Nota Técnica

A presente Nota Técnica é apresentada pelo Grupo de Apoio ao Enfrentamento dos Crimes Cibernéticos da 2ª. Câmara de Coordenação e Revisão com o fim de subsidiar manifestação do Ministério Público Federal antes da apreciação de pedido de medida cautelar formulado na Ação Declaratória de Constitucionalidade que a Federação das Associações das Empresas de Tecnologia da Informação – ASSESPRO NACIONAL – ajuizou perante o Supremo Tribunal Federal com pedido subsidiário de recebimento como Arguição de Descumprimento de Preceito Fundamental, ação na qual requereu e obteve sua admissão como *Amicus Curiae* a empresa *Facebook Online do Brasil Ltda*..

O pedido principal da ação versa sobre a declaração de constitucionalidade do Decreto Executivo Federal nº 3810/2001, bem como do artigo 237, II, do Código de Processo Civil, e dos artigos 780 e 783 do Código de Processo Penal, vindo alegar que decisões judiciais brasileiras, no bojo de investigações e ações criminais brasileiras, têm implicitamente reputado tais dispositivos inconstitucionais pela sua não utilização quando da requisição direta de dados de comunicação privada sob controle de provedores de aplicativos e Internet que tenham o exterior como sede controladora desses dados.

Assim, a autora alega que a não utilização do tratado de mútua assistência em matéria penal – *Mutual Legal Assistance Treaty - MLAT* – com os Estados Unidos da América e a não utilização de cartas rogatórias para a obtenção do conteúdo de tais comunicações indicaria o reconhecimento da inconstitucionalidade dos mencionados dispositivos.

Tal se daria porque com o fim de se obter esses dados, as decisões judiciais mencionadas na Ação determinam a entrega dos itens diretamente pelas empresas prestadoras do serviço de Internet no Brasil mediante a intimação de suas filiais com endereço em solo brasileiro e aqui constituídas sob as leis brasileiras.

A autora alega que os provedores de aplicativos de Internet estabelecidos no exterior, os quais também representa, estão sob a jurisdição do país onde se localiza a sede que controla os dados, de forma que as filiais brasileiras não poderiam ser responsabilizadas por não cumprirem ordens judiciais brasileiras, ainda que os dados buscados tenham sido coletados no Brasil, durante operação e prestação de serviços da empresa no Brasil, serviço este voltado especificamente, ainda que não unicamente, a usuários brasileiros.

A argumentação trazida pela inicial baseia-se em premissas equivocadas e contraria a legislação pátria frontalmente. Conforme se explanará detalhadamente a seguir, (**i**) a regra geral de jurisdição trazida pelo artigo 21 do Código de Processo Civil determina que o Poder Judiciário brasileiro tem jurisdição sobre empresas brasileiras e também sobre empresas estrangeiras que aqui possuam agência, filial ou sucursal; (**ii**) a norma específica do artigo 11 do Marco Civil da Internet determina a aplicação da legislação brasileira quando do oferecimento de serviços através da internet a usuários brasileiros, ainda que a empresa aqui não possua sede, agência ou filial; (**iii**) a legislação internacional reconhece essa mesma regra de jurisdição, não havendo conflito em sua aplicação; (**iv**) e não há controvérsia a ser sanada porque as decisões apontadas como inconstitucionais em verdade aplicam corretamente a legislação pátria e representam uniformização de jurisprudência feita pelo Egrégio Superior Tribunal de Justiça.

1. <u>Internet e Jurisdição</u>

1.1. Critérios de Definição de Jurisdição sobre Provas Eletrônicas e Dados Coletados no Provimento de Conexão e de Aplicativos na Internet

O princípio da territorialidade é há longa data objeto de estudo do direito internacional traduzindo-se, tradicionalmente, na forma mais simples e eficaz de definir jurisdição: o Estado pode exercer jurisdição sobre todos os bens, pessoas (físicas e jurídicas) que se encontram em seu território. Assim, sendo o Estado soberano em seu território, terá ele o poder de legislar, julgar e executar seus julgamentos dentro desse território, tendo acesso, dentro de regras previamente definidas, a todos os meios de prova fisicamente localizados em seu território. Por outro lado, quando necessitar de provas ou elementos localizados fisicamente no território de outro Estado soberano, poderá o país interessado buscar auxílio por meio de mecanismos de cooperação internacional.

Entretanto, em um mundo globalizado e conectado à Internet, cada vez mais dependente de dados e provas eletrônicas, o princípio da territorialidade passou a refletir diferentes facetas e a ser adotado em conjugação com outros critérios. Primeiro, porque enquanto a localização física de provas documentais está tradicionalmente ligada ao ato que elas demonstram, provas eletrônicas podem ser armazenadas em um lugar, mas referir-se a ato ocorrido em outro, sem nenhuma conexão com o território de armazenagem. Segundo

porque provas eletrônicas, sejam elas documentos ou dados de conexão, podem ser armazenadas em qualquer local e podem ser movidas com simples comandos eletrônicos, sendo absolutamente inútil, pois mutável em questão de segundos, a definição do local de armazenamento físico dos dados buscados[1].

Justamente por essas razões, 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.

Esses dois critérios, em substituição ao critério ordinário da pura localização física das provas, têm sido amplamente reconhecidos na legislação de diversos países como norteadores de fixação de jurisdição para a obtenção de provas eletrônicas, permitindo que os Estados tenham acesso direto a provas e dados coletados em seus territórios, ainda que

[1]Em alguns casos, quando utilizado o sistema de *Content Delivery Network* não é sequer possível determinar o local físico exato onde os dados estão armazenados, pois eles são parcialmente guardados em diferentes datacenters e podem ser realocados a qualquer momento, dependendo da disponibilidade da rede (https://cloud.google.com/cdn/?hl=pt-br).

por empresas estrangeiras. Nesse sentido é a *Guidance Note #10*[2], emitida pelo Comitê da Convenção sobre Cibercriminalidade (*Cybercrime Convention Committee – T-CY*)[3], que se encontra periodicamente para debater a implementação da Convenção, nos termos de seu artigo 46. Referida nota reforça o entendimento de que os países podem ter acesso direto a dados coletados por empresas localizadas em seus territórios, independentemente da localização física efetiva da prova, e também a dados coletados por empresas que prestam serviços em seu território, mesmo que a empresa ali não possua sede ou filial.

A legislação interna de vários países signatários da Convenção de Budapeste segue no mesmo sentido, reconhecendo a jurisdição de suas autoridades judiciárias sobre as provas coletadas por empresas sediadas ou que prestam serviços em seus territórios[4]. Essa mesma solução foi adotada pela legislação brasileira.

---

[2]O original, em inglês, pode ser acessado em https://rm.coe.int/16806f943e. A nota foi adotada em 27 de fevereiro de 2017.

[3]A Convenção sobre Cibercriminalidade do Conselho da Europa (CETS nº 185 - Convenção de Budapeste), ratificada por mais de trinta países, é hoje o único instrumento internacional sobre cibercriminalidade e provas eletrônicas, abrangendo, também o acesso direto, por autoridades judiciárias durante investigações criminais, a provas eletrônicas armazenadas fisicamente no território de outros países, nos termos de seu artigo 18: *In verbis*:

"***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.*
2. *Os poderes e procedimentos referidos no presente artigo devem estar sujeitos aos artigos 14º. e 15º.*
3. *Para os fins do presente artigo, a expressão "dados relativos aos assinantes" designa qualquer informação, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida por um fornecedor de serviços e que diga respeito aos assinantes dos seus serviços, diferentes dos dados relativos ao tráfego ou ao conteúdo e que permitam determinar:*
   a. *O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;*
   b. *A identidade, a morada postal ou geográfica e o número de telefone do assinante e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços;*
   c. *Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços*".

