MINISTÉRIO PÚBLICO FEDERAL

Memorial para Audiência Pública no STF em 10/02/2020

Grupo de Apoio Sobre Criminalidade Cibernética da Câmara Criminal

Ação Declaratória de Constitucionalidade (ADC) nº 51

O presente Memorial é apresentado pelo Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal do Ministério Público Federal com o fim de subsidiar participação da instituição em audiência referente à Ação Declaratória de Constitucionalidade (ADC 51) 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.*.

Conforme exposto em Nota Técnica anteriormente apresentada pelo Grupo de Apoio e em parecer apresentado nos autos pela Procuradoria-Geral da República, 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 a autora 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.

A Nota Técnica informa que a argumentação trazida na ação, composta por inúmeros equívocos, tenta afirmar que a legislação brasileira, em especial o artigo 21 do Código de Processo Civil, e o artigo 11 da Lei nº. 12.965/2014 (Marco Civil da Internet), confere às autoridades judiciárias brasileiras apenas "meia jurisdição", permitindo-lhes o acesso direto apenas a dados cadastrais e metadados, mas não ao conteúdo de comunicações coletado por empresas brasileiras, em território brasileiro, enquanto prestam serviços destinados a brasileiros, mas que são controladas por empresas sediadas no exterior. Para estes casos, afirmam os autores, seria necessário o uso de instrumentos de cooperação internacional, sob pena de criação de conflito internacional de graves proporções.

A Nota Técnica, a qual reiteramos na integralidade, também esclarece os erros da argumentação, em especial quanto à definição de jurisdição prevista na legislação brasileira, que não faz distinção entre os tipos de dados, as gravíssimas consequências da adoção do entendimento defendido pelos autores, notadamente a submissão do Legislador nacional à vontade do Legislador estrangeiro, e também a ausência de consequências no direito internacional, diante da adoção, por cada vez mais instrumentos internos e multilaterais, de regras de jurisdição semelhantes às adotadas pela legislação pátria.

Resta evidenciado nas manifestações anteriores, 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*". A legislação nacional, assim, adota o critério dos efeitos do serviço (*targeting test*) aliado ao critério da territorialidade para definir a jurisdição das autoridades brasileiras.

Pois bem. Desde a apresentação do referido documento, algumas alterações no cenário interno e internacional reforçaram ainda mais o argumento de ausência de conflito, com a adoção, por cada vez mais instrumentos de cunho transnacional, dos mesmos critérios de definição de jurisdição trazidos pela legislação pátria, em especial do *targeting test*.

1. Da Convenção de Budapeste

Em dezembro de 2019, o Conselho da Europa formalizou convite para que o Brasil aceda à Convenção sobre Cibercriminalidade, ETS 185, conhecida como Convenção de Budapeste. Este é o principal instrumento internacional sobre criminalidade cibernética, trazendo dispositivos de direito material e de direito processual, inclusive regras para acesso transfronteiriço a dados eletrônicos, como arcabouço mínimo para a matéria.

Conforme exposto de forma mais detalhada na Nota Técnica, a Convenção, contém em seu artigo 18 regra semelhante ao artigo 11 da Lei nº. 12.965/2014 (Marco Civil da Internet),

reconhecendo que cada país signatário possui jurisdição sobre as provas coletadas em seus territórios por empresas ali sediadas ou que prestam serviços direcionados a seus cidadãos[1].

Assim, uma vez ratificado o novo instrumento, com a inclusão de seus termos no ordenamento jurídico brasileiro como lei federal, haverá previsão assegurando a jurisdição das autoridades brasileiras sobre os dados coletados no Brasil por empresa estrangeira que presta serviços no Brasil não somente por força de lei local, mas também por força de instrumento internacional, adotado por dezenas de países e reconhecido por centenas de outros, incluindo os Estados Unidos.

A lei brasileira, ao trazer previsão semelhante ao principal instrumento internacional sobre a matéria, não representa qualquer conflito.

2. Do CLOUD Act

Quando da apresentação da referida Nota Técnica, havia sido apresentada proposta de alteração da legislação estadunidense, em especial do título 18 USC 121 §2713, que previa duas importantes mudanças. A primeira delas dizia respeito a uma alteração de regra de jurisdição, deixando explicitado o critério de controle, e também o critério de efeitos do serviço, como regra para a definição da jurisdição das autoridades dos Estados Unidos. A segunda alteração previa a possibilidade de serem firmados acordos bilaterais entre aquele país e outros que atendessem determinados critérios para que as decisões requisitando dados e outras informações fossem cumpridas diretamente pelos provedores, mediante acesso direto.

