lei nº 12.965/14, apelidada de Marco Civil da Internet.

Alega a requerente, em apertada síntese, que haveria controvérsia judicial relevante acerca da interpretação do referido art. 10, **notadamente quanto à necessidade de ordem judicial prévia e específica nas hipóteses em que são solicitados registros de conexão, associados ou não a dados cadastrais, com o objetivo de identificar usuário da rede ou terminal.** A seu ver, esses dados (também denominados “dados

cadastrais de IP”) se enquadram na categoria jurídica de dados pessoais, razão pela qual sua disponibilização dependeria de autorização judicial, sob pena de violação dos direitos fundamentais à privacidade, à intimidade e à proteção de dados.

No mais, acolho o relatório lançado aos autos.

O julgamento do feito foi iniciado em sessão virtual do Plenário realizada de **12 a 19 de dezembro de 2025**, ocasião em que o Relator, Ministro **Cristiano Zanin**, conheceu da ação e julgou procedente o pedido para declarar a constitucionalidade do dispositivo questionado e a ele atribuir interpretação conforme à Constituição de 1988, 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”.

Para Sua Excelência, os dados cadastrais são aqueles que se referem a “informações básicas de identificação, como qualificação pessoal, filiação e endereço de uma pessoa determinada”. Esses dados – **e apenas eles** – podem ser “requisitados diretamente pela autoridade policial e pelo Ministério Público (ou, a depender do caso, por outra autoridade competente)”, com fundamento no art. 10, § 3º, da Lei nº 12.965/14.

A esse respeito, o Relator explica o seguinte:

“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 nº 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” (grifo nosso).

Registra, ainda, o Relator que **o acesso a dados de tráfego** – ou seja, a registros de conexão ou de acesso a aplicações de internet –, **diversamente, depende de ordem judicial específica e fundamentada**, nos termos do art. 22 da Lei nº 12.965/14, o que também seria proporcional. Isso porque, a seu ver,

“o acesso a metadados permite traçar perfis comportamentais, 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 conseguinte, segundo esclarece o Relator,

“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 informações relativas a data, hora e fuso horário do acesso**” (grifos no original).

Até aqui, verifico que o voto do Relator, Ministro **Cristiano Zanin**, está em perfeita harmonia com a jurisprudência da Corte, que tem entendido pela possibilidade de compartilhamento direto de dados cadastrais com autoridades policiais e Ministério Público, para fins de investigação penal ou instrução processual penal, mas não o admite quando se trata de dados pessoais diversos, cujo fornecimento pelos provedores de internet continua a depender de ordem judicial.

Cito como exemplo a **ADI nº 4.906**, Rel. Min. **Nunes Marques**, na qual se questionava o **art. 17-B da Lei nº 9.613/98**¹. No julgamento da ADI, o Plenário do Supremo Tribunal Federal fixou a seguinte tese:

“É constitucional norma que permite o acesso, por autoridades policiais e pelo Ministério Público, a dados cadastrais e de pessoas investigadas independentemente de autorização judicial, **excluída do âmbito de incidência da norma a possibilidade de requisição de qualquer outro dado cadastral além daqueles referentes à qualificação pessoal, filiação e endereço** (art. 5º, X e LXXIX, da CF)” (ADI nº 4.906, Rel. Min. **Nunes Marques**, julgado em 11/9/24, DJe de 24/10/24).

Nesse sentido, colhe-se do voto condutor do acórdão o seguinte esclarecimento:

“[D]ados cadastrais são informações objetivas, fornecidas, não raro, pelo próprio usuário ou consumidor para registro de sua identificação nos bancos de dados de pessoas jurídicas públicas e privadas. Justamente por isso, dados como nome,

¹ Lei nº 9.613/98, **Art. 17-B**. “A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito”.

endereço e filiação não estão acobertados pelo sigilo.

A disposição dessas informações pelo indivíduo é, até mesmo hoje, imprescindível para o convívio em sociedade. Tanto é assim que informações objetivas são livremente divulgadas e, em princípio, não interferem ou prejudicam o livre desenvolvimento da personalidade, a despeito de hoje constituírem ativos valiosos a exigirem também tutela jurisdicional.