[4]Austrália, Espanha e Canadá permitem que órgãos de investigação requisitem de empresas localizadas em seus territórios informações, independente do local de armazenamento. Dinamarca, França e Reino Unido trazem dispositivos semelhantes, com um requisito a mais, permitindo a requisição e o acesso direto quando os dados estão sobre o controle de empresa local *e* podem ser acessados de seus territórios (Maxwell, Winston/Wolf, Christopher (2012): *A Global Reality: Governmental Access to Data in the Cloud* (Hogan Lovells White Paper, 23 May 2012. O documento original, em inglês, pode ser acessado em

1.2. **A Legislação Brasileira**

Embora o Brasil não seja ainda signatário da Convenção de Budapeste, quando da elaboração da Lei nº. 12.965/2014 (Marco Civil da Internet), o Legislador brasileiro, sabiamente, teve em mente as peculiaridades das provas eletrônicas e da coleta de dados no exercício de atividades de provimento de acesso à Internet e de aplicativos na rede, estabelecendo no artigo 11 do diploma legal o arcabouço necessário para determinar a aplicação da legislação brasileira e da jurisdição nacional para assegurar não apenas o acesso aos dados coletados em território nacional, mas principalmente o respeito aos direitos dos usuários. Determina o citado artigo, verdadeira regra de jurisdição, que:

> "*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***

---

https://www.hoganlovells.com/~/media/hogan-lovells/pdf/publication/revised-government-access-to-cloud-data-paper-18-july-12_pdf.pdf).

Decisões proferidas por Tribunais Superiores de diversos países também sustentam esse entendimento, sendo possível citar decisões da Suprema Corte da Bélgica (https://www.wsgr.com/attorneys/BIOS/PDFs/burton-yahoo-0411.pdf) e da Suprema Corte do Canadá (no endereço https://www.canlii.org/en/bc/bcsc/doc/2014/2014bcsc1063/2014bcsc1063.html é possível encontrar a decisão original da Suprema Corte de British Columbia exarada por Madam Justice Fenlon. A empresa Google Inc. foi vencida e recorreu para a Corte de Apelação de British Columbia (BCCA) que decidiu também contrariamente à Google, disponível em http://www.courts.gov.bc.ca/jdb-txt/CA/15/02/2015BCCA0265.htm. Essa decisão foi então objeto de recurso para a Suprema Corte do Canadá (SCC) que confirmou a jurisdição do juízo de British Colômbia em 28/06/2107, disponível em https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do).

mesmo grupo econômico possua estabelecimento no Brasil" (destaque nosso).

Do quanto exposto, resta claro que a lei brasileira adotou tanto o critério da nacionalidade da empresa (ao menos uma integrante do mesmo grupo econômicos possua estabelecimento no Brasil) quanto o critério dos efeitos do serviço (oferta do serviço ao público brasileiro), aliados ao critério territorial (ao menos um terminal localizado em território nacional), para a determinação da jurisdição brasileira. Deverá ser aplicada a lei brasileira, incluindo aí as regras para coleta de provas e de definição de jurisdição, desde que haja *oferta* de serviço no Brasil **ou** que a empresa, ou ao menos um integrante do grupo econômico, *possua estabelecimento no Brasil*.

Apesar da clareza do dispositivo legal, argumenta a inicial, para afirmar que as autoridades judiciárias brasileiras não possuem jurisdição sobre empresas de Internet sediadas no exterior, mesmo quando ofertando serviços no Brasil e com filiais constituídas em território nacional e sob as leis brasileiras, que o parágrafo único do artigo 3º do Marco Civil da Internet determina que as regras nela expostas não excluem outros dispositivos do ordenamento jurídico nacional e nem de tratados internacionais, incluídos aí os dispositivos sobre cartas rogatórias e pedidos de cooperação internacional. Assim, depreende-se que no seu entendimento, o artigo 11 somente seria aplicável em parte, para a preservação do sigilo, pois para a obtenção de dados deveria ser seguido o (penoso) processo de cooperação internacional descrito. Há três equívocos claros nessa interpretação.

O primeiro deles é que uma regra geral como a do citado parágrafo único do artigo 3º., que reconhece o ordenamento jurídico como um todo e a necessidade de se harmonizar dispositivos, seria suficiente para suplantar previsão específica contida no artigo 11. A regra geral em nada destoa de outras encontradas em diversos diplomas legais pátrios que admitem a aplicação analógica para suprir eventuais lacunas pontuais, mas nem por isso entende-se que a analogia e o respeito a outras regras gerais possam suplantar previsões específicas.

O Código de Processo Penal, por exemplo, admite expressamente a aplicação analógica de regras de processo civil, entretanto, por óbvio, as regras específicas referentes à citação no processo criminal não poderão ser substituídas pelas regras do processo civil.

O mesmo ocorre aqui: a regra específica de jurisdição trazida pelo artigo 11, que prevê a aplicação da lei brasileira, tanto material quanto processual, para a obtenção de

dados e comunicações, não pode ser suprimida pela aplicação de regra geral de cooperação, que somente incide quando as autoridades brasileiras *não possuem* jurisdição sobre a prova a ser coletada.

O segundo equívoco é impor limites à regra de jurisdição trazida pelo artigo 11 quando esses limites não estão expressos na norma. O dispositivo estabelece de forma bastante incisiva que a *legislação brasileira deverá ser respeitada* quando uma das atividades nele descritas ocorrer em território nacional. A legislação brasileira, por óbvio, inclui não apenas as regras de proteção de dados, mas também, e principalmente, as regras que definem jurisdição e a *forma* como os dados podem ser obtidos. De nada adiantaria o Marco Civil da Internet estabelecer que os dados são privados, sem determinar, como o faz nos artigos 10 e 13, que eles somente poderão ser obtidos por meio de ordem judicial. A proteção se completa com a restrição na coleta da prova, motivo pelo qual não é possível, sob pena de desvirtuar-se o arcabouço desenvolvido pelo legislador, dividir-se a proteção legal para fazer incidir a lei brasileira apenas quanto à guarda dos dados, mas não quanto à forma de obtenção desses mesmos dados. A *legislação brasileira* mencionada no dispositivo é uma só e inclui também a forma de obtenção dos dados coletados disciplinada especificamente nos artigos acima mencionados.

E nem se argumente que a *forma* de obtenção dos dados, neste caso, é através de pedido de cooperação internacional. Tal somente ocorreria, frise-se novamente, se o Poder Judiciário brasileiro não tivesse jurisdição sobre a prova. Entretanto, além do já citado § 2º do artigo 11, também o artigo 21 do Código de Processo Civil reconhece, expressamente, que o Brasil possui jurisdição para causas envolvendo empresas que aqui possuam "*agência, filial ou sucursal*", exatamente a situação dos casos citados na inicial. Esse artigo, regra geral de determinação de competência e jurisdição, também é a "*legislação brasileira*" citada pelo artigo 11 do Marco Civil.

