AÇÃO DECLARATÓRIA DE CONSTITUCIONALIDADE 51 DISTRITO FEDERAL

RELATOR	**: MIN. GILMAR MENDES**
REQTE.(S)	: FEDERAÇÃO DAS ASSOCIAÇÕES DAS EMPRESAS BRASILEIRAS DE TECNOLOGIA DA INFORMAÇÃO - ASSESPRO NACIONAL
ADV.(A/S)	: ADRIELE PINHEIRO REIS AYRES DE BRITTO
ADV.(A/S)	: MARCELO MONTALVÃO MACHADO
INTDO.(A/S)	: PRESIDENTE DA REPÚBLICA
PROC.(A/S)(ES)	: ADVOGADO-GERAL DA UNIÃO
INTDO.(A/S)	: CONGRESSO NACIONAL
ADV.(A/S)	: ADVOGADO-GERAL DO SENADO FEDERAL
AM. CURIAE.	: FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA
ADV.(A/S)	: THIAGO LUÍS SANTOS SOMBRA
ADV.(A/S)	: FERNANDO DANTAS MOTTA NEUSTEIN
AM. CURIAE.	: VERIZON MEDIA DO BRASIL INTERNET LTDA (ATUAL DENOMINAÇÃO DE OATH DO BRASIL INTERNET LTDA, ANTERIORMENTE CONHECIDA COMO YAHOO! DO BRASIL INTERNET LTDA - VERIZON MEDIA BRASIL)
ADV.(A/S)	: ANDRÉ ZONARO GIACCHETTA
ADV.(A/S)	: VICENTE COELHO ARAÚJO
ADV.(A/S)	: CIRO TORRES FREITAS
AM. CURIAE.	: INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE - IRIS
ADV.(A/S)	: HIGOR PEDROSO NEVES
AM. CURIAE.	: SOCIEDADE DE USUÁRIOS DE TECNOLOGIA - SUCESU NACIONAL
ADV.(A/S)	: RENATO MULLER DA SILVA OPICE BLUM
ADV.(A/S)	: JULIANA ABRUSIO
ADV.(A/S)	: RONY VAINZOF
ADV.(A/S)	: SAMARA SCHUCH BUENO
ADV.(A/S)	: MAURICIO ANTONIO TAMER
ADV.(A/S)	: CAMILA RIOJA ARANTES
AM. CURIAE.	: ABERT - ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO
ADV.(A/S)	: SERGIO BERMUDES

V O T O

O SENHOR MINISTRO GILMAR MENDES (RELATOR): Passo a apreciar as questões jurídicas necessárias ao julgamento do feito.

I – Da preliminar de ilegitimidade ativa suscitada pela AGU e pela PGR

A Advocacia-Geral da União (AGU) e a Procuradoria-Geral da República (PGR) suscitaram a preliminar de ilegitimidade ativa da parte requerente – A Federação das Associações das Empresas Brasileiras de Tecnologia da Informação (Assespro Nacional) -, uma vez que a referida entidade não representaria os interesses de uma específica categoria, sendo composta por empresas da área de informática que integrariam segmentos diversos, o que contrariaria a jurisprudência consolidada do Supremo Tribunal Federal.

No que se refere a essa questão, é importante pontuar, em primeiro lugar, que a extensão da lista de legitimados ativos para a propositura da ação direta de inconstitucionalidade e da ação declaratória de constitucionalidade buscou *"reforçar o controle abstrato de normas no ordenamento jurídico brasileiro, como peculiar instrumento de correção do sistema geral incidente"* (MENDES, Gilmar Ferreira; BRANCO, Gustavo Paulo Gonet. **Curso de Direito Constitucional.** 16ª ed. São Paulo: Saraiva Educação, 2021. p. 1.373).

Destarte, embora existam inúmeras controvérsias jurisprudenciais na definição e identificação das denominadas entidades de classe, à luz da homogeneidade dos interesses jurídicos representados, do caráter nacional de sua atuação e de outras questões sensíveis, não se deve ignorar o objetivo e a intenção do poder constituinte originário de democratizar o acesso à jurisdição constitucional no âmbito do Supremo Tribunal Federal, como resposta aos problemas e às regras vigentes no sistema anterior.

Outrossim, mesmo diante da consolidada jurisprudência do

Supremo, entendo que não assiste razão à AGU e à PGR, já que a entidade requerente representa o interesse comum das empresas de tecnologia, ou seja, de determinada categoria intrinsecamente distinta das demais, tal como assentado por esta Corte na remansosa jurisprudência firmada a partir da ADI 34/DF, Rel. Min. Octavio Gallotti, RTJ 128/481.

Não é por outro motivo que esta Corte já teve inclusive a oportunidade de reconhecer a legitimidade da parte requerente, tal como se observa do recente precedente estabelecido na ADI 4.829, Rel. Min. Rosa Weber, Tribunal Pleno, j. 22.3.2021.

Ressalte-se que a existência de algumas variações em termos de atividades exercidas pelas empresas de tecnologia que integram a entidade requerente não desconfiguram, a meu ver, a homogeneidade da entidade associativa ou a existência do interesse comum e específico que levou ao ajuizamento da presente ação.

Por esses motivos, **rejeito** a preliminar de ilegitimidade ativa.

II - Da rejeição da preliminar de ausência de comprovação de controvérsia jurídica relevante

Também entendo que deve ser afastada a alegação de ausência de comprovação de controvérsia jurídica relevante suscitada pela Advocacia-Geral da União (AGU) e pela Procuradoria-Geral da República (PGR), tendo em vista a demonstração do preenchimento desse requisito pela parte requerente.

Nessa linha, é importante reafirmar que o caso em análise envolve a declaração de constitucionalidade de dispositivos do Código de Processo Civil, do Código de Processo Penal e do Decreto Executivo nº 3.810/2001, que trata do Acordo de Assistência Judiciária em Matéria Penal firmado entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América.

Reproduzo o teor das referidas normas:

CÓDIGO DE PROCESSO CIVIL
Art. 237. Será expedida carta:

[...] II - Rogatória, para que órgão jurisdicional estrangeiro pratique ato de cooperação jurídica internacional, relativo a processo em curso perante órgão jurisdicional brasileiro;

CÓDIGO DE PROCESSO PENAL

Art. 780. Sem prejuízo de convenções ou tratados, aplicar-se-á o disposto neste Título à homologação de sentenças penais estrangeiras e à expedição e ao cumprimento de cartas rogatórias para citações, inquirições e outras diligências necessárias à instrução de processo penal.

[…]

Art. 783. As cartas rogatórias serão, pelo respectivo juiz, remetidas ao Ministro da Justiça, a fim de ser pedido o seu cumprimento, por via diplomática, às autoridades estrangeiras competentes.

Decreto Executivo 3.801/2001

Artigo I

Alcance da Assistência

1. As Partes se obrigam a prestar assistência mútua, nos termos do presente Acordo, em matéria de investigação, inquérito, ação penal, prevenção de crimes e processos relacionados a delitos de natureza criminal.

2. A assistência incluirá:

a) tomada de depoimentos ou declarações de pessoas;

b) fornecimento de documentos, registros e bens;

c) localização ou identificação de pessoas (físicas ou jurídicas) ou bens;

d) entrega de documentos;

e) transferência de pessoas sob custódia para prestar depoimento ou outros fins;

f) execução de pedidos de busca e apreensão;

g) assistência em procedimentos relacionados a imobilização e confisco de bens, restituição, cobrança de multas; e

h) qualquer outra forma de assistência não proibida pelas

leis do Estado Requerido.

3. A assistência será prestada ainda que o fato sujeito a investigação, inquérito ou ação penal não seja punível na legislação de ambos os Estados.

4. As Partes reconhecem a especial importância de combater graves atividades criminais, incluindo lavagem de dinheiro e tráfico ilícito de armas de fogo, munições e explosivos. Sem limitar o alcance da assistência prevista neste Artigo, as Partes devem prestar assistência mútua sobre essas atividades, nos termos deste Acordo.

