Instituto de Referência em Internet e Sociedade

Sigilo online, investigações criminais e cooperação internacional

contribuições para a ADC 51/2017

IRIS
Instituto de Referência em Internet e Sociedade

Instituto de Referência em Internet e Sociedade

Sigilo online, investigações criminais e cooperação internacional

Contribuições para a ADC 51/2017

Orientação científica
Fabrício Bertini Pasquot Polido

Coordenação do projeto
Lucas Costa dos Anjos
Luíza Brandão

Coordenação de pesquisa
Odélio Porto Jr.

Autoria
Fabrício Bertini Pasquot Polido
Lucas Costa dos Anjos
Pedro Vilela
Odélio Porto Jr.

Colaboração e Revisão
Luíza Brandão
Victor Vieira

Projeto Gráfico
André Oliveira

Capa
André Oliveira
Felipe Duarte

Diagramação e finalização
André Oliveira

Produção editorial
Instituto de Referência em Internet e Sociedade

Como citar em ABNT
POLIDO, Fabrício Bertini Pasquot et al. **Sigilo online, investigações criminais e cooperação internacional:** contribuições para a ADC 51/2017. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2018. Disponível em: http://bit.ly/2qJpHwj. Acesso em: DD mmm. AAAA

SUMÁRIO

1. Introdução[1]

Este trabalho resulta do requerimento realizado pelo Instituto de Referência em Internet e Sociedade para sua admissão como '**Amicus Curiae**'[2], bem como do memorial apresentado nessa condição, com vistas a auxiliar o Supremo Tribunal Federal na apreciação da Ação Declaratória de Constitucionalidade (ADC) no. 51, ajuizada pela Federação das Associações das Empresas de Tecnologia da Informação - Assespro Nacional. A Ação visa analisar a pertinência do Decreto 3.810/2001, do artigo 237, II do Código de Processo Civil e dos artigos 780 e 783 do Código de Processo Penal, em especial no que diz respeito à cooperação jurídica internacional para medidas de obtenção de dados de comunicação privada entre usuários de aplicações de internet, direcionadas a sociedades empresárias sediadas e com estabelecimento no exterior.

Em relação à **conexão temática** entre as **especialidades** e fins **institucionais** do **Instituto de Referência em Internet e Sociedade - IRIS** e as matérias sob controvérsia e repercussão constitucional veiculadas pela ADC 51/2017, é importante enfatizar que a intervenção do IRIS como 'amicus curiae' e terceiro não interessado se justifica em função da relação da demanda com questões de fundo e procedimentos implicados na interface entre direito internacional e novas tecnologias. Desde 2015, estudos do IRIS têm examinado os principais perfis e condicionantes da governança global da Internet e aspectos da jurisdição, lei aplicável, reconhecimento de decisões estrangeiras e cooperação jurídica internacional, em relevante análise interdisciplinar envolvendo temas de novas tecnologias, direito internacional público e privado.

Questões sobre observância de mecanismos de cooperação jurídica, (e.g. cartas rogatórias, auxílio direto, assistência jurídica mútua) em litígios transfronteiriços da internet, além do incondicional respeito a direitos fundamentais do processo civil transnacional são justamente as que inspiram o alcance e a efetividade das medidas de obtenção de dados telemáticos e divulgação do teor de comunicações privadas entre usuários de aplicações de internet no estrangeiro - temas que suscitam, como sustentado adiante, cautela adicional interpretativa e aplicativa, pelo Supremo Tribunal Federal, de normas internacionais e domésticas. Nesse sentido, o IRIS reuniu os subsídios apresentados para a decisão da Ação Declaratória de Constitucionalidade nº 51, em 11 itens, aqui apresentados, além das conclusões oferecidas ao Supremo Tribunal Federal.