Importante o detalhamento de cada uma dessas alterações, bem como de suas implicações na presente ação.

2.1 – Da mudança das regras de jurisdição estadunidense

A primeira alteração diz respeito à modificação dos critérios de definição de jurisdição daquele país.

Como exposto de forma detalhada na Nota Técnica apresentada, a jurisprudência

estadunidense estava se inclinando a reconhecer a jurisdição daquele país apenas sobre os dados e conteúdos armazenados em seu território, independente do local de coleta e de oferecimento do serviço.

Tal posicionamento, contrário ao que vem se firmando há anos no cenário internacional, e mesmo contrário ao disposto no artigo 18 da Convenção de Budapeste, do qual aquele país é parte, motivou a alteração legislativa que entrou em vigor em 23 de março de 2018 e que determina, de forma clara, o critério de controle para definição de jurisdição, estabelecendo que (tradução livre):

> "*Um provedor de serviço de comunicação eletrônica ou de computação remota deve cumprir os deveres definidos neste capítulo de preservar, guardar ou apresentar o conteúdo de comunicações eletrônicas e qualquer registro ou outra informação referente a consumidor ou usuário na posse, guarda ou controle do provedor, não importando se tal comunicação, registro ou outra informação está localizada dentro ou fora dos Estados Unidos.****[2]***"

Tal regra, aliada às demais modificações introduzidas no capítulo, permite que as autoridades norte-americanas tenham acesso direito às provas, sejam elas dados, metadados ou conteúdo, controladas por empresas estabelecidas em seu território, independente do local de efetiva armazenagem.

Segundo estudos publicados pelo Departamento de Justiça dos Estados Unidos (*Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act - White Paper, abril de 2019*)[3], a mencionada alteração legislativa, embora descreva expressamente o critério de controle dos dados, também admite a utilização do *targeting test* na definição da jurisdição das autoridades estadunidenses, quando o serviço for prestado de forma direcionada a usuários americanos, dentro do território daquele país, ocasião em que poderá ser reconhecida a existência de jurisdição sobre a empresa. Neste sentido (tradução livre):

> "*Nada no CLOUD Act altera a condição de que os Estados Unidos devem possuir jurisdição pessoal sobre a empresa para requisitar o fornecimento de informações que ela controla(...). Jurisdição pessoal será mais*

> *facilmente estabelecida quando uma empresa é localizada nos Estados Unidos.* ***Se uma empresa estrangeira localizada fora dos Estados Unidos, mas oferecendo serviços nos Estados Unidos tem contato suficiente com os Estados Unidos para estar sujeita à jurisdição americana é questão a ser determinada conforme a natureza, quantidade, e qualidade dos contatos da empresa com os Estados Unidos***"[4] (destaque nosso).

Essa interpretação nada mais reflete do que a aplicação, na legislação norte-americana, do critério dos efeitos do serviço (*targeting test*) reconhecido expressamente pelo art. 11 do Marco Civil da Internet. Segundo a orientação do Departamento de Justiça dos Estados Unidos, as autoridades norte-americanas terão acesso direto às provas eletrônicas, incluindo dados, metadados e conteúdo, se estas forem controladas por empresas sob sua jurisdição, entendendo-se aí aquelas que, mesmo estrangeiras, prestarem serviços direcionados a usuários estadunidenses.

Vê-se, assim, que mesmo a legislação do país sede da empresa principal interessada no deslinde desta causa determina a aplicação de critério idêntico ao vigente no Brasil e, justamente por isso, não pode a ele se opor.

2.2 – Dos acordos bilaterais

A outra mudança legislativa trazida pelo CLOUD Act foi introduzida no 18 USC 121 §2523 com a possibilidade de serem firmados acordos bilaterais entre os Estados Unidos e outros países, acordos estes que permitam o acesso direto a dados sob jurisdição dos Estados-Parte, com o reconhecimento mútuo da validade das decisões requisitórias. Nas explanações do Departamento de Justiça norte-americano (tradução livre – fonte citada acima):

> "*Ele autoriza o governo dos Estados Unidos a entrar em acordos bilaterais com governos estrangeiros mediante os quais cada país removerá qualquer impedimento legal que de qualquer forma proíba o cumprimento de ordens judiciais determinadas expedidas pelo outro país. Ambos os Estados seriam capazes de submeter requisições para provas eletrônicas necessárias para a persecução de crimes graves diretamente aos provedores, sem o*

> *envolvimento de outros governos e sem o receio de conflito com a lei dos Estados Unidos ou de qualquer outra nação*”[5].