Há ainda um terceiro ponto que põe em cheque toda a argumentação apresentada: a inicial demanda a aplicação do citado artigo 3º e das regras legais que regem os pedidos de cooperação internacional apenas e tão somente para as hipóteses de conteúdo de comunicações. Para todas as demais requisições, os pedidos feitos diretamente para a filial brasileira seriam válidos e aceitos. Ora, tem-se assim a seguinte situação: o Juízo brasileiro tem jurisdição sobre a filial brasileira e esta tem plenas condições técnicas de fornecer os dados requisitados, mas apenas quando a matriz entender conveniente. Nas demais

situações, o Juízo deixa de ter jurisdição e a filial deixa de ter condições técnicas de atender às requisições.

Trata-se, evidentemente, de aspecto ilógico da inicial. Como exposto, não há como se defender a existência de "meia jurisdição", apenas quando a matriz estrangeira de empresa brasileira entender cabível. Ou o Juízo brasileiro possui jurisdição, conforme determinado pelos artigos 21 do Código de Processo Civil e 11 do Marco Civil da Internet, ou não tem jurisdição e, nesse caso, toda e qualquer requisição deveria ser feita por meio de pedido de cooperação. O alardeado cumprimento, pelo *Facebook Brasil*, de centenas de requisições judiciais de dados demonstra claramente que a empresa reconhece a jurisdição das autoridades brasileiras e tem condições técnicas de cumprir as ordens delas emanadas.

De todo o exposto, resta evidente que, segundo a legislação brasileira, a autoridade judiciária brasileira tem jurisdição e pode exigir a entrega direta de provas eletrônicas, incluídas aí comunicações, desde que (**i**) o ato de coleta desses dados ou comunicações tenha ocorrido, ainda que parcialmente, em território nacional, mesmo que realizado por empresa estrangeira desde que (**ii**) esta oferte o serviço no Brasil **ou** (**ii**) possua ao menos uma integrante do grupo econômico estabelecida no Brasil, não necessariamente a sede. Nenhuma das decisões mencionadas na inicial deixou de cumprir o quanto determinado nesta regra.

1.3. Da Legislação Estadunidense e Dos Riscos do Conceito de Jurisdição Parcial Defendido na Ação

Como exposto e conforme reconhecido pela legislação internacional, o critério territorial aplicado somente para o local da guarda dos dados não se presta a definir jurisdição em matéria de provas eletrônicas. Entretanto, a inicial peca ao afirmar que a legislação estadunidense reconhece apenas o critério de controle para a fixação de jurisdição e que qualquer outra posição violaria a soberania daquele país. Trata-se, em verdade, de posicionamento que atende aos interesses de uma **única** empresa, não por acaso aquela que ingressa na presente ação como *Amicus Curiae* e que abertamente procurou a autora solicitando a propositura da presente ação[5].

[5]Conforme item 18 da Ata juntada no item 4 da documentação que acompanha a inicial, a propositura da presente ação foi de iniciativa da empresa *Facebook Online do Brasil Ltda.*, que, carente de legitimidade, procurou a autora solicitando o ingresso da demanda. A autora, na reunião minutada na referida ata, aprovou

A legislação norte-americana sobre armazenamento de provas eletrônicas, codificada no 18 US Code, capítulo 121 (§§ 2701 a 2712), prevê três níveis de proteção para dados eletrônicos. O primeiro deles refere-se a dados cadastrais, incluindo-se aí *logs* de acesso e conexão (números de *Internet Protocol – IP* utilizados para acessar a rede e aplicativos nela oferecidos), que podem ser voluntariamente apresentados pelas empresas às autoridades policiais e judiciais; o segundo refere-se a metadados, incluindo-se aí todos os demais dados de conexão que não se traduzem como dados cadastrais, e que somente podem ser requisitados pelas autoridades mediante ordem judicial; e as comunicações via eletrônica, que dependem de mandados de busca e apreensão, com critérios mais restritos para deferimento.

De forma bastante simplista, os dispositivos legais acima citados permitem que as empresas *estadunidenses* forneçam dados cadastrais e de conexão, aqui incluídos os chamados metadados, voluntariamente a autoridades estrangeiras[6], mas não autoriza o fornecimento de conteúdo de comunicações privadas[7]. Assim, argumenta a inicial, de forma um tanto quanto confusa quando não se compreende o contexto e os interesses que motivam tal argumentação, que as autoridades brasileiras teriam apenas "meia jurisdição", isto é, para a obtenção de dados e metadados, poderiam expedir requisições diretas às empresas brasileiras com matriz no exterior, mas para o conteúdo de comunicações, as mesmas regras definidoras de jurisdição não se aplicariam, e seria necessário pedido formal de cooperação internacional, ainda que a ordem fosse dirigida a empresa brasileira, constituída conforme as leis brasileiras e prestando serviços a brasileiros em território nacional.

---

a iniciativa, condicionando-a ao ingresso do *Facebook* como uma de suas associadas, o que de fato foi feito. Toda essa movimentação torna evidente que a empresa, embora se apresente apenas como *Amicus Curiae*, é o real motor e a principal interessada na presente ação.

[6] O 18 US Code §2702 permite a entrega voluntária de dados cadastrais e metadados a entidades não definidas como "governo", tendo sido a interpretação das autoridades estadunidenses que a restrição encontrada neste dispositivo, bem como no §2703, somente se aplica ao governo norte-americano. Assim, as empresas estadunidenses estariam autorizadas a fornecer dados cadastrais e metadados a autoridades estrangeiras.

[7] A decisão proferida pela Suprema Corte Norte-Americana em *Katz v. United States* (1967, 389 U.S. 347), que estabeleceu o conceito de "*expectativa de privacidade*" determina que todo o conteúdo de comunicações, incluindo-se as eletrônicas, somente poderá ser acessado mediante a expedição de mandado de busca e apreensão, nos termos da Quarta Emenda constitucional estadunidense. Em princípio, a legislação estadunidense previa tratamento diferenciado para conteúdo de comunicações armazenadas há mais ou menos de 180 dias. Atualmente, porém, decisões judiciais têm entendido que essas diferenças não devem persistir, reconhecendo as proteções da Quarta Emenda, e a consequente necessidade de mandado de busca, para todo conteúdo (*United States v. Warshak*, 631 F. 3d 266, 288 – 6º Circuito, 2010 – íntegra em: https://www.eff.org/files/warshak_opinion_121410.pdf).

Caberia ao juiz, segundo esse raciocínio, conhecer profundamente a legislação de todos os países do mundo, e determinar, em cada caso concreto, se o pedido de dados direto conflitaria ou não com a legislação do local da sede controladora dos dados. Caso o magistrado não tivesse condições de fazer essa análise, os advogados privados da empresa poderiam fazer esse juízo, transferindo-se a eles, os advogados privados contratados pela sede controladora dos dados, a função de dizer a lei no caso concreto e determinar se o Juízo que emite a ordem possui ou não jurisdição sobre a prova requisitada.

A par do absurdo da submissão do Poder Judiciário ao entendimento de advogados de empresa privada, é certo que essa argumentação atípica decorre da necessidade que tem a autora de adequar sua argumentação aos interesses do *Facebook Brasil* e de sua controladora norte-americana, que aqui se apresenta como *Amicus*, mas que é a real motivadora da ação, e que é hoje a **única** empresa de tecnologia constituída sob as leis brasileira que se recusa sistematicamente a cumprir as ordens emanadas de autoridades brasileiras.