2. A internet e os novos conflitos de jurisdição - contextualização

A petição inicial da ADC 51/2017 apresenta, dentre seus eixos argumentativos, a premissa de que a sede de uma sociedade empresária deve ser o principal elemento de determinação da jurisdição[3] , especialmente nas situações em que judiciário e auxiliares

1 Estudo realizado sob a coordenação científica de Fabrício B. Pasquot Polido, Membro do Conselho Científico do **Instituto de Referência em Internet e Sociedade - IRIS** e coodernação de pesquisa de Odélio Porto Júnior. Contribuíram na qualidade de coautores para este trabalho Fabrício B. Pasquot Polido, Lucas Costa dos Anjos, Pedro Vilela e Odélio Porto Júnior. A pesquisa conta também com a colaboração e revisão de Luíza Brandão e Victor Vieira.

2 A função do ***amicus curiae*** é, essencialmente, emitir sua opinião em causas de relevância social, repercussão geral ou cujo objeto seja bastante específico, de modo que o magistrado necessite de apoio técnico. THEODORO, Humberto Jr. ***Curso de Direito Processual Civil - Volume 1***. 56ª edição .Rio de Janeiro: Editora Forense, 2015. p. 410.

3 Alex Mills, em sua doutrina, discute a existência de três tipos distintos de jurisdição: i) "jurisdiction to prescribe or legislate" ("jurisdição prescritiva", em tradução livre), que diz respeito aos limites da autonomia de um Estado para legislar acerca de determinada matéria; ii) "jurisdiction to adjudicate" ("jurisdição adjudicatória", em tradução livre), que refere-se aos limites do poder judiciário de um Estado, ou seja, os limites de sua competência para julgar casos relativos a sujeitos de direito localizados no exterior; e iii) "jurisdiction to enforce" ("jurisdição executória", em tradução livre), que relaciona-se aos limites do poder executivo do Estado, responsável pela aplicação da Lei. Neste caso, a petição inicial da ADC 51 refere-se ao terceiro tipo de jurisdição mencionado por Mills, ou seja, aos

da justiça pretendam obter o conteúdo de comunicações privadas que trafegam em aplicativos online. Contudo, para que essa premissa seja avaliada adequadamente, é necessário entender como a internet tem afetado a forma com que os Estados exercem suas jurisdições no século. XXI.

De início, parte-se da constatação de que a internet não pode ser mero elemento adicional ao debate sobre jurisdição, mas sim verdadeiro componente de fragmentação, o que tem desafiado o clássico modelo internacional vestifaliano[4] e os modos de cooperação internacional tradicionais.

A rede internacional ***Internet & Jurisdiction***[5] - que tem buscado promover o debate sobre esse tema com atores estatais, sociedade civil, empresas e academia, ao redor do mundo - afirma que as tensões jurídicas entre sistemas legais nacionais, baseados no princípio da territorialidade, emergentes em função da natureza transfronteiriça da internet, podem ser resumidas em dois desafios[6]:

1. Como preservar a natureza global da internet enquanto se respeitam os sistemas jurídicos nacionais?

2. Como combater os usos indevidos e abusos cometidos na internet enquanto se garante a proteção dos direitos humanos?

Na visão da Proponente, são, justamente, essas as questões de fundo que estão por trás das controvérsias levantadas pela ADC 51/2017. Ao mesmo tempo em que os mecanismos de persecução criminal e aplicação da lei devem ser respeitados, o Estado brasileiro, simultaneamente, deve assegurar que as soluções adotadas não ignorem o caráter transnacional da internet. Ademais devem ser respeitados os direitos fundamentais de usuários, especificamente as garantias civis que se encontram na base da privacidade, da proteção de dados pessoais e telemáticos, e da inviolabilidade do sigilo das comunicações privadas

Assim, é necessário reconhecer que os instrumentos atuais de cooperação jurídica internacional - administrativa e jurisdicional - ainda são ineficientes e incompletos, quando comparados ao volume de demanda exigida não somente no Brasil como nos outros países. Fortalece esse ponto de vista a pesquisa anual realizada pela Symantec, empresa de segurança digital com atuação em inúmeros países do globo, a observar que 62 milhões de pessoas experienciaram práticas de crimes cibernéticos no Brasil no ano

limites que existem para que o Brasil faça valer a nossa legislação interna no território estrangeiro onde for sediada a empresa envolvida em um processo cujo objeto é a obtenção do conteúdo de comunicações privadas online. MILLS, Alex. *Rethinking Jurisdiction in International Law*. In: *The British Yearbook of International Law*, Vol. 84, No. I, 2014. p. 194-195. Disponível em: <https://goo.gl/dg9hvL> Acessado em 12/03/2018.