5. O presente Acordo destina-se tão-somente à assistência judiciária mútua entre as Partes. Seus dispositivos não darão direito a qualquer indivíduo de obter, suprimir ou excluir qualquer prova ou impedir que uma solicitação seja atendida.

Artigo II

Autoridades Centrais

1. Cada Parte designará uma Autoridade Central para enviar e receber solicitações em observância ao presente Acordo.

2. Para a República Federativa do Brasil, a Autoridade Central será o Ministério da Justiça. No caso dos Estados Unidos da América, a Autoridade Central será o Procurador-Geral ou pessoa por ele designada

3. As Autoridades Centrais se comunicarão diretamente para as finalidades estipuladas neste Acordo.

[…]

Artigo IV

Forma e Conteúdo das Solicitações

1. A solicitação de assistência deverá ser feita por escrito, a menos que a Autoridade Central do Estado Requerido acate solicitação sob outra forma, em situações de urgência. Nesse caso, se a solicitação não tiver sido feita por escrito, deverá ser a mesma confirmada, por escrito, no prazo de trinta dias, a menos que a Autoridade Central do Estado Requerido concorde que seja feita de outra forma. A solicitação será redigida no

idioma do Estado Requerido, caso não haja disposição em contrário.

2. A solicitação deverá conter as seguintes informações:

a) o nome da autoridade que conduz a investigação, o inquérito, a ação penal ou o procedimento relacionado com a solicitação;

b) descrição da matéria e da natureza da investigação, do inquérito, da ação penal ou do procedimento, incluindo, até onde for possível determiná-lo, o delito específico em questão;

c) descrição da prova, informações ou outra assistência pretendida; e

d) declaração da finalidade para a qual a prova, as informações ou outra assistência são necessárias.

3. Quando necessário e possível, a solicitação deverá também conter:

a) informação sobre a identidade e a localização de qualquer pessoa (física ou jurídica) de quem se busca uma prova;

b) informação sobre a identidade e a localização de uma pessoa (física ou jurídica) a ser intimada, o seu envolvimento com o processo e a forma de intimação cabível;

c) informação sobre a identidade e a localização de uma pessoa (física ou jurídica) a ser encontrada;

d) descrição precisa do local ou pessoa a serem revistados e dos bens a serem apreendidos;

e) descrição da forma sob a qual qualquer depoimento ou declaração deva ser tomado e registrado;

f) lista das perguntas a serem feitas à testemunha;

g) descrição de qualquer procedimento especial a ser seguido no cumprimento da solicitação;

h) informações quanto à ajuda de custo e ao ressarcimento de despesas a que a pessoa tem direito quando convocada a comparecer perante o Estado Requerente; e

i) qualquer outra informação que possa ser levada ao conhecimento do Estado Requerido, para facilitar o cumprimento da solicitação.

De acordo com o requerente, embora o procedimento estabelecido pelas referidas normas para cooperação jurídica em matéria penal seja observado, como regra, em relação aos dados ou documentos que se encontram em posse de empresas sediadas em outros países, tal como ocorre em relação aos dados bancários de cidadãos localizados no exterior, estaria ocorrendo o afastamento ou a não aplicação dessas leis em relação às empresas de tecnologia, com a declaração escamoteada de inconstitucionalidade.

Para comprovar a sua alegação, a parte autora colaciona aos autos inúmeros precedentes dos seguintes Tribunais:

> 1) do Superior Tribunal de Justiça (Inq 784/DF, Rel. Ministra LAURITA VAZ, Corte Especial, julgado em 17/4/2013; RHC 57.763/PR, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA, julgado em 01/10/2015; RMS: 44892 SP 2014/0020978-7, Relator: Ministro RIBEIRO DANTAS, Data de Julgamento: 05/04/2016; RMS: 46685 MT 2014/0254825-8, Relator: Ministro LEOPOLDO DE ARRUDA RAPOSO, Data de Publicação: DJ 06/04/2015; RMS: 46.685 MT 2014/0254825-8, Relator: Ministro Reynaldo Soares da Fonseca, Data da Publicação: DJ 11/10/2017);
>
> 2) do TRF-1ª Região (MS 0002854-06.2017.4.01.0000/DF, Relator: Desembargador Federal Cândido Ribeiro, Segunda Seção, Julgado em 07.06.2017);
>
> 3) do TRF-2ª Região (MS 11114 2013.02.01.010585-4, CNJ 0010585-65.2013.4.02.0000, Relator: Desembargador Federal Abel Gomes, 1ª Turma Especializada, julgado em 18/12/2013);
>
> 4) do TRF-4ª Região (TRF4, AG 0013618-43.2012.404.0000, OITAVA TURMA, Relator para Acórdão VICTOR LUIZ DOS SANTOS LAUS, D.E. 17/07/2013)

Nesses casos, o afastamento das leis e atos normativos federais estaria ocorrendo com base no princípio da territorialidade e da proteção à soberania nacional, o que violaria, segundo os autores, diversas normas

e princípios constitucionais, como a soberania e a igualdade entre os Estados, o princípio da cooperação internacional, a livre iniciativa, a não intervenção e a solução pacífica de conflitos (arts. 1º e 4º da CF/88).

Nos julgados indicados, os Tribunais do país não se utilizaram da via da cooperação jurídica internacional e determinam a solicitação direta de dados das empresas de tecnologia a suas subsidiárias instaladas no país, mesmo quando tais informações se encontram em servidores localizados no exterior.

Nessa toada, afirma a requerente que as empresas nacionais não possuem a disponibilidade desses dados. Outrossim, afirma que essas companhias vêm enfrentando diversas sanções ilegais, como a aplicação de pesadas multas e a ameaça de cumprimento de ordens de prisão contra os seus dirigentes.

A ASSESPRO NACIONAL também colacionou aos autos diversas decisões de outros Tribunais que tem assentado a constitucionalidade das normas do CPC, do CPP e do MLAT, com a remissão aos procedimentos diplomáticos de cooperação internacional para fins de obtenção dos dados pleiteados.

Nesse sentido, a requerente faz menção aos seguintes casos:

> 5) TJPE, MS nº 0014221-86.2013.8.17.0000, Relator para o acórdão: Desembargador Gustavo Augusto Lima, Terceira Câmara Criminal, Julgado 19.08.2014;
>
> 6) TJPR, MSC nº 1.396.365-4. Relator: Desembargador Arquelau Araujo Ribas, 3ª Câmara Criminal, Julgado em 19.11.2015
>
> 7) TRF5, PROCESSO: 00017365220154050000, HC5934/RN, DESEMBARGADOR FEDERAL FRANCISCO WILDO LACERDA DANTAS, Primeira Turma, JULGAMENTO: 17/12/2015
>
> 8) TJDFT, Acórdão nº 1020417, 20160020295498MSG, Relator: ROMÃO C. OLIVEIRA, CÂMARA CRIMINAL, Data de Julgamento: 15/05/2017
>
> 9) Decisão da Vara Criminal de Palmital/PR, Processo nº 0001994-70.2014.8.16.0125, julgado em 9.4.2015;

10) Decisão da Vara Criminal de Antonina, Processo nº 0001960-50.2014.8.16.0043.

Os inúmeros casos mencionados pela Requerente em sentidos diversos, com interpretações que afastam a aplicação de leis e atos normativos federais, e as relevantes consequências jurídicas, econômicas, tecnológicas e financeiras das referidas decisões são suficientes para se concluir pelo cabimento desta ação em virtude da demonstração de controvérsia jurídica relevante envolvendo a constitucionalidade dos dispositivos legais indicados (art. 14, III, da Lei 9.868/99).

Contudo, deve ser observado que a controvérsia constitucional veiculada nesta ADC é, a rigor, mais ampla do que a simples declaração de validade do uso das cartas rogatórias e dos acordos MLAT para fins de investigação criminal.

As decisões judiciais mencionadas na inicial, que estariam implicitamente declarando a inconstitucionalidade dos dispositivos relacionados ao cumprimento de cartas rogatórias e à aplicação de tratado de assistência mútua em matéria penal, baseiam-se também na aplicação do artigo 21 do Código de Processo Civil e do artigo 11 do Marco Civil da Internet, que atribuem jurisdição e determinam a imperiosa aplicação da lei brasileira sempre que a coleta de dados ocorrer em território nacional e ainda que a empresa responsável seja estrangeira.