(...)

Cabe, no entanto, uma observação. O fato de a proteção a ensejar a imposição de sigilo não contemplar dados cadastrais (nome, filiação, endereço) não significa que informações objetivas capazes de identificar o sujeito sejam carecedoras de tutela jurisdicional como consectário do direito à privacidade. É dizer apenas que sua tutela não implica a imposição de sigilo e a necessidade de autorização judicial (CF, art. 5º, XII)” (ADI nº 4.906, Rel. Min. **Nunes Marques**, julgado em 11/9/24, DJe de 24/10/24).

Seguindo a mesma linha de raciocínio, ao julgar a **ADI nº 5.642**, Rel. Min. **Edson Fachin**, na qual se discutiam os **arts. 13-A e 13-B do CPP**²,

² CPP, **Art. 13-A**. “Nos crimes previstos nos arts. 148, 149 e 149-A, no § 3º do art. 158 e no art. 159 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), e no art. 239 da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos. **Parágrafo único**. A requisição, que será atendida no prazo de 24 (vinte e quatro) horas, conterá: **I** - o nome da autoridade requisitante; **II** - o número do inquérito policial; e **III** - a identificação da unidade de polícia judiciária responsável pela investigação.

CPP, **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

incluídos pela Lei nº 13.344, de 2016, prevaleceu no Plenário do Supremo Tribunal Federal o entendimento de que

“[a] expressão ‘dados cadastrais’ não abrange a interceptação de voz; a interceptação telemática; os dados cadastrais de usuários de IP, os quais abarcam dados de usuário que em determinado dia, data, hora e fuso fixaram 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” (grifo nosso).

Eu mesmo já tive oportunidade de me pronunciar sobre a questão, em **obiter dictum**, ao apreciar as **ADI nºs 5.059 e 5.073**, de **minha relatoria**, cujo julgamento ainda não foi finalizado, nas quais se discute a constitucionalidade do **poder genérico de requisição do delegado de polícia**, conforme o art. 2º, § 2º, da Lei nº 12.830/13³.

Em ambas as ocasiões, entendi que o delegado de polícia (ou o membro do Ministério Público) não pode ter acesso direto a **quaisquer dados**, sob pena de, eventualmente, se franquear às autoridades da persecução penal acesso a dados sigilosos ou, então, a dados pessoais que, mesmo não estando revestidos de sigilo, gozam de proteção jurídica para preservar a privacidade e a intimidade dos envolvidos.

Por essas razões, **acompanho o Relator quanto à**

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”.

³ Lei nº 12.830/13, **Art. 2º, § 2º**. “Durante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos”.

constitucionalidade do art. 10, § 1º, da Lei nº 12.965/14 e quanto aos termos de sua interpretação conforme. Adiro, outrossim, ao item 1 da tese de julgamento proposta, cujo teor transcrevo:

“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.”

No entanto, **tenho ressalvas relativamente aos demais itens da tese**, pelos motivos que passo a expor.

O **item 2 da tese de julgamento** proposta pelo Relator tem a seguinte redação:

“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.”

A esse respeito, o Relator esclarece o seguinte:

“[R]econheço que há situações de extrema urgência que podem autorizar a superação da exigência de ordem judicial para obter dados cadastrais vinculados a dados de tráfego, com fundamento no estado de necessidade. Isso seria possível, por

exemplo, nas situações em que o acesso imediato aos dados for comprovadamente imprescindível para localizar uma pessoa sequestrada, evitar um ataque terrorista iminente ou impedir a consumação de um crime cibernético que está acontecendo naquele momento.”

Com a devida vênia, penso que esse verbete de tese **estabelece exceção muito ampla e sem lastro em lei formal**, o que, **por si só, vulnera o direito fundamental à proteção de dados pessoais – e, com ele, os direitos à intimidade e à vida privada, à honra e à imagem das pessoas –, além de, na prática, dar margem ao exercício abusivo e arbitrário do poder estatal**.