4 O modelo internacional Westfaliano remonta à Paz de Westfália, instaurada pelos Tratados de Münster e Osnabrück, assinados em outubro de 1648, na Westfália, Alemanha. Esses tratados foram os instrumentos empregados para cessar a Guerra dos Trinta Anos, e resultaram no conceito moderno de "soberania", compreendida na época como necessário para a sobrevivência de um Estado. A soberania, nessa concepção, configura-se como um conceito simultaneamente político e jurídico, que confere a um Estado o poder absoluto sobre tudo e todos que estiverem em seu território, sendo que, segundo este conceito, todo Estado seria igualmente soberano e independente com relação aos demais (princípio da igualdade soberana de todos os Estados). GIANNATTASIO, Arthur. Roberto Capella. *O Direito Internacional entre Dois Pós-Modernismos: A Ressignificação das Relações entre Direito Internacional e Direito Interno*. In: *Revista Eletrônica do CEDIN*, v. 6, 2010, p. 42-90. Disponível em: <https://goo.gl/DCrJgT>

5 "Internet & Jurisdiction is the global multistakeholder policy network addressing the tension between the cross-border Internet and national jurisdictions. It facilitates a global policy process to enable transnational cooperation and preserve the global character of the Internet. Since 2012, Internet & Jurisdiction has engaged more than 100 key entities from different stakeholder groups around the world: states, Internet platforms, technical operators, civil society, academia, and international organizations. Internet & Jurisdiction helps catalyze the development of shared cooperation frameworks and policy standards that are as transnational as the Internet itself in order to promote legal interoperability and establish due process across borders." LA CHAPELLE, Bertrand de; FEHLINGER, Paul. *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*. Acessado em: 15/02/2018. 2016. p. 4. Disponível em: <https://goo.gl/uy7Fpe>.

6 Ibid, p. 6.

de 2017[7]. A partir desse dado pode-se inferir que há uma demanda, no mínimo, razoável pelo acesso à dados armazenados por provedores de aplicação situados no estrangeiro, já que muitas vezes as sedes desses provedores e unidades de processamento e guarda de dados (***data centers***) se encontram no exterior.

A esses elementos, acrescenta-se o fato de o Brasil ser um grande mercado consumidor de serviços online, com 99 milhões de usuários mensais no ***Facebook***[8]; 50 milhões de usuários mensais no ***Instagram***, sendo o segundo país em números totais[9]; e 120 milhões de usuários no ***WhatsApp***[10]. Parte da população jovem brasileira também integra significativo mercado de nativos digitais, o que caracteriza o conjunto dos usuários brasileiros como um enorme repositório de informações e dados pessoais.

Além disso, é razoável afirmar que, no contexto histórico[11] das negociações e entrada em vigor do Acordo de Cooperação Brasil-Estados Unidos (incorporado pelo Decreto nº 3.810/2001), os instrumentos ali previstos não foram planejados de modo a considerar o impacto que a internet, a velocidade de sua interações e o grande número de usuários da rede teriam sobre a dinâmica de litígios transfronteiriços e processos com conexão internacional em matéria civil, comercial e criminal.[12]

3. Esclarecimento sobre a noção de jurisdição, em particular "jurisdição prescritiva"

A jurisdição, de acordo com o sentido que lhe atribui o direito internacional clássico, "define os limites do poder dos coexistentes 'soberanos', em particular, o escopo de atividades regulatórias dos estados no direito internacional"[13]. Sua delimitação, contudo, abrange três de suas dimensões centrais, estabelecidas de acordo com um poder de elaborar e aplicar o direito nos limites do território de um Estado e endereçado a seus cidadãos e pessoas nele residentes ou domiciliadas: jurisdição prescritiva, jurisdição adjudicatória e jurisdição executiva. Essa divisão, que não é hermética ou estanque, considerado o objetivo de entrega do direito material, presta-se a dois propósitos distintos: primeiramente, o de situar o distintos níveis de discussão relativos aos casos/litígios de internet com conexão internacional, assim como seria, em relação mais ampla, a