Portanto, penso que é imprescindível que se considere esse plexo normativo no julgamento desta ação, sob pena de se decidir sobre a constitucionalidade de uma norma, sem se analisar as consequências que serão reproduzidas sobre a constitucionalidade ou a operabilidade desses outros dispositivos legais e, em última análise, sobre a realidade subjacente.

Nessa perspectiva, não é demais recordar a sempre atual advertência feita por Eros Roberto Grau, quando aduz que não se interpreta a Constituição e o Direito em tiras, aos pedaços. Ao contrário, a atividade interpretativa se exerce a partir do Direito e da Constituição no seu todo.

A jurisprudência do STF segue essa linha de raciocínio, ao aduzir a

possibilidade de julgamento dos processos de controle abstrato de constitucionalidade com base em fundamentos distintos daqueles indicados pelo autor da ação (causa de pedir ou *causa petendi* aberta, conforme estabelecido no julgamento da ADI 3796/PR, Rel. Min. Gilmar Mendes, julgado em 8.3.2017).

Destarte, todo e qualquer dispositivo da Constituição Federal ou do restante do bloco de constitucionalidade poderá ser utilizado pelo STF como fundamento jurídico para declarar uma lei ou ato normativo (in)constitucional.

Assim, a rigor, o que está em debate nesta ação não é apenas a constitucionalidade de determinados dispositivos do Código de Processo Civil, do Código de Processo Penal e do Decreto Executivo nº 3.810/2001 que estabelecem a cooperação jurídica internacional, já que é igualmente importante analisar se os Tribunais brasileiros podem utilizar o art. 11 do Marco Civil da Internet para estabelecer o dever das empresas de tecnologia a fornecer essas informações, desde que observados os requisitos legais. Ou seja, cabe a esta Corte analisar a compatibilidade de todos esses dispositivos normativos com a Constituição Federal.

No que se refere à mencionada norma do marco civil da internet, veja-se a redação do referido artigo:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua

> estabelecimento no Brasil.
>
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
>
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Outra regra semelhante recentemente incorporada ao ordenamento jurídico brasileiro é o art. 18 da Convenção de Budapeste, o qual estabelece que:

> "**Artigo 18º. – Injunção**
>
> 1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:
>
> **a. A uma pessoa que se encontre no seu território** que comunique os dados informáticos específicos, na sua posse ou sob o seu controle e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e
>
> **b. A um fornecedor de serviços que preste serviços no território da Parte**, que comunique os dados na sua posse ou sob o seu controle, relativos aos assinantes e respeitantes a esses serviços."

Destarte, entendo que deve ser rejeitada a preliminar suscitada pela AGU e pela PGR. Contudo, com base na teoria da causa de pedir aberta, compreendo que a análise da constitucionalidade e obrigatoriedade de utilização do dispositivos invocados deve levar em consideração a legislação superveniente, em especial a norma prevista pelo **art. 11 do Marco Civil da Internet** e pelo **art. 18 da Convenção de Budapeste**.

Por fim, teço uma última demarcação do objeto desta Ação: **o uso de medidas constritivas do art. 12 do Marco Civil da Internet <u>não é objeto</u>**

desta ADC 51, mas sim da ADI 5.527, (de Relatoria da Eminente Presidente, Ministra Rosa Weber) **e da ADPF 403** (de Relatoria do Eminente Ministro Edson Fachin)**.** Esses dois casos, sim, discutem diretamente as medidas e sanções judiciais cabíveis em caso de recusa de entrega das informações determinadas em requisições diretas, no qual há discussões relevantes em termos de proporcionalidade em sentido abstrato e concreto.

Em assim sendo, delimitada a questão da relevância da controvérsia jurídica indicada na petição inicial, à luz da constitucionalidade dos dispositivos acima mencionados com a ordem constitucional, passo a apreciar o mérito desta ADC.

III – Do estado da arte das discussões sobre a obtenção de dados como evidências criminais por requisição judicial direta ou por acordos de cooperação mútua

A discussão jurídica travada no caso em tela tem sido debatida ao redor do mundo. O mote desse debate tem a ver com as dificuldades que os órgãos de persecução criminal muitas vezes enfrentam para acessar legalmente dados e conteúdos de comunicações que são armazenadas ou transportadas por provedores de aplicações de internet.

Quando um suspeito de utiliza aplicativos como o WhatsApp ou Telegram, os dados de comunicação estão naturalmente protegidos pelo acesso a terceiros. As interceptações de dados que os órgãos Estatais conseguem fazer de maneira remota geralmente só revelam informações criptografadas e, portanto, ilegíveis.

Essa realidade dá ensejo ao que na literatura jurídica e na comunidade policial internacional se chama de risco de efeito "*Going Dark"*. Essa expressão foi cunhada em 2014 pelo então diretor do FBI James Comey que se refere a ele como "*o fenômeno em que os agentes da lei, mesmo possuindo um mandado judicial para interceptar e acessar as comunicações de alguém, não tem a capacidade técnica de fazê-lo"* (COMEY, James. **Going Dark: Are Technology, Privacy, and Public Safety in a**

Collision Course? Discurso proferido no Brookings Institute, 14 out. 2014).

De forma mais específica, no presente caso, o que importa definir é em que medida o Poder Judiciário brasileiro pode ordenar que provedores de aplicações como redes sociais, provedores de e-mails e aplicativos de mensagens instantâneas concedam acesso aos dados e conteúdos de comunicações privadas que são armazenadas em bancos de dados sediados em países estrangeiros.

A questão suscita naturalmente conflitos entre direitos fundamentais básicos relacionados à privacidade e à segurança da informação. Além disso, o debate torna-se ainda mais sensível do ponto de vista da reflexão sobre os limites da jurisdição, considerando que as grandes plataformas de internet, como redes sociais e os veículos de comunicação em geral, não armazenam esses dados no mesmo país em que as comunicações ocorrem.

Nas últimas décadas, tem se diagnosticado um movimento estratégico por parte dos Estados nacionais de criação de leis domésticas que impõem aos agentes econômicos que atuam na internet o dever de obedecer às determinações dos Tribunais nacionais, ainda que as operações *on-line* mediadas por essas empresas não ocorram inteiramente dentro do país (LAMBACH, Daniel. "The Territorialization of Cyberspace". **International Studies Review**, p. 1–25, 2019, p. 13–17.).

Essa tendência se fortaleceu sobretudo a partir da revelação do escândalo Snowden. Após esse caso, diversos países aprovaram leis que obrigam provedores de comunicação como Facebook, Google e Apple a armazenar nacionalmente os conteúdos das comunicações (DASKAL, Jennifer. "Privacy and Security Across Borders". **Yale Law Journal Forum**, v. 1029, p. 1–16, 2019, p. 1047).

Conforme já tive a oportunidade de observar, em trabalho acadêmico escrito em conjunto com Victor Oliveira Fernandes, as disputas acerca da obtenção de evidências criminais digitais em cooperações internacionais notabilizam os desafios do constitucionalismo digital diante da tendência de re-territorialização do ciberespaço. Como

destaquei:

> Uma das principais estratégias normativas que os Estados Nacionais têm utilizado para contrapor sua soberania na internet consiste na edição de leis nacionais que tentam "re-territorializar" a rede. Essas estratégias em geral se concretizam em legislações formais que impõem aos agentes econômicos o dever de obedecer às determinações dos Tribunais nacionais, ainda que as operações *on-line* mediadas por essas empresas não ocorram inteiramente dentro do país. Também se observam situações mais extremas em que os governos implantam *firewalls* que inviabilizam o acesso dos usuários nacionais a conteúdos censurados. Essa agenda política de recuperação da soberania estatal na rede é vista com extrema preocupação por muitos autores que temem que esse movimento resulte em uma "fragmentação" da rede, comprometendo sua integridade. (MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. "Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro". **Revista Brasileira de Direito**, Passo Fundo, v. 16, n. 1, out. 2020, p. 22)

No caso em tela, o objetivo intrínseco de disposições normativas como a contemplada regra do art. 11 do Marco Civil da Internet é o de resguardar a soberania nacional, obrigando que certos tipos de dados coletados dentro do país possam ser armazenados e processados nacionalmente.