A principal interessada no desfecho da presente ação, *Facebook Brasil*, embora empresa brasileira aqui constituída sob leis brasileiras e prestando serviços a usuários brasileiros, entende-se impedida por legislação estrangeira a cumprir parte das ordens judiciais legais de autoridades brasileiras, buscando o alívio desta Ação como forma de adequar-se ao entendimento dos advogados estrangeiros de sua matriz. O entendimento da empresa é de que somente poderia fornecer dados de conexão e metadados, mas não conteúdo, daí o esforço argumentativo para reconhecer apenas a existência de jurisdição em parte: para alguns itens, mas não para outros.

Neste ponto, a Ação pretende criar um precedente gravíssimo. Ao flexibilizar o reconhecimento da jurisdição brasileira a apenas algumas hipóteses, determinadas conforme o entendimento dos advogados estrangeiros da empresa especialmente interessada em um julgamento positivo, corre-se o risco de ferir mortalmente a soberania brasileira e o Poder Judiciário Nacional. Acatada a argumentação, não caberá mais ao Poder Judiciário dizer o direito e definir, no caso concreto, se determinada prova pode ou não ser obtida diretamente. Caberá aos advogados estrangeiros de empresa privada definir, segundo os critérios próprios da empresa e sua interpretação da legislação do Estado que naquele momento ele entender como tendo jurisdição sobre si, definir se a autoridade judiciária poderá obtê-los diretamente ou terá de seguir o tortuoso caminho da cooperação internacional.

O risco de tal precedente pode ser visto de pronto quanto analisada a atual jurisprudência norte-americana sobre a definição de jurisdição em matéria de provas eletrônicas. A única decisão de Corte Regional sobre o assunto foi proferida no chamado caso Microsoft Irlanda pelo Corte Regional do 2o Circuito[8]. Essa decisão entendeu que a legislação norte-americana que rege a matéria não possui alcance extraterritorial e que, portanto, terá jurisdição sobre a prova o país em que está fisicamente armazenado o dado e não a sede de sua controladora, como argumenta a autora e a empresa que se apresenta como Amicus. Assim, tem-se que, hoje[9], a interpretação dada pelos advogados da empresa é contrária à jurisprudência do país sede da controladora[10], de onde se extrai com clareza os riscos e prejuízos aos quais estará submetido o Brasil ao deixar ao arbítrio de empresa privada a interpretação legal.

As regras legais não podem ser flexibilizadas conforme os interesses de empresa privada. Há, como exposto, normas claras na legislação brasileira definindo os critérios de fixação de jurisdição para provas eletrônicas, sejam meros dados de conexão, seja conteúdo de comunicações, não sendo possível, como pretende a autora, submeter o Poder Judiciário ao arbítrio e interpretação de empresas privadas, em especial quando esta gera distorções como as narradas acima.

2. <u>Da Ausência de Declaração Implícita de Inconstitucionalidade</u>

De todo o explanado até o momento, verifica-se que a controvérsia apontada na inicial simplesmente não existe. Nenhuma das decisões citadas como contrárias ao ordenamento jurídico, em grande maioria emanadas do Egrégio Superior Tribunal de Justiça, deixaram de aplicar a legislação pátria em sua inteireza ou reconheceram, de forma implícita, a inconstitucionalidade de qualquer preceito legal.

---

[8] A decisão original em inglês pode ser acessada em https://www.justice.gov/archives/opa/blog-entry/file/937006/download.

[9] O Caso *Microsoft Irlanda* atualmente pende de decisão pela Suprema Corte norte-americana, com a apresentação de argumentos orais em 27 de fevereiro de 2018.

[10] Observe-se que segundo informações da própria empresa, os dados de usuários brasileiros coletados pelo *Facebook* estão armazenados na Irlanda (em verdade, segundo informações constantes na documentação que instrui a inicial, o contrato de prestação de serviços de usuários brasileiros é firmado com o *Facebook* Irlanda e não com a matriz americana). Assim, conforme a interpretação atual da lei americana, eventual pedido de cooperação deveria ser dirigido àquele país e não aos Estados Unidos, como pretende a empresa autora.

A situação que se extrai dos dispositivos legais vigentes, todos eles e não somente aqueles citados na inicial, é a seguinte:

- Como regra geral, nos termos do artigo 21 do Código de Processo Civil, a autoridade judiciária brasileira tem jurisdição sobre pessoas jurídicas nacionais, aqui constituídas, bem como sobre pessoas jurídicas estrangeiras desde que aqui possuam "*agência, filial ou sucursal*";
- Como regra específica, para o caso de empresas provedoras de serviços através da Internet, sejam eles de conexão ou de aplicativos, o artigo 11 da Lei n^{o}. 12.965/2014 estabelece a necessária aplicação da legislação brasileira, com observância dos "*diretos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros*", tanto na preservação desses dados quanto no fornecimento deles mediante ordem judicial. A necessidade imperiosa de observância a essas regras incide não apenas para empresas brasileiras, como também para empresas estrangeiras que aqui ofertem serviços **ou** possuam ao menos um dos componentes de seu grupo econômico estabelecido no Brasil.
- Empresas que, como o *Facebook Brasil*, são constituídas sob a lei brasileira, ofertam serviços especialmente, ainda que não unicamente, voltados para brasileiros em território nacional e no oferecimento desses serviços coletam dados e comunicações, são obrigadas a cumprir a legislação nacional e a atender às requisições legais de autoridades brasileiras, que sobre elas possuem jurisdição.
- Os dispositivos que disciplinam o cumprimento de cartas rogatórias e de pedidos de cooperação internacional direta somente incidirão em outras hipóteses que não as mencionadas acima, isto é, quando as autoridades brasileiras, segundo a legislação nacional, não tiveram jurisdição. Isso ocorrerá, por exemplo, no caso de empresa que aqui não possui filial e nem presta serviços para usuários brasileiros[11].

Importante salientar neste ponto que a distinção laboriosamente apresentada no parecer do ilustre Professor Francisco Resek quanto às atividades da empresa matriz e da filial

[11]São inúmeros os exemplos de empresas de Internet estrangeiras que não possuem qualquer tipo de vínculo com o Brasil e não oferecem serviços direcionados a brasileiros. Em alguns casos, através da utilização de tecnologias que permitem a geolocalização do usuário com base no endereço de *IP* utilizado para conexão, o acesso aos serviços é bloqueado para usuários conectando a partir do Brasil. Nesses casos, resta evidente que as autoridades brasileiras não terão jurisdição sobre a empresa e os pedidos de cooperação internacional se farão necessários.

brasileira pouco importa para o deslinde da presente questão. O artigo 11 do Marco Civil da Internet, como exposto detalhadamente acima, determina a jurisdição brasileira desde que o *serviço seja prestado no Brasil* **ou** que uma *representante do grupo econômico* esteja em território nacional, sendo absolutamente desnecessário verificar qual a atividade da representante do grupo econômico e se esta tem acesso ou não aos dados coletados.