Esses acordos, em princípio, poderiam representar uma solução para o suposto conflito aqui apontado pela empresa interessada no deslinde da ação. Poder-se-ia argumentar que, uma vez firmado o acordo, as ordens de autoridades brasileiras poderiam ser cumpridas diretamente pelo *Facebook* sem risco de conflito com a legislação de sua sede e de forma a preservar a rapidez do processo, afastando-se o tão temido conflito de leis internacional. Essas benesses, porém, são ilusórias.

Primeiro, porque a aprovação dos acordos depende do preenchimento de uma séria de requisitos impostos pela legislação americana e cuja avaliação é de absoluta discricionariedade daquele país, passando por duas fases de escrutínio, uma no Poder Executivo e outra no Poder Legislativo.

Segundo, e mais grave, porque esses acordos não poderão ser utilizados para a obtenção de informações referentes a um cidadão ou pessoa jurídica dos Estados Unidos e nem em casos onde a liberdade de expressão, nos termos definidos pela Constituição estadunidense, puder ser restringida

Determina o 18 USC 121, § 2523 (b)(3)(A) que (tradução livre):

> “*(A) o governo estrangeiro não poderá intencionalmente buscar informações de um cidadão norte-americano ou de pessoa localizada no território dos Estados Unidos, e deve adotar procedimentos para cumprir essa condição*”[6].

Assim, caso um cidadão estadunidense, residente no Brasil, cometa um crime em território brasileiro, contra vítima brasileira, as autoridades brasileiras que investigam os fatos não poderão utilizar de eventual acordo para a obtenção direta de prova eletrônica retida por provedor controlado por empresa norte-americana. Restaria, aqui, apenas a demorada cooperação internacional, com todos os limites e restrições.

Igualmente, determina o § 2523(b)(3)(E) que (tradução livre):

> "*(E) uma requisição expedida por governo estrangeiro não pode ser usada para restringir a liberdade de expressão*"[7].

Desse modo, e nos termos detalhados na Nota Técnica, nenhuma investigação brasileira por crime de discriminação ou preconceito praticado por meio da internet (artigo 20, §2º da Lei 7.716/89), por crime de incitação ao terrorismo ou mesmo infração de natureza eleitoral que envolva, ainda que tangencialmente, a exposição de ato ou fato falso, praticados em território brasileiro, por brasileiros, poderá se utilizar do acordo para a obtenção direta de dados. E, nestes casos, nem mesmo pedido de cooperação internacional é possível.

Tem-se, assim, que embora à primeira vista os acordos propostos pareçam solucionar as inquietações expostas pela empresa principal interessada na presente ação, *Facebook*, eles não solucionam os problemas de ordem prática impostos pela aceitação cega e inconsequente da jurisdição norte-americana sobre dados coletados de brasileiros em território nacional por empresa brasileira.

Pior. Esses acordos criam uma categoria de cidadãos intocáveis, pois se um cidadão norte-americano residente no Brasil divulgar notícias falsas (*fake news*) com finalidade eleitoral, em eleições brasileiras, utilizando-se dos serviços oferecidos por empresa brasileira em território nacional, provas eletrônicas aqui colhidas, como diálogos, jamais conseguirão ser obtidas, seja porque o uso dos acordos é vedado contra cidadãos estadunidenses, seja porque as regras constitucionais daquele país impedem a persecução de crimes relacionados a discurso, ainda que falso, fora de hipóteses bastante restritas.

Justamente em razão das restrições impostas, a primeira proposta de acordo apresentada[8], e que ainda pende de análise pelo congresso norte-americano, traz regras claras que afastam sua aplicação como instrumento de determinação de jurisdição[9].

Na proposta apresentada em conjunto pelos governos dos Estados Unidos e do Reino Unido, o acordo somente será utilizado quando a situação não estiver abarcada pela jurisdição do país requisitante. Estabelece o artigo 11, item 1 que (tradução livre):

> "*Este acordo é firmado sem prejuízo e não afetará outras autoridades legais e mecanismos do país demandante para requisitar ou preservar*

> *dados eletrônicos do país demandado e dos provedores abrangidos sujeitos à jurisdição do país demandado, incluindo instrumentos legais e práticas conforme a lei doméstica de qualquer Parte para os quais a Parte não invoque este acordo; requerimentos de assistência mútua; e requisições de emergência*"[10].