A despeito da complexidade desse debate no âmbito transnacional, o qual será aprofundado a seguir, fato é que, em diversos países que adotam esse tipo de legislação, conflitos judiciais têm se desenvolvido entre autoridades de persecução penal, que alegam deter autoridade para compelir as empresas de internet a divulgar os dados de comunicação que armazenam, e as grandes empresas de internet, que defendem que tais informações só poderiam ser compartilhadas com estados estrangeiros por meio de acordos de assistência mútua (MLATs), mecanismos tradicionais para essa finalidade de compartilhamento de

provas.

Os MLAT são os mecanismos mais utilizado para requisição de assistência estrangeira de provas em investigações criminais domésticas. O seu processamento exige que o Estado requerente faça um pedido diplomático e aguarde a resposta da jurisdição que detém o controle sobre essas provas.

Tal processo é naturalmente moroso, já que, mesmo quando o governo assistente concorda em compartilhar as provas, é necessário que sejam cumpridas etapas formais desse processo, que às vezes demoram meses ou anos. Essa morosidade torna-se crítica para o compartilhamento de dados digitais, já que esses dados são naturalmente efêmeros e podem não estar mais disponíveis quando do cumprimento da assistência mútua.

Por outro lado, a principal preocupação com os regimes de requisição direta é que eles podem permitir que os Estados Nacionais submetam unilateralmente empresas estrangeiras ao regime jurídico do país que expediu a ordem judicial sem que nenhum *standard* de cooperação substantiva ou procedimental seja previamente observado, o que claramente suscita tensões do ponto de vista da soberania nacional.

Além disso, do ponto de vista econômico, gigantes de internet como o Facebook defendem que a possibilidade de requisição judicial direta pode fazer com que as empresas fiquem expostas a violações das leis de proteção de dados vigentes no local de sua sede, o que resultaria em obstáculos significativos para o funcionamento global dos modelos de negócios dessas plataformas.

Do ponto de vista técnico, as dificuldades de compreensão desses embates residem na natureza diferenciada dos dados enquanto meio de prova. Os dados gerados em comunicações digitais são armazenados por empresas como Facebook, Google e Apple em redes de unidades de armazenamento situadas em um território (comumente chamadas de "nuvens"). Desse modo, a uma primeira vista, seria possível entender que os desafios do compartilhamento de evidências criminais digitais não difeririam substancialmente das disputas tradicionais em matéria de

cooperação internacional.

Todavia, como destacado por autores como a professora Jennifer Daskal, da faculdade de Direito da Universidade de Yale, há particularidades técnicas do armazenamento de dados – como a sua mobilidade, a divisibilidade das informações que eles contêm e a possibilidade de dissociação entre a localização do acesso e a localização do dado – que sugerem uma inadequação do próprio critério de territorialidade que tradicionalmente define os limites da jurisdição dos estados nacionais. Daí porque a autora chega a afirmar que "*os dados subvertem a pressuposição tradicional de que existe uma vinculação entre a localização do dado e o regime jurídico que deve ser a ele aplicado*". Nesse sentido, Daskal afirma que, mais do que multi-territoriais, os dados possuem uma verdadeira natureza "a-territorial" (DASKAL, Jennifer. **The Un-Territoriality of Data.** *The Yale Law Journal*, v. 2015, p. 326–398, 2015).

Devido a esse perfil "aterritorial" dos dados, diversos embates jurídicos sobre os limites da requisição têm sido travados em jurisdições estrangeiras. Um casos mais conhecidos ocorreu nos **Estados Unidos**, no precedente **Microsoft Corporation v. United States**. Nesse caso, no ano de 2014, um juiz de primeira instância expediu mandado judicial autorizando que o governo dos EUA tivesse acesso a dados de comunicações armazenados pela Microsoft na Irlanda e que seriam importantes para uma investigação de tráfico de drogas nos Estados Unidos. Esse mandado foi expedido com base no § 2703(a) do *Stored Communications Act*, o qual autorizava esse tipo de requisição direta para a instrução de processos penais. A Microsoft se opunha à execução da ordem argumentando que a apreensão dos dados armazenados na Irlanda configuraria uma busca e apreensão extraterritorial, que fugiria à competência do Judiciário norte-americano, sendo, por isso, necessário acionar os mecanismos de cooperação internacional por intermédio do Departamento de Justiça.

A decisão foi confirmada em segunda instância e o Tribunal condenou a Microsoft por descumprimento de ordem judicial, considerando que a decisão não havia sido inteiramente adotada. Em

seguida, a condenação foi anulada com base no fundamento de que a disponibilização de tais dados seria uma aplicação extraterritorial não autorizada da legislação. Em 2018, a **Suprema Corte dos Estados Unidos** reconheceu a relevância constitucional da demanda e concedeu o *writ of certiorari*, mas logo em seguida considerou que a causa havia perdido o objeto, ante à entrada em vigor do *Clarifying Lawful Overseas Use of Data Act* (*CLOUD Act*), que será discutido a seguir.

Na **Noruega**, a Suprema Corte daquele país proferiu a decisão nº HR *2019-610-A*, em 28.3.2019, na qual declarou a legalidade de busca e apreensão realizada pela Polícia na empresa Norueguesa Tidal Music AS, em Oslo, com a validação da apreensão de arquivos digitais encontrado nos computadores das empresas que estavam localizados no exterior. Nesse caso, a Corte considerou que a busca não violaria o princípio da soberania de outros Estados (http://www.codices.coe.int/NXT/gateway.dll/CODICES/full/eur/nor/eng/nor-2019-x-005).

A Suprema Corte da **Bélgica** declarou a legalidade de decisão que impôs multa à empresa Yahoo por não colaborar com a aplicação da lei belga em uma investigação de fraude cometida por meio de contas de e-mails da companhia (https://rm.coe.int/16806b8a7c).

Por sua vez, a Liga Internacional contra o Racismo e o Antisemitismo (LICRA) e a União dos Estudantes Judeus da França (UEJF), organizações localizadas no país europeu, conseguiram obter no Superior Tribunal de **Paris** uma ordem para proibir o serviço de leilões on-line promovidos pelo Yahoo que estava comercializando itens de coleção do período nazista, o que violava o artigo R645-1 do Código Penal francês (http://www.techlawjournal.com/topstories/2004/20040823.asp).

A empresa argumentou que esses leilões foram conduzidos sob a jurisdição dos Estados Unidos e que não haveria meios técnicos para impedir que residentes franceses participassem desses eventos sem colocar a empresa em dificuldades financeiras e comprometer a existência da Internet, já que os servidores que armazenavam essas informações estavam localizados no território dos EUA, sendo voltados

principalmente para residentes desse país (http://www.techlawjournal.com/topstories/2004/20040823.asp).

A empresa alegou ainda que a Primeira Emenda à Constituição dos Estados Unidos garante o direito à liberdade de expressão e que o tribunal francês era incompetente para o caso (http://www.techlawjournal.com/topstories/2004/20040823.asp).

Ao julgar em favor dos requerentes, o tribunal francês considerou possuir jurisdição sobre o caso e ordenou que a Yahoo tomasse medidas para impedir o acesso de residentes franceses ao leilão (http://www.techlawjournal.com/topstories/2004/20040823.asp).

Após serem notificados para o cumprimento da ordem nos Estados Unidos, a empresa decidiu levar o caso para o *District Court* do Norte da Califórnia, requerendo que a decisão não produzisse efeitos no país. O Tribunal julgou favorável à empresa e entendeu que a decisão era incompatível com a Primeira Emenda dos EUA, mas esse acórdão foi revertido pelo Tribunal do Nono Circuito, com a manutenção da decisão proferida pelo tribunal francês (http://www.techlawjournal.com/topstories/2004/20040823.asp).