7 "The Norton Cyber Security Insights Report is an online survey of 21,549 individuals ages 18+ across 20 markets, commissioned by Norton by Symantec and produced by research firm Reputation Leaders. The margin of error for the total sample is +/ -.7% . Data was collected Oct . 5 – Oct. 24, 2017 by Reputation Leaders".SYMANTEC CORPORATION. Norton Cyber Security Insights Report 2017 Global Results. 2018. Acessado em: 15/02/2018. Disponível em: <https://goo.gl/RC7q5i>

8 COSETTI, Melissa Cruz. Facebook revela dados do Brasil na CPBR9 e WhatsApp 'vira ZapZap'. Techtudo. 28/01/2016. Acessado em 20/02/2018. Disponível em: <https://goo.gl/g7Pm5p>

9 *Com 50 milhões de usuários, Brasil é segundo no ranking do Instagram.* Folha de S. Paulo. 28/10/2017. Acessado em 20/02/2018. Disponível em: <https://goo.gl/hgh3gol>

10 *WhatsApp chega a 120 milhões de usuários no Brasil.* O Estado de S. Paulo .29/05/2017. Acessado em 20/02/2018. Disponível em: <https://goo.gl/gJVGEF>

11 "De uma perspectiva histórica, as interações transfronteiriças eram raras, e ferramentas de cooperação jurídica internacional eram voltadas para tratá-las como exceções. Contudo, na Internet aberta, interações que transpõem os limites das fronteiras internacionais estão se tornando o novo normal" (tradução nossa). CHAPELLE, Bertrand de La, FEHLINGER, Paul. *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation.* In: *Global Commission on Internet Governance, Paper Series*: No. 28 - April 2016. p. 2. Disponível em: <https://goo.gl/PySHxo>

12 A Access Now mostra-se contrária ao modelo de MLATs empregados atualmente, e defendem a necessidade urgente de uma reforma em mecanismos dessa natureza. As críticas, em resumo, giram em torno de características como a morosidade do processo envolvido nos MLATs, bem como na falha do modelo em devidamente proteger a privacidade e as informações dos indivíduos. *The urgent need for MLAT reform*. Access Now. 12/09/2014. Disponível em: <https://goo.gl/dcqCWi>. *How to fix MLATs* — and a path toward resolving jurisdictional issues. Access Now. 23/05/2017. Disponível em: <https://goo.gl/JCNv5i>. Sobre este tema, a InternetLab também argumenta, em seu parecer para a Suprema Corte dos Estados Unidos da América, que são necessárias reformas no modelo de MLATs utilizado atualmente, para que possa adequar-se melhor ao cenário internacional atual. Disponível em: <https://goo.gl/V5htVv>. p. 31-37.

13 MILLS, Alex. Rethinking Jurisdiction in International Law. In: *British Yearbook of International Law*, volume 84, n. 1, 1 2014, pp. 187–239, especialmente p. 194.

análise de questões de lei aplicável aos casos pluriconectados[14], jurisdição e competência internacional dos tribunais nacionais e reconhecimento de decisões estrangeiras. Em segundo lugar, ela permite esclarecer o grau de complexidade em torno dos casos inseridos no ciberespaço.

No caso ***Microsoft Ireland vs. USA***, da Suprema Corte dos Estados Unidos, e apresentado na Ação Declaratória de Constitucionalidade nº 51 (número único 00144965220171000000), o termo "jurisdição" refere-se especificamente ao seu aspecto prescritivo relacionado à previsão, pelos Estados, de leis substantivas aplicáveis em determinadas circunstâncias para regular fatos no seu território, com seus nacionais ou ainda cujos efeitos possam sentir.[15] Nesse sentido, a expressão pode também ser interpretada, nos termos aplicados ao Direito Internacional privado, como "lei aplicável" ou "jurisdição substantiva"[16].