Em outras palavras, ainda que o Brasil firmasse acordo de bases semelhantes, o que parece ser o principal interesse da empresa que impulsiona a presente demanda, ele não solucionaria o quanto aqui posto: o Brasil, por força de cláusulas específicas da legislação, em conformidade com normas internacionais, tem jurisdição sobre os dados coletados em seu território, de brasileiros, por empresa brasileira ou estrangeira que presta serviços aqui, podendo a eles ter acesso diretamente. Somente seria necessário o uso do acordo nas raras hipóteses em que a lei não concede essa jurisdição (por exemplo, quando a empresa requisitada não tem filial/sucursal no Brasil e nem presta serviços direcionados a brasileiros), e nessas hipóteses não se incluem os serviços prestados pelo *Facebook*, empresa brasileira.

Essa realidade torna inócua a expectativa da postulante, bem como sua insistência em fazer valer legislação estrangeira sobre dados coletados em território nacional por empresa nacional.

3. Dos demais instrumentos internacionais e nacionais

Além do citado CLOUD Act, que trata especificamente do acesso direto e compartilhamento de provas eletrônicas, outros instrumentos, nacionais e internacionais, ainda que não voltados especificamente para provas eletrônicas, trazem regras de jurisdição semelhantes, tudo a reforçar a correção da previsão contida na legislação brasileira, em especial do artigo 11 do Marco Civil da Internet.

Isto porque, tais instrumentos, reconhecendo a peculiaridade dos dados eletrônicos e das comunicações, também aplicam como critério de definição de jurisdição e incidência, os efeitos dos serviços.

3.1 – Da Regulação 2016/679 do Parlamento Europeu (Regulação de Proteção Geral de Dados)

A Regulação UE 2016/679 (*General Data Protection Regulation – GDPR*), que entrou em vigor em maio de 2018, estabelece regras para a proteção da privacidade dos usuários no exercício de atividades que envolvam o processamento de dados de pessoas naturais.

Ciente da natureza peculiar dos dados, que podem ser coletados em um lugar, processados em outro e armazenados em um terceiro, a Resolução, ao estabelecer as regras de jurisdição para sua aplicação, utilizou os *mesmos* critérios empregados pelo Marco Civil, em seu artigo 11, quais sejam, o do estabelecimento da empresa que realiza a atividade e o dos efeitos do serviço. Assim, estabelece o Artigo 3 que (tradução livre):

> "*1. Esta Regulação aplica-se ao processamento de dados naturais no contexto das atividades de um estabelecimento de um controlador ou processador localizado na União, independente de o processamento ocorrer no território da União ou não.*
>
> *2. Esta Regulação aplica-se ao processamento de dados pessoais de titulares de dados que estejam na União por um controlador ou processador não estabelecidos na União, quando as atividades de processamento estão relacionadas a:*
>
> *(a) a oferta de produtos ou serviços, gratuito ou não, a titulares de dados na União; ou*
>
> *(b) o monitoramento de seu comportamento, desde que este ocorra na União.*
>
> *3. Esta Regulação aplica-se ao processamento de dados pessoais por um controlador não estabelecido na União, mas em um lugar onde a lei de um Estado Membro aplica-se por força de regra de direito público internacional"* ***[11]*** (destaques nossos).

Em outras palavras, a nova legislação da União Europeia sobre proteção geral de dados

incidirá sobre as empresas estabelecidas no território da União (critério territorial) e também sobre empresas estabelecidas em outros territórios, mas que ofereçam serviços às pessoas no território europeu (critério de efeitos do serviço), tudo em absoluta consonância com o citado artigo 11 do Marco Civil da Internet que, editado dois anos antes da norma europeia, acabou por traçar o caminho seguido agora por outros países.

3.2 – Da Lei Geral de Proteção de Dados (LGPD)

De outro lado, a Lei Geral de Proteção de Dados (LGPD) brasileira (Lei no. 13.709/2018), que introduziu dispositivos semelhantes ao GDPR, traz regras idênticas de definição de jurisdição. Estabeleceu seu artigo 3º. que:

> "*Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:*
>
> *I- a operação de tratamento seja realizada no território nacional;*
>
> *II- a atividade de tratamento tenha por objeto a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou*
>
> *III- dos dados pessoais objeto do tratamento tenham sido coletados no território nacional*" (destaque nosso).