Pelo que se observa a partir desses casos, a legislação estrangeira e a decisão dos tribunais internacionais tem se pautado em alguns critérios para definir o alcance da jurisdição estatal sobre os dados e as comunicações eletrônicas, como: a) a nacionalidade e o local de residência dos cidadãos envolvidos em pedidos de acesso a dados e a comunicações digitais; b) o impacto dos dados ou conteúdos sobre atividades ou serviços existentes no território nacional; c) o uso de registro de domínios vinculados a serviços prestados no país como indicativo do exercício de atividades capaz de estabelecer a submissão à jurisdição brasileira; d) a localização dos servidores das empresas prestadoras de serviços de conexão ou de aplicativos para a internet; e) a prestação de algum serviço ou a realização de algum ato em território nacional, como o envio, a coleta, o armazenamento ou o tratamento de dados e de comunicações.

Em relação ao item "e", é importante destacar que o Departamento de Justiça dos Estados Unidos, a partir da interpretação do novo CLOUD

ACT recentemente promulgado, tem estabelecido que "*quanto maior for o direcionamento de uma empresa para conduzir seus negócios nos Estados Unidos, maior será a probabilidade de os tribunais considerarem a submissão dessa empresa à jurisdição norte-americana*" (ESTADOS UNIDOS, US Department of Justice, **Promoting Public Safety, Privacy, and the Rule of Law Around The World:** The Purpose and Impact of the CLOUD Act. White Paper. 2019. p. 8).

Feita essa breve exposição sobre o estado da arte das discussões envolvendo a requisição de dados de empresas localizados no exterior, passo a apreciar a constitucionalidade dos dispositivos anteriormente indicados.

IV – Da constitucionalidade das normas indicadas e dos parâmetros para a aplicação do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste

Fixadas as premissas da discussão travada nesta ADC, percebe-se que, em verdade, a requerente busca que este STF se pronuncie sobre a constitucionalidade dos dispositivos que estabelecem a cooperação jurídica internacional em contraposição ao modelo de requisição direta definido pelo art. 11 do Marco Civil da Internet.

Pelo que se observa, a tese autoral ancora-se no pressuposto de que a jurisdição brasileira sobre a internet deve ser pautada primordialmente, ou exclusivamente, pelo princípio da territorialidade que tradicionalmente guia a persecução criminal.

De fato, o Decreto Executivo Federal no 3.810/2001, bem como o artigo 237, II, do Código de Processo Civil e os artigos 780 e 783 do Código de Processo Penal, formam um sistema importante e válido de cooperação jurídica internacional para obtenção de provas que estão localizadas fora do território nacional.

Nessa linha, é relevante ressaltar que a expedição de cartas rogatórias e a celebração de acordos unilaterais ou multilaterais é solução tradicionalmente aceita para a comunicação de atos processuais,

a obtenção de dados ou a prática de qualquer outro ato que exija a cooperação de Estados estrangeiros.

Nesse sentido, em parecer juntado aos autos, o eminente Ministro Francisco Rezek destaca que "*o caminho para que o Estado exercite sua jurisdição além dos limites de seu território, fazendo valer sua autoridade em território alheio, é o da cooperação internacional*", com a emissão de "*carta rogatória, emitida pelo juízo que deseja afetar, de algum modo, pessoa, bem ou relação jurídica no estrangeiro*" (eDOC 5, p. 28).

Discorrendo sobre o tema no âmbito do processo penal, Aury Lopes Jr. destaca que:

> "Ao contrário do que ocorre no Direito Penal, onde se trava longa e complexa discussão sobre a extraterritorialidade da lei penal, no processo penal a situação é mais simples. **Aqui vige o princípio da territorialidade. As normas processuais penais brasileiras só se aplicam no território nacional, não tendo qualquer possibilidade de eficácia extraterritorial."** (LOPES JR., Aury. **Direito Processual Penal.** Recurso eletrônico (e-book). Posição 2.420).

Portanto, a prática de atos investigatórios ou processuais, a obtenção de provas localizadas no exterior, sob a jurisdição de um Estado estrangeiro, deve observar a independência das nações, a autodeterminações dos povos, a não intervenção, a igualdade entre os Estados, a cooperação e a solução pacífica dos conflitos, conforme expressamente estabelecido pelos incisos do art. 4º da CF/88.

Esse modelo tem funcionado de forma adequada em relação a bens físicos, tendo em vista a sua excepcionalidade e a precisa delimitação das fronteiras territoriais.

Contudo, por diversos motivos, a transposição da lógica de territorialidade penal para o campo das discussões sobre os limites da atuação judicial na internet compromete significativamente a efetividade da persecução penal.

De acordo com Jacqueline de Souza Abreu, o modelo de cartas

rogatórias e de cooperação jurídica internacional:

> "funcionou com sucesso – e, na maior parte das situações, ainda funciona –por duas razões centrais. Primeiro, porque, em geral, é um esquema idealizado para situações raras e excepcionais. Na grande maioria dos processos, não há que se realizar extradições, ouvir testemunhas estrangeiras nem obter provas no exterior. Segundo, porque a identificação dos limites da jurisdição e da necessidade de se recorrer a meios de cooperação é relativamente simples para meios físicos: se autoridades do país 'A' precisam de pessoas ou documentos fisicamente localizados no território do país 'B', o país 'A' necessariamente precisa solicitar cooperação do país 'B', já que não pode exercer poder fora de seu território." (ABREU, Jacqueline de Souza. Obtenção de Evidências Digitais: quando são necessários pedidos de cooperação internacional? *In*: ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. **Direitos Fundamentais e Processo Penal na Era Digital.** São Paulo: InternetLab, 2018. p. 156).

Contudo, em relação a dados ou a comunicações virtuais, a situação é mais sensível. Conforme destacado por Jacqueline Abreu na audiência pública realizada:

> "os documentos digitais, como já foi dito aqui, possuem uma natureza intangível. Ou seja, ao mesmo tempo que eles estão de fato localizado na forma de *bits*, em algum servidor ou lugar no mundo, eles podem também ser acessados virtualmente de qualquer outro lugar. E, também, as pessoas que controlam essas informações e detêm o poder sobre esses servidores estão presentes multinacionalmente, seja através de sua sede, de subsidiárias ou simplesmente virtualmente. […]
>
> A natureza aterritorial de dados, como diz a professora Jennifer Daskal, e também a existência desses diversos elementos de conexão para dados eletrônicos faz com que também a proteção legal conferida a essas informações, a esses

> dados, seja suscitada simultaneamente por diversos países. Então, dados podem ter sido coletadas aqui no Brasil, mas estarem armazenados em servidores na Suécia e ser controlados por empresas americanas. Isso atrai simultaneamente a legislação dos três países."

Os problemas do modelo de obtenção de dados pela via diplomática restaram claramente demonstrado através dos dados aportados pelo Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), que trouxe aos autos informações bastante relevantes acerca da morosidade do atendimento dos pedidos de cooperação via MLAT.

Nessa linha, as informações prestadas na Audiência Pública e replicada nos autos apontam que em relação aos pedidos de quebra de sigilo e obtenção de dados telemáticos nos Estados Unidos, em dados consolidados de 2014 a 2017, 28 pedidos ainda se encontram em andamento, sendo que oito foram enviados em 2014, outros oito em 2015, cinco em 2016 e sete em 2017 (eDOC 92, p. 19).

Ademais, as autoridades brasileiras apenas obtiveram respostas positivas em 22,5% dos casos, o que reforça a conclusão dos representantes do Poder Executivo e do Ministério Público no que se refere ao baixo índice de efetividade desses pedidos de assistência jurídica enviados aos Estados Unidos para a quebra de sigilo de dados ou obtenção de informações telemáticas (eDOC 92, p. 20).