Entretanto, no caso das empresas de tecnologia em geral e do *Facebook Brasil* em particular, principal interessada no deslinde da causa, os grupos econômicos compartilham os dados coletados para o correto desenvolvimento de suas atividades, ao contrário do que alega a inicial. O grupo econômico *Facebook* oferece serviços em português, voltados especificamente para brasileiros em território nacional, e possui subsidiária no Brasil, ainda que escondida sob a fachada de mera empresa de marketing. Essa filial, responsável pela comercialização de espaços publicitários, recebe do grupo informações cruciais para o desenvolvimento de sua atividade, informações estas que são coletadas de usuários brasileiros. A estrutura de venda de anúncios do *Facebook* leva em consideração os interesses de cada usuário da plataforma traduzidos em páginas visitadas e "*curtidas*", dados esses coletados durante o provimento do serviço de acesso ao aplicativo. Assim, ainda que a empresa brasileira afirme que não é responsável pela coleta dos dados, é certo que, componente do mesmo grupo econômico, recebe esses dados para o exercício de suas atividades específicas, tudo a demonstrar que se trata, em verdade, de uma única atividade, desenvolvida em várias frentes interligadas. Resta evidente, assim, que a empresa brasileira é também responsável pelos dados e a eles têm acesso[12].

Necessário frisar novamente aqui um ponto que reforça a ligação entre a empresa brasileira e sua controladora: conforme amplamente documentado na inicial e nos demais documentos apresentados, o Facebook Brasil recebe as requisições judiciais de autoridades brasileiras e, salvo nos casos de conteúdo de comunicações, as atende sem maiores questionamentos. Ora, se de fato a empresa brasileira fosse completamente isolada na demais componentes do grupo, inclusive do Facebook Irlanda onde os dados estão efetivamente armazenados, não poderia ter acesso a nenhum deles. Tal situação demonstra

[12]Os serviços de publicidade oferecidos pelo *Facebook Brasil* podem ser acessados na página https://pt-br.facebook.com/business/help/714656935225188/?helpref=hc_fnav&bc[0]=AHCv1&bc[1]=Ads%20Help&bc[2]=Advertising%20Basics&bc[3]=About%20Facebook%20Advertising, a qual descreve detalhadamente os dados coletados dos usuários e que podem ser utilizados em anúncios direcionados.

que as reiteradas recusas em cumprir determinações judiciais não estão relacionadas a impedimentos de ordem técnica, mas a mera intransigência da empresa privada.

A análise dos dispositivos citados, e da forma de atuação das empresas de tecnologia acima descrita, deixa claro que as decisões mencionadas na inicial, que supostamente estariam reconhecendo implicitamente a inconstitucionalidade dos dispositivos relacionados ao cumprimento de cartas rogatórias e à aplicação de tratado de assistência mútua em matéria penal, em verdade apenas aplicam a lei brasileira. Elas reconhecem que o artigo 21 do Código de Processo Civil e o artigo 11 do Marco Civil da Internet 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. No caso da empresa que se apresenta como *Amicus*, a necessidade de respeito à legislação brasileira é ainda mais flagrante, pois ela presta serviços diretamente a usuários brasileiros em território nacional e, componente do mesmo grupo econômico, compartilha com ele as informações necessárias ao correto funcionamento da plataforma, inclusive aquelas para a venda de anúncios direcionados, e recebe das demais empresas do grupo os dados para o cumprimento de requisições judiciais.

Argumenta a autora, porém, que a situação aqui descrita, referente especificamente a comunicações eletrônicas e a dados colhidos durante o provimento de acesso à Internet e a seus aplicativos, é semelhante àquela verificada para obtenção de dados bancários, na qual não há questionamento sobre a necessidade de pedido de cooperação internacional quanto a dados retidos por empresa estrangeira com filial no Brasil.

A comparação é absolutamente equivocada por dois motivos.

Primeiro, porque para a obtenção de dados de conexão e de acesso à Internet, incluídas aí comunicações privadas, há regra específica na legislação brasileira, como exposto acima, baseada nos critérios de controle e efeitos da atividade, além do critério territorial.

Segundo, porque quando se utiliza de pedido de cooperação para a obtenção de dados bancários, busca-se documentos que comprovam transações ocorridas no exterior, referentes a serviço prestado em outro país. Não se admitiria, jamais, pedido de cooperação internacional para a obtenção de extratos bancários de conta referente a serviço prestado no Brasil, ainda que a matriz responsável fosse sediada no exterior e guardasse ali esses dados. O que diferencia de forma crucial as duas situações é o local e forma de prestação do serviço: no caso de empresas de tecnologia, o serviço é oferecido em português, a usuários brasileiros,

localizados no Brasil; no caso dos dados bancários citados na inicial, o serviço é oferecido no exterior, a usuários diversos, que podem ou não ser brasileiros. As situações nem de longe são similares, o que justifica o tratamento diferenciado dado pelos tribunais. Não há nenhuma controvérsia.

Ressalte-se, por fim, que a ausência de controvérsia também é verificada pela origem das decisões citadas pela inicial. As principais decisões que supostamente estariam reconhecendo implicitamente a inconstitucionalidade dos dispositivos questionados são oriundas do Egrégio Superior Tribunal de Justiça; as demais, que negam aplicabilidade ao artigo 11 do Marco Civil da Internet e ao artigo 21 do Código de Processo Civil, são oriundas de Tribunais de 2º Grau ou de juízos monocráticos de 1º Grau. Resta claro que a suposta "controvérsia" sobre os artigos a serem aplicados tem sido sistematicamente solucionada pela Corte Superior que, ao reconhecer as peculiaridades da prova eletrônica e as previsões específicas do Marco Civil da Internet, reafirma a jurisdição das autoridades brasileiras sobre dados colhidos em território nacional e afasta a necessidade de cooperação. Não há controvérsia e sim harmonização de entendimento pela Corte Superior constitucionalmente responsável.

3. **Da Ineficiência dos Instrumentos de Cooperação Internacional**

Após discorrer sobre jurisdição, afirma a inicial que estariam disponíveis às autoridades judiciárias brasileiras instrumentos perfeitamente eficazes e que garantiriam o cumprimento rápido e eficiente das ordens judiciais sem as supostas controvérsias apontadas, consubstanciados nas cartas rogatórias e nos pedidos de assistência mútua.

De início, cumpre salientar que o sistema de cooperação internacional não é, em condições normais, meio rápido de obtenção de provas. Em geral, os pedidos levam anos para serem atendidos, muitas vezes exigem diversas interações entre autoridades e, em regra, não se prestam à interceptação de fluxo de dados, incluindo aí comunicações.

No caso específico de provas eletrônicas, esse sistema é absolutamente ineficaz por três motivos.

Primeiro, porque os registros de conexão e acesso são guardados pelas empresas responsáveis por breve período de tempo, que varia de 90 (noventa) dias a 6 (seis) meses, tempo esse absolutamente insuficiente para a obtenção por vias diplomáticas tradicionais. Mesmo quando há pedido de preservação de dados, que pode ser feito rapidamente, quando

do retorno das informações serão necessários novos dados de conexão, a depender do que for inicialmente revelado, e esses dados, com a demora natural do procedimento, já estarão irremediavelmente perdidos.