Recordo, por oportuno, que o Supremo Tribunal Federal, ao apreciar o referendo das medidas cautelares concedidas nas Ações Diretas de Inconstitucionalidade nºs 6.387, 6.388, 6.389, 6.390 e 6.393, reconheceu expressamente os direitos fundamentais à autodeterminação informativa e à proteção de dados como direitos autônomos e desvinculados do direito à vida privada (e seus consectários), **e isso antes mesmo de entrar em vigor a Lei Geral de Proteção de Dados (LGDP), ou de ser promulgada a EC nº 115, de 2022, pela qual se inseriu o “direito à proteção dos dados pessoais, inclusive nos meios digitais” no catálogo do art. 5º do texto constitucional**.

Referidos precedentes representam, sem dúvida, um ponto de inflexão na jurisprudência da Corte e no direito brasileiro. Deles decorrem pelo menos **três efeitos práticos e igualmente relevantes** do ponto de vista jurídico-constitucional. O primeiro deles é que, a partir daí, **não se pode mais cogitar a existência de dados pessoais neutros ou de dados pessoais desprovidos de proteção constitucional**. Isso porque, como explica a Ministra Rosa Weber,

“[n]a medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação

de dados pessoais não de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, **caput**), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos” (ADI nºs 6.387-MC-Ref, 6.388-MC-Ref, 6.389-MC-Ref, 6.390-MC-Ref e 6.393-MC-Ref, Rel. Min. **Rosa Weber**, Tribunal Pleno, julgado em 7/5/20, DJe de 12/11/20).

O segundo efeito prático é justamente o de deixar claro que **qualquer intervenção no direito à proteção de dados e à autodeterminação informativa, para ser legítima, deve estar amparada por lei formal e proporcional**. Nada é mais natural, uma vez que a jurisprudência da Corte há muito recomenda que a restrição a direito fundamental seja feita por lei em sentido formal e que a medida restritiva atenda ao postulado da proporcionalidade.

O terceiro efeito prático foi o de **enunciar a importância da proteção de dados para a manutenção da democracia na atual sociedade da informação**. A propósito, transcrevo o seguinte excerto do voto condutor do acórdão:

“Situações de crise, como a deflagrada pela pandemia global da COVID-19 e marcada pelas medidas excepcionais que têm sido adotadas para o seu enfrentamento, tendem a favorecer o enfraquecimento de direitos, especialmente porque as instituições que em outro momento estariam menos permeáveis a tais investidas tornam-se, em momentos tais, menos vigilantes ou aderem às narrativas que visam a justificá-las a partir da crise posta. Tais movimentos têm sido objeto da literatura jurídica internacional, em que identificada, na pandemia de COVID-19 em curso, ‘uma oportunidade sem precedentes para os governos justificarem a expansão pós-pandêmica de políticas de vigilância e de coleta de dados tanto

de cidadãos quanto de não-cidadãos’” (ADI nºs 6.387-MC-Ref, 6.388-MC-Ref, 6.389-MC-Ref, 6.390-MC-Ref e 6.393-MC-Ref, Rel. Min. **Rosa Weber**, Tribunal Pleno, julgado em 7/5/20, DJe de 12/11/20).

Para **Laura Schertel**, aliás, uma das grandes virtudes da histórica decisão do STF pela qual se reconheceu a autodeterminação informativa é a de reconhecer também a existência de um direito fundamental e autônomo à proteção de dados pessoais. Diz a autora que,

“[e]m uma sociedade conectada, a **proteção de dados não é mais um direito entre tantos, mas um elemento essencial para a manutenção da confiança dos cidadãos nas estruturas de comunicação e informação, bem como para o necessário fluxo de dados e inovação dele decorrente**. Como regulação de uma ordem comunicacional e informacional, que é por definição multidimensional, a **proteção de dados tem como objetivo equilibrar os direitos de proteção, de defesa e de participação do indivíduo nos processos comunicativos**”⁴ (grifo nosso).