Destaque-se que esse baixo índice de efetividade do MLAT em relação à obtenção de dados eletrônicos é inversamente proporcional às demais diligências realizadas com base no acordo, já que em relação às demais matérias, as estatísticas apresentadas pelo DRCI apontam para uma taxa de êxito em torno de **setenta por cento.**

Portanto, constata-se que há uma situação de baixa efetividade do MLAT no que se refere à obtenção de dados eletrônicos, com severas consequências sobre a apuração de crimes cometidos em ambiente virtual e sobre o dever do Estado e o direito dos cidadãos brasileiros à segurança pública e à proteção dos demais direitos fundamentais (arts.

5º e 144 da CF/88).

Além disso, a corroborar a inadequação do princípio da territorialidade, as legislações nacionais de diversos países e os Tratados Internacional aplicáveis à matéria têm proposto critérios complementares de definição da jurisdição penal.

Nesse sentido, o art. 18 da Convenção sobre Cibercriminalidade do Conselho da Europa (CETS nº 185 - Convenção de Budapeste), que foi recentemente incorporada ao ordenamento jurídico brasileiro por intermédio do Decreto Legislativo nº 37, de 16.12.2021, traz como critérios adicionais de extensão da jurisdição (i) a localização da pessoa jurídica que tem a posse ou o controle dos dados armazenados em um sistema informático e (ii) o fato de a pessoa jurídica fornecedora dos serviços de internet prestar o serviço no território daquele país.

Com base nessa orientação geral, diversos países passaram a editar legislações nacionais que impõem aos agentes econômicos o dever de obedecer às determinações dos tribunais nacionais, ainda que as operações *on-line* mediadas por essas empresas não ocorram inteiramente dentro do país, o que enseja um fenômeno de "territorialização" do ciberespaço, conforme anteriormente mencionado (LAMBACH, Daniel. "The Territorialization of Cyberspace". **International Studies Review**, p. 1–25, 2019, p. 13–17).

Também no plano internacional se observam situações mais extremas em que os governos implantam *firewalls* que inviabilizam o acesso dos usuários nacionais a conteúdos censurados.

No caso do Brasil, além da recente adesão à Convenção de Budapeste, que possibilita a requisição de dados sob posse ou controle de empresas ou em relação a serviços prestados em território nacional, nos termos do já mencionado art. 18 do tratado internacional, o art. 11 do Marco Civil da Internet também prevê a obrigatoriedade de os provedores de conexão e de aplicações de internet submeterem-se à legislação nacional, inclusive para fins de prestar informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de

dados.

Transcrevo, mais uma vez, a redação do referido dispositivo:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> § 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
>
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
>
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Com fundamento no art. 11 do MCI, os Tribunais brasileiros têm rejeitado o argumento da imprescindibilidade do uso dos acordos MLAT. Nesse sentido, decisões do STJ, por exemplo, reforçam que o funcionamento da empresa em território nacional submete-a ao cumprimento das leis nacionais, inclusive no que diz respeito à requisição de dados:

> QUESTÃO DE ORDEM. DECISÃO DA MINISTRA

> RELATORA QUE DETERMINOU A QUEBRA DE SIGILO TELEMÁTICO (GMAIL) DE INVESTIGADOS EM INQUÉRITO EM TRÂMITE NESTE STJ. GOOGLE BRASIL INTERNET LTDA. DESCUMPRIMENTO. ALEGADA IMPOSSIBILIDADE. INVERDADE. GOOGLE INTERNATIONAL LLC E GOOGLE INC. CONTROLADORA AMERICANA. IRRELEVÂNCIA. EMPRESA INSTITUÍDA E EM ATUAÇÃO NO PAÍS. OBRIGATORIEDADE DE SUBMISSÃO ÀS LEIS BRASILEIRAS, ONDE OPERA EM RELEVANTE E ESTRATÉGICO SEGUIMENTO DE TELECOMUNICAÇÃO. TROCA DE MENSAGENS, VIA E-MAIL, ENTRE BRASILEIROS, EM TERRITÓRIO NACIONAL, COM SUSPEITA DE ENVOLVIMENTO EM CRIMES COMETIDOS NO BRASIL. INEQUÍVOCA JURISDIÇÃO BRASILEIRA. DADOS QUE CONSTITUEM ELEMENTOS DE PROVA QUE NÃO PODEM SE SUJEITAR À POLÍTICA DE ESTADO OU EMPRESA ESTRANGEIROS. AFRONTA À SOBERANIA NACIONAL. IMPOSIÇÃO DE MULTA DIÁRIA PELO DESCUMPRIMENTO (RMS 55.019/DF, Rel. Ministro Joel Ilan Paciornik, Quinta Turma, julgado em 12/12/2017, DJe 01/02/2018 e Inq 784/DF, Rel. Ministra LAURITA VAZ, CORTE ESPECIAL, julgado em 17/04/2013, DJe 28/08/2013).

Pelo que se observa, o art. 11 do Marco Civil da Internet, que encontra respaldo no art. 18 da Convenção de Budapeste em termos de deveres acordados pelo Estado brasileiro com os demais países do mundo a nível internacional, é norma específica em relação às regras gerais do MLAT, das cartas rogatórias e da cooperação jurídica internacional, e estabelece a aplicação da legislação brasileira e a jurisdição nacional sobre atividades de coleta, armazenamento, guarda e tratamento de registros, dados e comunicações eletrônicas ocorridas em território nacional, desde que pelo menos um dos atos ou terminais se encontrem em território nacional e ainda que a pessoa jurídica portadora dessas informações esteja localizada ou armazene tais informações no exterior.

É importante observar que essa específica diretriz da legislação brasileira está em consonância com os mais atuais diplomas normativos sobre o tema. Nessa linha, a nota técnica apresentada pela PGR nos autos desta ação aponta para a incidência do critério da atividade para fins de definição da jurisdição dos Estados nacionais.

Segundo consta do parecer ministerial (eDOC 112, p. 24/25):

> "há anos diversas soluções têm sido pensadas pela comunidade internacional, algumas delas já traduzidas em entendimentos internacionais e em normais legais internas, incluindo a legislação pátria, que possui dispositivos específicos sobre o assunto. **As soluções que vêm sendo aplicadas utilizam-se de dois critérios adicionais ao da territorialidade sobre os dados, passando-se a utilizar também controle de dados e efeitos da atividade para definir jurisdição sobre a prova.**
>
> O primeiro critério reconhece, justamente, a peculiar mobilidade dos dados informáticos. Como é possível alterar o local de armazenamento dos dados a qualquer momento, o que torna inútil fixar a jurisdição unicamente pela localização de tais dados, segundo o critério de controle, terá autoridade sobre a prova o Juízo ou as autoridades legais do local em que estiver constituída a empresa que controla os dados, e neste ponto, pouco importa se essa empresa é a sede de um grande conglomerado ou apenas uma subsidiária componente de grupo econômico.
>
> **O segundo critério, baseado na fixação de jurisdição a partir dos efeitos da atividade desenvolvida, estabelece que terá autoridade sobre a prova eletrônica o Estado no qual o serviço que coleta esses dados e comunicações for, especialmente, ainda que não exclusivamente, oferecido.** Segundo esse critério, pouco importa o local onde se situa a empresa, que pode sequer ter filial ou representante no território do Estado requisitante: este terá jurisdição sobre os dados colhidos desde que os efeitos da atividade desenvolvida sejam sentidos em seu território."

Na mesma linha, o art. 18 da Convenção de Budapeste (Convenção sobre Cibercriminalidade do Conselho da Europa nº 185), que foi recentemente incorporada ao ordenamento jurídico brasileiro, prevê que:

> "**Artigo 18º. – Injunção**
>
> 1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:
>
> **a. A uma pessoa que se encontre no seu território** que comunique os dados informáticos específicos, na sua posse ou sob o seu controle e armazenados num sistema informático ou num outro suporte de armazenamento de dados informáticos; e
>
> **b. A um fornecedor de serviços que preste serviços no território da Parte**, que comunique os dados na sua posse ou sob o seu controle, relativos aos assinantes e respeitantes a esses serviços."

Destarte, não vislumbro violação aos princípios da autodeterminação dos povos, da igualdade entre os Estados e da cooperação previsto pelo art. 4º, III, V e IX da CF/88, nas hipóteses de requisição direta fundados no art. 11 do Marco Civil da Internet e no art. 18 da Convenção de Budapeste.