Segundo porque os dados informáticos são móveis e, às vezes, sequer se conhece sua localização. A empresa controladora pode utilizar de tecnologia que roteia os dados em diferentes servidores, em diferentes locais do mundo, para otimizar sua prestação de serviços, sem poder precisar exatamente onde eles se encontram. Ela também pode armazená-los em alto-mar ou em locais que não atendem a requisições de autoridades estrangeiras. Mais do que isso, a empresa pode alterar a sede de sua controladora a qualquer momento, buscando a jurisdição que melhor lhe convier e sempre se eximindo de cumprir qualquer requisição legal. A natureza dos dados permite que a empresa que os controla, ciente da existência de pedido de cooperação, simplesmente altere sua sede, e o faça repetidas vezes, tornando inócua qualquer exigência.

Terceiro porque questões legais peculiares a determinados países podem simplesmente impedir a investigação de ofensas que são consideradas graves em outros. Utilize-se como exemplo a empresa que se apresenta como *Amicus* e que é responsável pela maior rede social do mundo: caso alguém, a partir do território brasileiro, utilize o *Facebook* especialmente ofertado para usuários brasileiros, para a prática de crime eleitoral em território nacional, o pedido de cooperação que vise a obtenção de conteúdo simplesmente será negado pelas autoridades norte-americanas[13], pois fatalmente a conduta estará protegida pela Primeira Emenda da Constituição estadunidense. Assim, a Justiça Eleitoral brasileira estará diante do seguinte dilema: crime foi praticado em território nacional, por pessoas localizadas no território nacional, através de serviço oferecido por empresa brasileira, mas a prova da infração não será obtida porque autoridades estrangeiras, que não têm absolutamente nenhum interesse na causa, estão impedidas de atender ao pedido de cooperação.

Justamente em razão de todos os problemas citados, mesmo as autoridades americanas têm reconhecido que o *MLAT* não é o instrumento adequado para a coleta de

[13]Utiliza-se aqui o exemplo das autoridades americanas apenas para fins de argumentação, aplicando-se o entendimento da empresa que, como exposto acima, não está de acordo com a jurisprudência atual estadunidense.

provas e dados eletrônicos e têm buscado ativamente formas de solucionar a questão[14], com interpretações que permitem o acesso direto às provas, defendidas enfaticamente no caso *Microsoft Irlanda*[15], e com a apresentação de proposta de mudança legislativa para incluir critério misto (territorial e de controle) na definição de jurisdição[16] .

Neste ponto, importante endereçar um outro argumento defendido na inicial, o de que a aplicação da regra legal trazida pelo artigo 11 do Marco Civil da Internet e o reconhecimento da jurisdição brasileira sobre serviços ofertados no Brasil, traria graves consequências no âmbito internacional, pois estar-se-ia buscando informações controladas por empresa estrangeira e forçando-a a cumprir as requisições mesmo quando estas forem contrárias à legislação do país onde sediada a matriz, o que geraria graves conflitos internacionais e seria contrária ao conceito de cortesia (*international comity*). Tal argumento não se sustenta.

O conceito de cortesia, ou *comity*, amplamente reconhecido pelas regras de Direito Internacional Público e de forma bastante sistematizado pela Suprema Corte Norte-Americana, estabelece que a aplicação da lei de um Estado deve ser limitada pela regra internacional da *razoabilidade*[17] e que *razoabilidade* deve ser avaliada levando em conta, dentre outros fatores, (**i**) a extensão da conexão entre a atividade realizada e o território de

---

[14]No último mês de dezembro, durante o *Internet Governance Forum 2017*, o representante do Departamento de Estado norte-americano, *Seth E. Bouveir*, assessor sênior para políticas de Internet, reconheceu as falhas do processo de cooperação através do *MLAT* para provas eletrônicas e dados de conexão, e a necessidade urgente de ajustes, inclusive com a ampliação das hipóteses de acesso direto na legislação norte-americana. Transcrição do quanto explanado por ser acessada em https://www.intgovforum.org/multilingual/content/igf-2017-day-3-room-xxv-ws149-criminal-jurisdiction-in-cyberspace-towards-solutions.
Essas mesmas falhas são reconhecidas expressamente pelo Departamento de Justiça norte-americano nas razões apresentadas em recurso perante a Suprema Corte daquele país no caso *Microsoft Irlanda*. Ali há menção expressa de que pedidos de cooperação via MLAT são lentos e de resultados incertos, podendo levar até anos para serem finalizados.

[15]A tese defendida pelo Departamento de Justiça norte-americano no caso citado é justamente a de que o critério controle deveria ser utilizado e que como a *Microsoft Estados Unidos*, controlava aos dados e as comunicações, ela deveria fornecê-los diretamente às autoridades locais, mesmo que os dados estivessem fisicamente localizados em provedor na Irlanda.

[16] Em fevereiro de 2018 foi apresentada proposta legislativa que altera a legislação estadunidense sobre a matéria. A íntegra pode ser acessada em https://www.hatch.senate.gov/public/_cache/files/6ba62ebd-52ca-4cf8-9bd0-818a953448f7/ALB18102%20(1).pdf .

[17]*Restatement of The Foreign Relations Law of the United States*, § 403 (http://www.kentlaw.edu/perritt/conflicts/rest403.html). No original:

> "*(1) Even when one of the base of jurisdiction under § 402 is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable*".

determinado país; (**ii**) conexões, como nacionalidade e atividade econômica, entre o país e o autor da ação; (**iii**) a importância da atividade para o Estado; (**iv**) como a atividade é regulada em outros países; e (**v**) harmonia entre a regulação e o sistema internacional.

No caso, os dados e comunicações buscadas são de brasileiros, colhidos em território nacional, e se relacionam à prática de crimes graves de competência da Justiça brasileira, cuja persecução é de suma importância para o Estado (**iii**). Ademais, esses dados foram coletados durante a prestação de serviço a brasileiros, oferecida por empresas brasileiras, de onde se conclui que há extensa conexão entre a atividade e os autores da ação e o Brasil, (**i** e **ii**) a justificar a jurisdição brasileira, ainda que esta venha a surtir efeitos em outros países, onde armazenados os dados, por exemplo.

Além disso, como exposto acima, o Tratado Internacional que rege a matéria, a Convenção de Budapeste, estabelece em seu artigo 18 a possibilidade de acesso direto a provas e dados coletados por empresa que presta serviço no território do país requisitante, de onde se conclui que o sistema de acesso previsto na legislação brasileira está em acordo com o sistema internacional (**v**).

Por fim, como exposto, o próprio governo norte-americano tem defendido, veementemente e em diversas instâncias, que também sua legislação local o autoriza a acessar dados controlados por empresas norte-americanas, independente do local de armazenamento físico desses dados. Em razões apresentadas perante a Suprema Corte daquele país, no já citado caso *Microsoft Irlanda*, afirmou o Departamento de Justiça norte-americano que:

> "*Em resposta, Microsoft alega que seu entendimento é necessário para evitar conflitos internacionais. Essa preocupação é exagerada. Muitos outros países interpretam suas leis para autorizar a requisição a empresas locais de provas armazenadas no exterior, ainda que existam restrições variadas para o exercício desse poder. De fato, os Estados Unidos são parte de um tratado que demanda que os Estados-parte tenham o poder de requisitar que provedores de serviço em seu território apresentem dados sob seu controle para fins penais. E o argumento de Microsoft de que ficará sujeita a regimes legais conflitantes interna e externamente, essa situação não tem ocorrido com frequência e pode ser solucionada através dos mecanismos*

existentes caso ocorra. De toda forma, isto não serve como base para afastar a melhor interpretação da lei"[18]

Essa afirmação deixa claro que as preocupações da autora e do *Facebook* quanto a eventuais conflitos legais com autoridades norte-americanas são infundadas, pois também naquele país prevalece a interpretação que o Estado obedece ao quanto disposto na legislação brasileira (**iv**) e internacional.