As regras relativas à jurisdição e aplicabilidade de LGPD, além de estarem em harmonia com as disposições do GDPR e da Convenção de Budapeste, fazendo valer a jurisdição local quando o serviço é ofertado no território, independente do local do estabelecimento da empresa, também estão em absoluta consonância com as regras de jurisdição previstas no artigo 11 do Marco Civil da Internet. Na verdade, a norma brasileira vai além, prevendo a aplicação das regras de proteção sempre que os dados tiverem sido coletados em território brasileiro, ainda que a empresa coletora ou processadora não tenha estabelecimento no Brasil e aqui não oferte serviços

direcionados a brasileiros.

3.3 – Da proposta de Regulação sobre prova eletrônica da União Europeia (*E-evidence*)

Apesar da previsão expressa no artigo 18 da Convenção de Budapeste, a União Europeia, visando assegurar o acesso direto de seus membros aos dados coletados durante a prestação de serviços em seu território, apresentou proposta de Resolução que trata, especificamente, de ordens de preservação e requisição de provas eletrônicas.

É da essência desta proposta, que ainda está em discussão e, por isso, não possui texto final aprovado, que as autoridades legais dos países membros poderão expedir ordens de preservação ou de requisição direta de dados e demais provas eletrônicas, incluindo conteúdo, a provedores que oferecem serviços no território da União Europeia, independente do local de estabelecimento da empresa. Assim como ocorreu com a previsão do artigo 3º. do GDPR, a jurisdição é determinada pelo local de oferta do serviço (efeitos do serviço) e não pelo local de sede da empresa controladora e nem de armazenagem dos dados.

Verifica-se, dessa forma, que mesmo instrumentos internacionais ainda em fase de gestação preveem regras de jurisdição com critérios semelhantes e harmônicos ao Marco Civil da Internet, tudo a consolidar o posicionamento de que o fator a determinar a jurisdição sobre a prova eletrônica deve ser, primordialmente, o local onde o serviço é oferecido, ainda que outros possam também ser empregados.

4. Das consequências

Como mencionado na referida Nota Técnica, a prevalecer o entendimento defendido pelos autores da ADC 51, investigações de diversos tipos penais, inclusive modificações introduzidas recentemente pelo Legislador pátrio, não serão mais possíveis quando envolverem acesso a conteúdo de comunicações de brasileiros controlados por empresas com sede nos Estados Unidos, ainda que estas possuam representante no Brasil e tenham colhido estes dados em território nacional.

Assim, investigações referentes ao crime definido no artigo 326, § 3º do Código Eleitoral, introduzido em 8 de novembro de 2019, não poderão contar com dados de conteúdo colhidos no Brasil por empresas prestando serviços a brasileiros porque o entendimento da Suprema Corte norte-americana impede a persecução penal nestes casos[12].

Vê-se, portanto, que mais do que afetar a investigação criminal, o entendimento que quer fazer prevalecer a empresa privada principal interessada no deslinde da presente ação retira do Legislador brasileiro o poder soberano de definir quais condutas praticadas por brasileiros em território nacional merecem ser criminalmente investigadas e punidas. Aquelas infrações que não estiverem de acordo com as estritas definições legais de corte estrangeira não poderão utilizar provas colhidas de brasileiros em território nacional por empresa brasileira simplesmente porque a empresa que as coletou, embora brasileira e aqui oferecendo serviços, mantém sua sede corporativa em outro país. Tamanho desrespeito ao poder soberano de autorregulação da sociedade brasileira não pode ser sufragado.

5. Conclusão

De todo o quanto narrado, apesar da insurgência da autora e da empresa *Facebook*, que a impulsiona, as modificações nos cenários internacional e nacional ocorridas desde a apresentação da Nota Técnica pelo Grupo de Apoio sobre Criminalidade Cibernética, apenas reforçaram os conceitos de jurisdição existentes na legislação brasileira.

Em razão das peculiaridades da prova eletrônica, os conceitos de jurisdição adotados pelos países têm se afastado do critério puramente territorial, aproximando-se cada vez mais dos critérios de efeitos do serviço, estabelecendo que um país possui jurisdição sobre os dados coletados em seu território por empresas que prestam serviços direcionados a seus residentes, seja para ter acesso a eles mediante o devido processo legal em investigações criminais, seja para proteger a privacidade de seus titulares quando do processamento e tratamento das informações.