A jurisdição prescritiva, assim, denota o poder do Estado de legislar e regular materialmente os fatos, situações e relações jurídicas que se manifestam em seu território, e excepcionalmente fora dele, como em matéria criminal, tributária, antitruste, ambiental e anticorrupção. Como será examinado, o Art.11 do Marco Civil, por exemplo, contempla normas com suportes fáticos submetendo determinadas relações jurídicas envolvendo pessoas jurídicas e físicas à **regulação substantiva** da lei brasileira, nada referindo-se, por seu turno, à "jurisdição adjudicatória", i.e. ao poder-julgar dos tribunais brasileiros; esse campo, especificamente, seria adstrito às questões de competência internacional, como regulados por normas de tratados e convenções e normas processuais internas (cf. Art. 13, sobre a determinação da jurisdição civil e Arts. 21 e ss do CPC de 2015, sobre as regras de competência internacional dos tribunais brasileiros)[17].

A essa altura de maturidade processual no direito brasileiro e no tratamento do contencioso instaurado perante tribunais superiores - STF e STJ, seria inadmissível uma confusão entre questões de lei aplicável e competência internacional dos tribunais para solução de disputas e casos pluriconectados da Internet[18].

14 Admite-se, aqui, a expressão "casos pluriconectados" ou "casos com conexão internacional", conforme tradicionalmente adotada no direito internacional privado para designar conjunto de fatos, situações e relações jurídicas contendo elementos de estraneidade, vinculados a distintos sistemas jurídicos em contato. Sobre isso, cf. POLIDO, Fabrício B. P. *Direito Internacional Privado nas Fronteiras do Trabalho e Novas Tecnologias*: ensaios e narrativas na era digital. Rio de Janeiro: Lumen Iuris, 2018, p.97 e ss.

15 WILSKE, Stephan; SCHILLER, Teresa. International Jurisdiction in Cyberspace: Which States May Regulate the Internet? Federal Communications Law Journal, vol. 50, issue 1, pp.117 – 178, 1997, p. 127.

16 ***Ibidem.***

17 Sobre o tema, cf. POLIDO, Fabrício B.P. Comentários aos arts. 21-40. In: STRECK, Lenio Luiz; NUNES, Dierle; CUNHA, Leonardo C. (org.). *Comentários ao Código de Processo Civil*. 2. ed. São Pau lo: Saraiva, 2017. p. 73-108 (examinando aspectos da competência internacional do juiz brasileiro e regimes e mecanismos de cooperação jurídica internacional no CPC brasileiro).

18 Essa, contudo, parece não ser a percepção recente em julgados do STJ, particularmente quanto à confusão feita entre lei aplicável, jurisdição e cooperação jurídica internacional, inclusive com questionável "dispensa" de atos de assistência jurídica mútua e cooperação, como se fossem opcionais para as autoridades judiciárias e administrativas brasileiras. A esse respeito, cf. criticamente, STJ, RMS 44.892/SP, Rel. Ministro Ribeiro Dantas, Quinta Turma, acórdão de 5 de abril de 2016, DJe 15.04.2016 (*"4. Por estar instituída e em atuação no País, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pelo juízo"*); STJ, Recurso em Mandado de Segurança n. 55.109/PR, Rel. Min.Joel Paciornik, acórdão de 17.12.2017 (MPF vs. Yahoo!, caso *Castanheira-Brasil 247*), mantendo uma tese de que a quebra de sigilo de dados telemáticos mantidos no estrangeiro, como comunicação por e-mail e em redes sociais, independem de procedimentos de cooperação internacional. Se fosse esse o argumento, apenas em função da sede da empresa, do setor (indústria da Internet), por que não seria possível admitir a mesma "dispensa de cooperação" para que uma subsidiária brasileira de uma instituição financeira na Espanha (e.g. Santander) seja obrigada a divulgar/fornecer/entregar dados bancários de um nacional ou residente brasileiro em conta corrente mantida em uma agência no exterior? Assim como dados bancários e o sigilo são sensíveis no curso do contencioso civil/criminal, os dados telemáticos deveriam receber o mesmo tratamento de proteção.