Ao contrário, entendo que as referidas hipóteses de requisição reafirmam os princípios da soberania e da independência nacional (art. 1º, I e art. 4º, I da CF/88), concretizando o dever do Estado de proteger os direitos fundamentais e a segurança pública dos cidadãos brasileiros ou residentes no país (art. 5º e 144 da CF/88).

Destaque-se que a solução aqui preconizada vem sendo adotada por diversos países ao redor do mundo. Nessa linha, Estados Unidos, Austrália, Canadá, Dinamarca, França, Espanha e Irlanda possuem regras que possibilitam às autoridades nacionais o acesso a dados em nuvem mantidos no exterior, desde que preenchidos os critérios da atividade e

do controle de dados anteriormente exposto (MAXWELL, Winston; WOLF, Christopher. "A Global Reality: Governamental Acess to Data in the Cloud – a comparative analysis of ten international jurisdictions". **Hogan Lovells White Paper**. 23 mai. 2012).

Ressalte-se ainda que os recentes tratados e acordos internacionais relativos ao tema, como a Convenção de Budapeste, já incorporada pelo Brasil, e o *Clarifyng Lawful Overseas Use of Data Act* (Cloud Act), disponível para adesão por parte das autoridades brasileiras, são capazes de afastar inúmeros questionamentos suscitados pela parte requerente, como a possível violação à legislação estrangeira ou os riscos de imposição de sanções legais no exterior em virtude do uso ou da não proteção dos dados dos indivíduos.

Isso porque tais instrumentos têm estabelecido uma base comum para a proteção e a solicitação de dados pessoais que afastam a ocorrência de conflitos com base nas leis internas de cada um dos países signatários ou acordantes, tal como será melhor explicitado no tópico seguinte.

Aliás, é importante destacar que existem políticas e termos de serviços bastante diversos por parte das empresas de tecnologia em relação ao atendimento às solicitações das autoridades judiciais.

Nessa linha, há empresas que adotam uma postura mais colaborativa e que inclusive já se adequaram à necessidade de fornecimento de dados e comunicações eletrônicas.

Destaco, por exemplo, o depoimento apresentado pelo representante da Verizon Brasil na sustentação oral realizada na data de ontem, Dr. André Zonaro Ciacchetta, quando aduz que *"O Yahoo já se adaptou e possui uma estrutura que propicia o atendimento às ordens judiciais aqui proferidas, entretanto existem hipóteses nas quais ou o serviço é prestado por uma empresa estrangeira ou o usuário ao qual se refere a quebra de sigilo ou o fornecimento de conteúdo não guardam ponto de conexão com o território brasileiro"*.

Pelo que se observa, essa política é significativamente distinta da postura adotada por outras empresas, que sustentam de forma genérica e aplicável a todos os casos a impossibilidade de fornecimento de dados relativos a comunicações ocorridas em território nacional, praticadas por

cidadãos brasileiros, com base em uma possível violação à legislação de outros países.

O que a legislação interna e os acordos internacionais têm buscado é impedir esse tipo de alegação descontextualizada, com a facilitação no fornecimento desses dados e a exigência de um maior ônus na indicação das hipóteses de possível ocorrência desses conflitos.

Destarte, com base em todos esses motivos, concluo pela constitucionalidade dos dispositivos do MLAT, do CPC e do CPP que tratam da cooperação jurídica internacional e da emissão de cartas rogatórias, em especial nos casos em que a atividade de comunicação ou a prestação de tais serviços não tenham ocorrido em território nacional, **sem prejuízo da aplicação específica do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste para a solicitação de dados, registros e comunicações eletrônicas relativos a atos praticados no país.**

Isso significa que, fora das hipóteses do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste, que tratam de atividades e serviços prestados em território nacional, o único instrumento cabível é o da cooperação previsto pelo tratado bilateral e pelas regras das cartas rogatórias.

Não por último, teço, no ponto, breve observação, atento à tese vocalizada nos autos quanto à possibilidade de eventuais abusos cometidos na requisição direta por parte das autoridades nacionais. Ora, casos que tais poderão e deverão ser controlados por esta Corte e por outras instâncias judiciais sob o enfoque do princípio da proporcionalidade na sua perspectiva *in concreto* – que é a mais adequada para situações em que a fórmula legislativa não contém uma valoração de todos os aspectos e circunstâncias que compõem cada hipótese de aplicação (JAKOBS, Michael. **Der Grundsatz der Verhältnismässigkeit**. Colônia: Carl Heymanns, 1985, p. 150). Perspectiva não propriamente inédita para este Tribunal, consoante testemunham as considerações do Eminente Min. Sepúlveda Pertence na **ADI 223**, ajuizada em face da Medida Provisória 173/1990, que vedava a concessão de provimentos

liminares contra dispositivos que estruturavam o "Plano Collor", dentre vários outros casos.

Contudo, ressalto mais uma vez que tais discussões não constituem objeto da presente ação, mas sim da **ADI 5.527**, (de Relatoria da Eminente Presidente, Ministra Rosa Weber) **e da ADPF 403** (de Relatoria do Eminente Ministro Edson Fachin), no qual o Tribunal certamente dará uma solução adequada para coibir abusos decorrentes de atos estatais e de decisões judiciais desproporcionais.

V - Da necessidade de reforço dos quadros institucionais de cooperação internacional para o combate a crimes cibernéticos

Antes de concluir o presente voto, é ainda necessário ressaltar que o caso em tela demonstra que seria bastante inócuo e até mesmo ingênuo que o exercício da jurisdição constitucional se desse de forma isolada em relação ao quadro institucional que hoje se desenvolve no âmbito transnacional no tocante ao compartilhamento de evidências criminais digitais.

Essa ressalva é importante para que se compreenda que os limites da jurisdição constitucional em casos como este são ainda mais sensíveis. É que de pouco importaria se esse STF julgasse constitucional ou inconstitucional os dispositivos do MLAT, do CPC, do CPP ou do Marco Civil da Internet, sem considerar a intrincada rede de leis estrangeirais tratados internacionais que dispõem sobre o tema.

Como tive a oportunidade de discutir em recente artigo acadêmico, já mencionado neste voto, o fenômeno do chamado "**Constitucionalismo Digital**" requer que se compreenda que a internet faz nublar uma das premissas estruturantes do constitucionalismo que é a adesão da jurisdição constitucional aos limites nacionais. Nesse sentido, destacamos que:

> "Há poucas áreas da jurisdição constitucional que são mais afetadas pelo movimento de transnacionalização do que a adjudicação de direitos fundamentais na internet. Desde as

primeiras discussões teóricas sobre a regulabilidade do ciberespaço, já se presumia inicialmente que a coexistência de regimes jurídicos nacionais ensejaria competições entre sistemas normativos.

Com o avanço da literatura sobre a governança da internet, esse diagnóstico tornou-se mais sofisticado, compreendendo-se que o papel dos Estados-Nacionais é redefinido não apenas por uma disputa entre as formas tradicionais de regulação nacional, mas por uma verdadeira reorganização das forças de poder na rede em decorrência da atribuição de funções públicas a entidades não governamentais e a importantes atores privados.

Esse rearranjo do poder político entre governos, instituições internacionais e fóruns *multistakeholders* revela que o modelo de governança da internet se afasta da predominância de uma autoridade central hierárquica qual ocorre dentro dos Estados Nacionais e se caracteriza, mais precisamente, pela formação de redes multilaterais em que atores independentes e operacionalmente autônomos se articulam reciprocamente.

(...) A discussão colocada na ADC 51 mais uma vez respalda a necessidade de construção de pontes de diálogo entre a teoria do constitucionalismo digital e a jurisdição constitucional. Enquadrar essa discussão como uma simples análise *in abstracto* da compatibilidade dos acordos de cooperação mútua previstos no Decreto Executivo Federal nº 3.810, de 2 de maio de 2001 com a literalidade do texto constitucional certamente não seria suficiente para resolver os embates judiciais sobre o tema. Na linha do que demonstrou a própria Audiência Pública realizada pelo STF, o cerne da discussão constitucional consiste em saber como compatibilizar a efetividade do nosso sistema de persecução criminal com o respeito à soberania dos estados estrangeiros e a proteção da privacidade dos usuários a nível global.