Ademais, não se tem notícia, na *década* em que o entendimento que permite acesso direto a dados vem sendo aplicado pelo Poder Judiciário brasileiro, de nenhum provedor sediado no exterior que tenha sofrido qualquer tipo de sanção ao atender às requisições de autoridades brasileiras para o fornecimento de dados diretamente. Igualmente, conforme informado na petição acima citada, apresentada pelo Governo dos Estados Unidos à Suprema Corte daquele país, também ali não se tem notícia de uma única empresa estadunidense que tenha sido punida por outro país em razão do fornecimento de dados a autoridades americanas[19]

Verifica-se, assim, que a realidade não corresponde ao quanto descrito na inicial. A submissão da jurisdição brasileira, com flagrante desrespeito às normas legais, impedirá a correta apuração de crimes praticados no Brasil, com vítimas e autores em território nacional, em clara violação ao poder-dever de punição e prevenção do Estado, e prejuízos imensos à sociedade brasileira.

De outro lado, a aplicação da lei brasileira não acarretará nenhum conflito internacional, pois ela está de pleno acordo com a legislação internacional sobre o assunto e

---

[18] Tradução livre. No original, que pode ser acessado em https://www.supremecourt.gov/DocketPDF/17/17-2/22902/20171206191900398_17-2tsUnitedStates.pdf:

"*In response, Microsoft argues that its theory is necessary to avoid international discord. That concern is overstated. Many other countries construe their laws to authorize compelling domestic entities to produce foreign-stored evidence, even if they place varying restrictions on the use of that power. Indeed, the United States is a party to a treaty that requires parties to have the power to compel service providers within their territory to produce data under the providers' control for law enforcement purposes. Ando to the extent Microsoft worries that it will be subject to conflicting legal regimes at home and abroad, that situation has not often arisen and can be addressed through existing mechanisms if it does. In any event, it provides no basis for overriding the best reading of the statutory scheme*".

[19] No original (https://www.supremecourt.gov/DocketPDF/17/17-2/22902/20171206191900398_17-2tsUnitedStates.pdf) :

"*In fact, Microsoft has not identified a single example of a U.S. service provider that has been compelled to disclose foreign-stored data under Section 2703 and has been sanctioned by a foreign nation for doing so.*"

com legislações locais de países estrangeiros. Torna-se cada vez mais consenso no direito internacional a *necessidade* do acesso direto a provas.

4. **<u>Da Ausência de Violação a Normas Constitucionais Brasileiras</u>**

Prossegue argumentando a inicial que a não aplicação do procedimento do MLAT aos pedidos de dados coletados de usuários brasileiros por empresas brasileiras feriria os princípios do devido processo legal e da igualdade. Esta última, simplesmente em razão da suposta existência de decisões contraditórias. O primeiro porque a não formulação de pedido de cooperação internacional impediria o exercício do direito de defesa das empresas e não observaria o processo legal previsto para a hipótese.

O primeiro argumento foi rebatido acima, quando se analisou a alegada existência de controvérsia. Como exposto, a inicial compara situações que não são semelhantes para tentar extrair delas as mesmas consequências. O setor bancário em nada se assemelha ao setor de empresas de tecnologia que oferecem aplicativos via internet: no primeiro, o serviço é prestado no exterior e voltado ao exterior; no segundo, o serviço é prestado no Brasil, voltado a usuários brasileiros; no primeiro, aplicam-se as regras gerais de jurisdição; no segundo, há norma específica. Aliás, ainda que as situações fossem semelhantes, a simples existência de norma legal específica consubstanciada no artigo 11 do Marco Civil da Internet é suficiente para afastar qualquer possibilidade de aplicação analógica.

O segundo argumento também não se sustenta. Como já exposto à exaustão, há procedimentos distintos para a obtenção de documentos mantidos no exterior, por pessoas localizadas no exterior, e dados e documentos mantidos em lugar indefinido por empresas que oferecem serviços no Brasil a usuários brasileiros. O devido processo legal em um caso exige pedido formal de cooperação internacional; o segundo, não.

Igualmente, não se pode dizer que as empresas que recebem as ordens têm tido seus direitos violados. São inúmeros os recursos manejados contra as decisões que determinam o fornecimento dos dados, de onde se extraem as diversas decisões proferidas pelo Egrégio Superior Tribunal de Justiça, não sendo possível afirmar que elas não têm encontrado mecanismos legais de tentar fazer prevalecer seu entendimento. O fato de o litigante não ter razão não leva à conclusão de que a ele não foi assegurado o devido processo legal.

Também argumenta a inicial que as decisões estariam violando o princípio constitucional da livre iniciativa. Neste ponto, confunde a inicial o direito ao exercício livre de atividade empresarial, com o direito, evidentemente inexistente, de em nome do empreendedorismo violar as normas legais de um país. Em nenhum momento as decisões questionadas, e as regras legais que regem as empresas prestando serviços no país a usuários brasileiros, impedem que as sociedades empresariais desenvolvam seus modelos de negócios. Elas apenas determinam de forma clara e transparente, que qualquer modelo de negócios a ser desenvolvido no Brasil deve seguir a legislação brasileira, conforme editada pelo Congresso Nacional que nada mais faz do que expressar a vontade da sociedade brasileira. A empresa que não concorda com os valores e regras defendidos pela sociedade brasileira através de seus representantes legais tem a liberdade de simplesmente não realizar negócios no Brasil e aqui não oferecer seus serviços.

O que não é possível, e parece ser essa a intenção da autora e da principal interessada na ação, é submeter a sociedade brasileira a regras estrangeiras definidas pelo Congresso de outro país. Ora, o serviço oferecido pelo *Facebook* ***não é essencial*** e possui inúmeras deficiências, sendo as chamadas *fake news*, abordadas com mais vagar abaixo, apenas uma delas, mas ainda que o fosse, não pode a sociedade brasileira, sob pena de ceder parcela considerável de sua soberania, aceitar regulações estrangeiras apenas para receber serviço que é oferecido livremente por concorrentes que obedecem à legislação nacional.

Frise-se, novamente, que o modelo desenvolvido na legislação brasileira está em acordo com tratados internacionais, com a legislação de diversos países e com o posicionamento do governo norte-americano. Em nenhum momento esse modelo viola regras constitucionais brasileiras e nem impede o livre exercício de atividades empresariais. O que pretende a inicial é que a legislação se adeque ao modelo de negócios de uma empresa privada específica, o *Facebook*, ao invés do contrário.

5. Da Ausência de Descumprimento de Preceito Fundamental

Alternativamente, em caso de não recebimento da presente ação como Declaratória de Constitucionalidade, requer a inicial o reconhecimento de descumprimento de prefeitos fundamentais. Argumenta que a não formulação de pedidos de cooperação internacional para a obtenção de dados coletados no Brasil de usuários brasileiros por empresas que oferecem serviço em território brasileiro violaria os princípios da

"*territorialidade, da não-intervenção, da igualdade entre os Estados, da reciprocidade e da cooperação entre os povos para o progresso da humanidade*".