De fato, na atual sociedade da informação, **o direito fundamental à proteção de dados é uma garantia crucial, sem a qual outros direitos fundamentais tendem a perecer rapidamente**. Sua previsão formal no texto da Constituição de 1988, a partir da **EC nº 115, de 2022**, torna indiscutível que ele é um direito fundamental e autônomo — tal qual já decidido pelo próprio Supremo Tribunal Federal —, **com o que se reduz o ônus argumentativo do julgador**, que não precisa mais recorrer aos direitos fundamentais da intimidade e da vida privada (ou a seus

⁴ MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. JOTA, publicado em 10/5/20. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais>. Acesso em: 7/10/25.

consectários), ou à inviolabilidade da comunicação de dados (CRFB/88, art. 5º, incisos X e XII) para sua proteção.

Entretanto, há, ainda, outros efeitos dessa previsão formal, como o de criar para o estado um **dever negativo**, qual seja, o de **não interferir em seu âmbito de proteção, a não ser excepcionalmente, quando autorizado por lei formal e proporcional**; e, ao mesmo tempo, um **dever positivo** de se compelir o estado a adotar as providências cabíveis para assegurar sua observância nas relações particulares.

Desse modo, a meu ver, hoje, só se pode conceber restrição (legítima) ao direito à proteção de dados pessoais SE HOUVER lei em sentido formal e proporcional que especifique os parâmetros e critérios necessários para tanto. **Inexistente essa, como no caso em apreço, há de se assegurar a inviolabilidade do direito à proteção de dados.**

Soma-se a isso que a LGPD, por disposição expressa, não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de atividades de investigação e repressão de infrações penais (art. 4º, inciso III, alínea d) e que, **até o momento, não foi editada uma LGPD Penal.**

Ademais, conquanto o Marco Civil da Internet possibilite o acesso a alguns dados pessoais, mediante prévia autorização judicial, como é o caso dos registros de conexão e de acesso a aplicações de internet (art. 22), estejam eles associados ou não a dados cadastrais ou a outras informações, **ele não contém um regramento mínimo para o tratamento dos dados assim compartilhados, prescrevendo apenas que cabe ao juiz “tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário” (art. 23).**

Nesse quadro, ainda que o Relator assegure um controle judicial **posterior** para as hipóteses excepcionais de acesso direto a dados pessoais pelos órgãos da persecução penal, **não havendo, na tese sugerida, qualquer esclarecimento quanto à forma de tratamento desses dados e seu descarte pelos órgãos da persecução penal**, compreendo que o controle judicial **posterior** não é suficiente para evitar (ou reparar)

danos a direitos da personalidade, promovendo a responsabilização dos agentes estatais envolvidos, **de modo a contrabalancear os riscos que decorrem naturalmente desse excepcional tratamento de dados.**

Seguindo essa linha raciocínio, **proponho adicionar, na parte final do item 1 da tese de julgamento, em substituição à integralidade de seu item 2, que as únicas exceções possíveis são aquelas previstas em lei formal e proporcional (a exemplo do art. 17-B da Lei nº 9.613/98 e do art. 13-B do CPP, já declaradas proporcionais pelo STF).**

Já no tocante ao **item 3 da tese julgamento**, o Relator propõe a modulação dos efeitos da decisão, nos seguintes termos:

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

Parece-me que a intenção do Relator, salvo melhor juízo, é a de evitar que a interpretação conforme conferida ao art. 10, § 1º, do MCI produza efeitos retroativos, **permitindo a reabertura de processos findos, inclusive naqueles casos em que tal questão não tenha sido suscitada tempestivamente pela defesa.**

Assim, considerando que se reconhece, aqui, a constitucionalidade da norma questionada, e não sua inconstitucionalidade, **sugiro uma nova redação para o enunciado**, cujo teor, a meu ver, apreende melhor a intenção do Relator:

“2. 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 ressaltadas dessa modulação apenas as investigações ou ações penais em curso nas quais a defesa tenha levantado a controvérsia até a conclusão deste julgamento.**”

Ante todo o exposto, **acompanho o Relator com ressalvas relativamente aos itens 2 e 3 da tese de julgamento.**

Por conseguinte, proponho reformulação da tese de julgamento nos seguintes termos:

“1. É constitucional o art. 10, § 1º, da Lei nº 12.965/14 (Marco Civil da Internet), que condiciona o compartilhamento de dados de tráfego por provedores – 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, **ressalvados apenas os casos previstos em lei formal e proporcional.**

2. 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.**”

É como voto.