De forma mais profunda, o que se deve investigar é como o critério que tradicionalmente define os limites da jurisdição constitucional – a territorialidade – pode ou não ser

> compatibilizado com a sobreposição de regimes jurídicos estrangeiros que servem de base para o desenvolvimento de atividades econômicos e sociais para além das fronteiras nacionais. A resposta a esse questionamento invariavelmente perpassa a compreensão de princípios estruturantes do constitucionalismo digital, em especial dos valores atrelados à ideia de governança da internet e dos embates sobre estratégias de re-territorialização e fragmentação da rede." (MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. "Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro". **Revista Brasileira de Direito**, Passo Fundo, v. 16, n. 1, out. 2020, pp. 20-21; 26-27)

Faço aqui essas observações teóricas para acentuar que, a rigor, a decisão que este STF tomar sobre a matéria não irá resolver de forma definitiva os debates sobre a legitimidade da jurisdição brasileira nos casos de compartilhamento transnacional de dados, ainda mais diante do cenário de aumento exponencial de crimes cibernéticos, que cresceram no patamar de 300% apenas durante o período da pandemia do Covid-19 no Brasil (ROLFINI, Fabiana. **Cibercrime: ataques no Brasil aumentam mais de 300% com a pandemia**, 3jul. 2020. Disponível em: <https://olhardigital.com.br/2020/07/03/seguranca/cibercrime-ataques-no-brasil-aumentam-mais-de-300-com-a-pandemia>).

Por isso, é de fato indispensável que o Poder Legislativo e o Poder Executivo adotem as medidas necessárias para o **aperfeiçoamento do quadro legislativo**, com a análise de novos modelos de tratados multilaterais ou de acordos executivos que possibilitam a obtenção de dados eletrônicos com mais segurança jurídica e agilidade, evitando os riscos de colisão entre ordenamentos jurídicos e simplificando o marco regulatório aplicável às relações entre os Estados e as empresas de tecnologia.

Para além da adesão à Convenção de Budapeste que deve ser exaltada enquanto importante iniciativa do Estado brasileiro, é possível citar, a título de exemplo, o *Clarifying Lawful Overseas Use of Data Act*, o

chamado CLOUD Act, nos Estados Unidos, bem como as propostas de negociações do *e-Evidence Regulation*, também na União Europeia.

Em todos esses diplomas normativos, um dos requisitos essenciais para a habilitação dos países é a existência de leis adequadas sobre cibercrimes e provas eletrônicas, **o que reforça a necessidade de aprovação de uma Lei Geral de Proteção de Dados para Fins Penais (LGPD Penal)**, cujo anteprojeto já se encontra em tramitação na Câmara dos Deputados (VERONESE, Alexandre; CALABRICH, Bruno. **Crimes na internet e o Brasil no cenário da cooperação jurídica internacional.** Portal Jota. 24.4.2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/judiciario-e-sociedade/crimes-na-internet-e-o-brasil-no-cenario-de-cooperacao-juridica-internacional-24042021>).

Ao tratar da importância desses novos marcos regulatórios, Alexandre Veronese e Bruno Calabrich apontam que:

> "existe uma necessidade imperativa de aprovação não apenas de uma Lei de Proteção de Dados Pessoais e Privacidade na Segurança Pública e na Investigação e Repressão Criminal; mas, também, de uma legislação-quadro que determine parâmetros, em sintonia com a Convenção de Budapeste e com a legislação da UE, para a realização de acordos de cooperação. Ainda, uma parte muito importante nessas duas leis – proteção de dados pessoais e meios de cooperação – se refere à previsão de um sistema de supervisão que seja eficiente, autônomo e transparente. É somente por meio da atenção a esses três elementos que será possível inserir – de forma responsável e segura – o Brasil em meios de investigação e de repressão criminal compatíveis com a era digital."

Ainda de acordo com os autores, é possível vislumbrar um cenário de aumento quantitativo e coordenado dos mecanismos de cooperação, ao invés de se restringir essas atividades a um único instrumento jurídico, tal como pretendido nesta ação (VERONESE, Alexandre; CALABRICH, Bruno. **Crimes na internet e o Brasil no cenário da cooperação jurídica internacional.** Portal Jota. 24.4.2021. Disponível em:

<https://www.jota.info/opiniao-e-analise/colunas/judiciario-e-sociedade/crimes-na-internet-e-o-brasil-no-cenario-de-cooperacao-juridica-internacional-24042021>).

Destaque-se que os quadro legais dos tratados multilaterais e dos acordos executivos parecem caminhar para uma situação intermediária em que as jurisdições nacionais mantenham o poder de requisição direta dos dados, mas compartilhem com os países estrangeiros regras de cooperação jurisdicional claras para a proteção da privacidade e de outros direitos digitais envolvidos (DASKAL, Jennifer. "Privacy and Security Across Borders". In: **Yale Law Journal Forum**, v. 1029, p. 1–16, 2019, p. 1029).

Nesse sentido, o CLOUD Act, por exemplo, prevê como regra geral que os provedores de internet devem cumprir os mandados judiciais de requisição de dados ainda que estes estejam armazenados fora dos EUA. Contudo, a legislação também prevê duas exceções que permitiriam o afastamento da ordem judicial: (*i*) quando o provedor tiver elementos suficientes para presumir que o usuário do serviço cujos dados devem ser fornecidos não é um cidadão norte-americano ou não reside nos EUA e (*ii*) quando a divulgação dos dados puder ensejar uma violação das leis de país estrangeiro. A legislação também permite que estados estrangeiros requeriam o acesso a dados diretamente das empresas situadas nos EUA, sendo necessário para isso o estabelecimento de acordos executivos entre o governo norte-americano e o governo solicitante.

Desta feita, embora se conclua pela constitucionalidade dos **modelos complementares** do MLAT e da requisição direta, com base no art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste, não se deve ignorar que há a possibilidade de aperfeiçoamento desse quadro, com a celebração de outros tratados e acordos que possibilitem a obtenção a dados eletrônicos com maior agilidade e segurança.

Portanto, embora conclua-se pela constitucionalidade do modelo do MLAT, em complementação com as hipóteses de requisição direta, o aperfeiçoamento dos instrumentos de cooperação poderá levar a uma

situação de aprimoramento e de melhoria do procedimento de requisição e obtenção de dados eletrônicos transnacionais.

Com base nessa situação, entendo que esta Corte deve comunicar o teor deste acórdão aos Poderes Legislativo e Executivo, como forma de se instaurar um diálogo que possa levar à adesão a outros tratados e acordos internacionais, para além da Convenção de Budapeste, como, por exemplo, a assinatura de acordos bilaterais com base no CLOUD Act.

VI – Conclusão

Ante o exposto, conheço da ADC e voto para julgar **parcialmente procedente** o pedido formulado à inicial para declarar a constitucionalidade dos dispositivos indicados, sem prejuízo da possibilidade de solicitação direta de dados e comunicações eletrônicas das autoridades nacionais a empresas de tecnologia nas específicas hipóteses do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste, ou seja, nos casos de atividades de coleta e tratamento de dados no país, de posse ou controle dos dados por empresa com representação no Brasil e de crimes cometidos por indivíduos localizados em território nacional.

Voto, outrossim, para que o Tribunal faça a comunicação desta decisão ao **Poder Legislativo e o Poder Executivo,** para que adotem as providências necessárias ao aperfeiçoamento do quadro legislativo, com a discussão e a aprovação do projeto da Lei Geral de Proteção de Dados para Fins Penais (LGPD Penal) e de novos acordos bilaterais ou multilaterais para a obtenção de dados e comunicações eletrônicas, como, por exemplo, a celebração do Acordo Executivo definido a partir do *Cloud Act*.

É como voto.