Cada um desses pontos foi abordado acima. Entretanto, é necessário ressaltar, mais uma vez, que o modelo mundialmente aceito para a coleta de dados tem sido exatamente o trazido pela legislação brasileira. Assim, ainda que não ausente tratado assinado pelo Brasil, é necessário reconhecer a existência de *soft law* e de entendimento internacional sobre a matéria, sendo certo que a simples observância de modelo internacional, antes de violar o princípio da cooperação entre os povos, apenas reforça o compromisso brasileiro com o seu pleno atendimento.

6. **Das Consequências em Caso de Procedência da Ação**

Em razão de todo o exposto, resta evidente que as decisões indicadas na inicial, em especial as oriundas do Egrégio Superior Tribunal de Justiça, que apenas unificou a jurisprudência sobre o assunto, em nada violam regras constitucionais e em nada destoam dos mecanismos internacionais hoje vigentes. Apesar disso, requer a inicial a concessão imediata de medida liminar que afaste todas as decisões que dão plena eficácia ao artigo 21 do Código de Processo Civil e ao artigo 11 do Marco Civil da Internet. A concessão da ordem como requerida trará gravíssimas e irremediáveis consequências para incontáveis investigações e ações criminais em andamento, além de iniciativas do Tribunal Superior Eleitoral.

Em nome da proteção financeira de uma *única* empresa que sistematicamente se recusa a cumprir decisões legais emanadas de autoridades competentes, busca a inicial a paralisação de inúmeras investigações e ações criminais. Como exposto, o reconhecimento da jurisdição brasileira para a obtenção direta de dados coletados por empresas brasileiras prestando serviços de tecnologia a usuários brasileiros em território nacional vem de longa data, sendo certo que há mais oito anos a jurisprudência do Superior Tribunal de Justiça se harmonizou neste sentido. Desde então, inúmeras investigações e ações criminais, inclusive apurações atualmente em andamento perante o Supremo Tribunal Federal, têm em seu bojo provas colhidas de forma direta. Igualmente, inúmeras ações criminais possuem sentenças condenatórias transitadas em julgado baseadas nas provas assim colhidas. A concessão da medida pretendida, desse modo, poderá colocar em dúvida a legitimidade das provas colhidas em centenas de ações penais, sentenças sendo executadas e investigações em

andamento, gerando insegurança jurídica que, nos anos de construção do entendimento, nunca aconteceu.

Ademais, não se pode esquecer que no ano de 2018 serão realizadas eleições gerais, sendo certo que as iniciativas que estão sendo desenvolvidas para evitar a proliferação de notícias falsas serão amplamente prejudicadas por qualquer medida que altere bruscamente o arcabouço constitucional hoje existente.

Como exposto acima, a Primeira Emenda da Constituição Federal norte-americana torna bastante restritos os casos em que pedidos de conteúdo podem ser atendidos[20]. Ainda que as mensagens sejam de cunho criminoso em território brasileiro, as restrições impostas pelo citado dispositivo e pela jurisprudência da Suprema Corte estadunidense tornam praticamente impossível a obtenção de determinados conteúdos por via de cooperação internacional.

Assim, tem-se que, caso concedida a medida pretendida, crimes graves simplesmente deixarão de ser investigados e as infrações de cunho eleitoral, em ano de eleições gerais, não serão corretamente apuradas e seus responsáveis punidos. Justamente em razão das peculiaridades da legislação de cada local, o acesso direto às provas colhidas durante a prestação de serviços naquele território deve ser garantido às autoridades locais, sem interferência de outros Estados que não possuem interesse nem legitimidade para se imiscuir na questão.

De outro lado, a não concessão da medida não acarretará qualquer tipo de prejuízo insanável. Primeiro porque, como exposto, nos mais de dez de aplicação do entendimento, não há notícia de ***nenhum*** caso em que empresa sediada no exterior tenha

---

[20] Apenas a título de exemplo, mencione-se o entendimento da Suprema Corte estadunidense sobre a Primeira Emenda da Constituição daquele país e o discurso ofensivo e de ódio. Nos termos do quanto decidido em Brandenburg v. Ohio (395 US 444, 1969), restrições à liberdade de expressão, ainda que visando restringir discurso de ódio, devem ser submetidas a escrutínio estrito: somente quando há incitação expressa de violação da lei e essa violação é iminente e provável a restrição pode ser considerada legal. Em outras palavras, na maior parte das situações em que há discurso de ódio e ofensivo, como não há incitação a violência imediata e provável, não há dupla incriminação, o que impede o pedido de cooperação.

A decisão original pode ser encontrada em https://www.law.cornell.edu/supremecourt/text/395/444, da qual se destaca:

> "*Freedoms of speech and press do not permit a State to forbid advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent Lawless action and is likely to incite or produce such action*".

sido punida porque sua subsidiária brasileira forneceu provas diretas a autoridades brasileiras.

Segundo, porque a principal empresa que se recusa a cumprir as ordens tem sido capaz de apresentar seus argumentos e exercer seus direitos. As multas impostas, além de representar valor irrisório quanto comparadas ao poderio do grupo econômico, podem ser imediatamente afastadas bastando a ela cumprir o quanto determinado o que, aliás, vem sendo feito pelas demais empresas.

Ante o exposto, ausente risco na não concessão da medida pretendida, mas prejuízo incompensável na concessão, inviável o atendimento do quanto requerido.

7. **Conclusão**

Do quanto exposto, necessário concluir que a suposta violação constitucional apontada na inicial não existe.

O que existe é a aplicação plena de regra geral, consubstanciada no artigo 21 do Código de Processo Civil, e de regra específica para dados colhidos durante o oferecimento de serviços a usuários brasileiros trazida pelo artigo 11 do Marco Civil da Internet. As empresas que oferecem esse serviço, sejam porque brasileiras, constituídas segundo as leis brasileiras, seja porque aqui possuem "*agência, filial ou sucursal*", são submetidas à legislação brasileira e às regras que definem jurisdição.

A existência de regra específica para provas colhidas através do oferecimento de aplicativos na internet não conflita com a regra geral de cooperação internacional em outras hipóteses. O fato de o Estado brasileiro, em razão de previsão específica, ter jurisdição sobre essas provas não afasta a aplicação das regras que regem as cartas rogatórias e os pedidos de cooperação direta em outras hipóteses onde a regra não se aplica.

A legislação brasileira está em acordo com a legislação de outros países e com o entendimento que têm sido dado à matéria em foros internacionais. O próprio governo norte-americano defende a aplicação de regra semelhante, sendo certo que não se tem notícia de nenhum caso de punição a empresa sediada em outro país em razão do cumprimento do quanto determinado pelas autoridades brasileiras nos longos anos em que esse entendimento tem vigorado.

A sociedade brasileira, que debateu amplamente o Marco Civil da Internet, não pode se ver submetida à conveniência de uma empresa ou ao entendimento dos legisladores de outros países.

Qualquer restrição à capacidade das autoridades brasileiras de obterem diretamente dados e comunicações de brasileiros, coletados por empresas aqui constituídas ou que aqui prestam serviços direcionados a brasileiros gerará imenso prejuízo a investigações em andamento e ações penais já transitadas em julgado, tornando praticamente impossível a correta e eficiente apuração de crimes praticados através da rede mundial de computadores.

Fernanda Teixeira Souza Domingos
Procuradora da República

Melissa Garcia Blagitz de Abreu e Silva
Procuradora da República