O cenário de completo conflito de normas e de caos propagado pelos autores não está ocorrendo na prática, servindo a previsão do artigo 11 do Marco Civil da Internet de modelo para legislações do mundo inteiro, tornando a proposição regra aceita e incentivada de direito

internacional costumeiro.

A Convenção de Budapeste, da qual o Brasil é observador e que inclui dezenas de signatários, inclusive os Estados Unidos, contém dispositivo semelhante ao citado artigo 11 e não se tem notícia de conflitos emergindo entre os vários países que a adotam.

A legislação internacional, portanto, converge para a adoção dos mesmos critérios vigentes no Brasil, sendo certo que qualquer alteração, em especial a pretendida pela ação, transformará o Brasil, de expoente no tema e possuidor de regras harmônicas com os demais países, em ator isolado, sujeito aos ditames e à interpretação de regras de advogados privados de empresa privada.

Observe-se, ademais, como já exposto na referida nota técnica, que eventuais conflitos entre normas poderão ser facilmente solucionados com o conceito de cortesia, ou *international comity*, segundo o qual a aplicação da lei local com efeitos internacionais deve ser limitada pela razoabilidade, que deve ser avaliada levando-se em conta, dentre outros fatores, (**i**) a extensão da conexão entre a atividade realizada e o território de 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 de dados e conteúdos coletados de brasileiros em território nacional por empresa que presta serviços voltados a brasileiros, todos esses elementos estão presentes, sendo certo que nenhum país que adota regras semelhantes criará entraves para a prevalência da jurisdição brasileira até porque, 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.

Por fim, como já exposto na referida Nota Técnica:

> "*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".

Brasília, 07 de fevereiro de 2020.

Fernanda Teixeira Souza Domingos
Procuradora da República
Coordenadora do Grupo de Apoio sobre Criminalidade Cibernética – GACC

Neide M. C. Cardoso de Oliveira
Procuradora Regional da República
Coordenadora Adjunta do Grupo de Apoio sobre Criminalidade Cibernética – GACC

---

[1]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*".

[2] No original: "*A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States*"

[3] https://www.justice.gov/dag/page/1153436/download

[4] No original: "*Nothing in the CLOUD Act changed the requirement that the United States must have personal jurisdiction over a company in order to require the disclosure of information the company holds (...). Personal jurisdiction is most readily established when a company is located in the United States. Whether a foreign company located outside the United States but providing services in the United States has sufficient contacts with the United States to be subject to U.S. jurisdiction is a fact-specific inquiry turning on the nature, quantity, and quality of the company's contacts with the United States*".

[5] No original: "*It authorizes the U.S. government to enter into executive agreements with foreign nations under which each country would remove any legal barriers that may otherwise prohibit compliance with qualifying court orders issued by the other country. Both nations would be able to submit orders for electronic evidence needed to combat serious crime directly do CSPs, without involving the other government and without fear of conflict with U.S. or the other nation's law.*".

[6] No original: "*(A) the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement.*"

[7] No original: "*(E) na order issued by the foreign government may not be used to infringe freedom of speech*".

[8]https://www.justice.gov/ag/page/1207496/download#Agreement%20between%20the%20Government%20of

%20the%20United%20States%20of%20America%20and%20the%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%20on%20Access%20to%20Electronic%20Data%20for%20the%20Purpose%20of%20Countering%20Serious%20Crimes

[9] *Artigo 6, item 3, determina (tradução livre): "Este acordo não restringe, de nenhuma forma, ou elimina nenhuma obrigação legal que os provedores abrangidos tenham para produzir dados em resposta a procedimento legal expedido consoante a lei do país demandante*".

No original; "*This Agreement does not in any way restrict or eliminate any legal obligation Covered Providers have to produce data in response to Legal Process issued pursuant to the law of the Issuing Party*".

[10] No original: "*This Agreement is without prejudice to and shall not affect other legal authorities and mechanisms for the Issuing Party to obtain or preserve electronic data from the Receiving Party and from Covered Providers subject to the jurisdiction of the Receiving Party, including legal instruments and practices under the domestic law of either Party as to which the Party does not invoke this Agreement; requests for mutual legal assistance; and emergency disclosures.*"

[11] No original: "*1. This Regulations applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*

2. This Regulation applies to the processing of personal data of data subjects who are n the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behavior as far as their behavior takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

[12] Conforme decidido pela Suprema Corte estadunidense em *United States v. Alvarez* (567 U.S. 709, de 2012), afirmações falsas, simplesmente por serem falsas, não estão fora da proteção concedida pela Primeira Emenda.