4. Critérios de determinação da lei aplicável - Uma perspectiva internacional

Chapelle e Fehlinger afirmam que há pelo menos quatro fatores territoriais de determinação de qual a lei aplicável aplicável a um determinado caso envolvendo a internet[19]:

1. A localização do usuário;
2. A localização dos servidores que armazenam os dados;
3. O local onde a empresa que fornece os serviços foi constituída (sede);
4. E, potencialmente, a localização dos atores que realizam os registros de nomes de domínio (.com; .org; .net ; .br; entre outros);[20]

Assim, as dificuldades na escolha sobre qual deve ser o critério determinante da lei aplicável, - além de questões de jurisdição - para casos envolvendo empresas de tecnologia da informação, não têm sido exclusividade do Judiciário brasileiro. A partir desses critérios, decisões judiciais diferentes têm sido proferidas pelos tribunais estatais ao redor do mundo. Nesse sentido, iremos explicar como determinados julgados de outros países utilizaram os critérios de 1 a 3, os mais recorrentes, para determinar qual a jurisdição aplicável a um caso concreto. Desse modo, esperamos demonstrar como o foco em um dos critérios pode levar a resultados jurídicos diversos, e assim melhor instruir V.Exas. no julgamento da ADC 51/2017.

4.1. A localização do usuário: o caso Zippo Manufacturing

Entre os casos mais célebres no debate sobre o estabelecimento de jurisdição em relações envolvendo a internet é o da Zippo Manufacturing Company vs. Zippo Dot Com[21]. Ainda no final dos anos 1990, essa demanda ofereceu alguns caminhos para questões até então pouco comuns, como a determinação de onde está a jurisdição para uma disputa na internet. O tribunal distrital da Pensilvânia, que proferiu a decisão, dividiu as atividades da internet em três tipos: ativa, passiva e interativa.

Segundo o precedente estabelecido, um réu ***ativo*** seria aquele que deliberadamente faz uso extensivo da internet, por exemplo, por meio da celebração de contratos com residentes de outra jurisdição, e esses contratos exigem a transmissão repetida de arquivos de computador pela internet. Nesses casos, o réu era suscetível à jurisdição dos lugares que afetou deliberadamente. Um site ***passivo***, por sua vez, seria meramente informativo e não solicitava nem esperava atividades nos e dos locais que atingia; seus operadores não poderiam ser levados a juízo nesses locais.

O meio termo seria o site ***interativo***. Nesses casos, o precedente aqui firmado visava a examinar o nível de interatividade e natureza comercial da troca de informações que ocorre no site, de forma a determinar o quão razoável e esperado seria para os criadores do site serem processados naquele local.

19 LA CHAPELLE, Bertrand de; FEHLINGER, Paul. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. Acessado em: 15/02/2018. 2016. p. 7. Disponível em: <https://goo.gl/qAisYB>.

20 No Brasil o responsável pelo registro do ".br" é o *Registro.br*, órgão executivo do *Núcleo de Informação e Coordenação do Ponto BR* - NIC.br. Disponível em: <http://www.nic.br/quem-somos/>

21 ZIPPO MANUFACTURING COMPANY, Plaintiff, v. ZIPPO DOT COM, INC., Defendant. Nº. 96-397. *Memorandum Opinion*. 16/01/1997. Acessado em: 26/03/2018. Disponível em: <https://goo.gl/DUXEbG>

O teste do caso Zippo, apesar de claro e simples, dividindo os sites da internet em três categorias e permitindo que a questão jurisdicional fosse decidida com base nesses locais, é hoje um método ultrapassado, como se pretende demonstrar. Por meio da complexificação dos relacionamentos estabelecidos na rede mundial de computadores, bem como o crescimento das interações entre provedores, usuários e tribunais de diferentes jurisdições, esse teste tem sido insuficiente para as questões transfronteiriças hodiernas envolvendo a internet.

a. Zippo Manufacturing Company vs. Zippo Dot Com e o teste trifásico

A Zippo Manufacturing era uma corporação da Pensilvânia, com seu principal local de negócios no município de Bradford,onde fabricava isqueiros de cigarro "Zippo". Já sua contraparte, a empresa Zippo Dot Com, tinha sede em Sunnyvale, Califórnia. Ela operava um site na internet e um serviço de notícias, para os quais obteve o direito exclusivo de usar os nomes de domínio "zippo.com", "zippo.net" e "zipponews.com". O site da Zippo Dot Com continha informações sobre a empresa, anúncios e um aplicativo para seu serviço de notícias, que oferecia acesso diferentes grupos de notícias online. O aplicativo atribuía ao assinante uma senha, que o permitia visualizar e/ou baixar as mensagens armazenadas em seu servidor na Califórnia, do grupo de notícias correspondente a sua assinatura.

Todos os escritórios, funcionários e servidores da Zippo Dot Com estavam localizados na Califórnia, sem qualquer atividade na Pensilvânia, exceto o contato com eventuais clientes residentes naquele estado (aproximadamente dois por cento do total da empresa, 3.000 assinantes). A base das alegações de marca registrada seria o uso da palavra "Zippo" pela Zippo Dot Com nos nomes de domínio que detinha, em vários locais em seu site e no título de mensagens de grupos de notícias da internet postados por assinantes da Zippo Dot Com, o que poderia causar confusão em seus consumidores.

O acórdão desse caso propõe um teste de três fases para determinar se o exercício de jurisdição sobre um réu não residente (no estado de exercício da mesma) é apropriado: 1) o réu deve ter "contatos mínimos" suficientes com o Estado do foro, 2) a reivindicação feita contra o réu deve surgir desses contatos, e 3) o exercício da jurisdição deve ser razoável. Ou seja, há contatos mínimos se o réu propositalmente o estabeleceu com o estado do foro.

Além disso, os réus que se estendem além de um estado e criam relações e obrigações contínuas com os cidadãos de outro estado estariam sujeitos à regulamentação e às sanções de outro estado por conseqüências de suas ações comerciais. Já a razoabilidade decorre do fato de que a conduta do réu e sua conexão com o estado do foro são tais, que ele deveria razoavelmente esperar ser levado ao tribunal lá. Isso protegeria os réus de serem forçados a responder por suas ações em uma jurisdição estrangeira baseada em contatos aleatórios, fortuitos ou praticamente inexistentes.

b. Obsolescência anunciada: por que o caso Zippo é ultrapassado

O teste Zippo funcionou bem inicialmente, em especial naquele contexto dos primórdios de expansão da rede, com sites que eram claramente ativos dentro de uma jurisdição, ou totalmente passivos e informativos em outra, sem nenhum elemento de interatividade. No entanto, as demandas que tinham que lidar com a crescente intera-

tividade das redes, havia poucos parâmetros para embasamento objetivo das decisões judiciais.

O teste Zippo ainda adotou abordagem de tamanho único para todas as disputas online, sendo que essas cresciam em forma, natureza e complexidade: violações de cláusulas contratuais, privacidade, publicidade, hackeamento ou apropriação indébita de dados, violação de direitos autorais, cobrança de dívidas, entre outras especificidades que deveriam ser consideradas para além dos níveis de interação entre provedor e usuário.

Outro problema com a escala de interatividade da Zippo, do ativo ao passivo, é que ela pode descrever falsamente a natureza da internet e das tecnologias de informação e comunicação, que podem ser bastante distintas entre si. Cada uma dessas tecnologias é empregada hodiernamente de forma diferente e requer análise jurisdicional própria, dada suas especificidades técnicas e operacionais. Além disso, muitas das disputas envolvendo a internet vão além da classificação clássica e tripartite do caso Zippo. Invasões e violações de privacidade, por exemplo, podem surgir sem o envolvimento de um site. Essas questões evidenciam a obsolescência do caso Zippo.

c. Critérios para além dos contatos com a jurisdição de localização do usuário

Atualmente, quando os tribunais se deparam com algumas disputas excepcionais, faz mais sentido analisar se um provedor segmentou especificamente determinado usuário ou jurisdição em sua atuação. Particularmente em casos de difamação, por exemplo, o teste por meio desse direcionamento se enquadra adequadamente à solução do feito, como se por perceber em Calder v. Jones[22], caso em que a Suprema Corte dos Estados Unidos permitiu que um processo contra um jornal fosse levado ao estado de residência do autor quando o jornal visitou ativamente aquele estado, conduziu pesquisas nesse território e publicou seu relatório sabendo que seus efeitos seriam maiores naquele local.

O caso Sioux Transportation v. XPO Logistics[23], por sua vez, envolveu uma alegada difamação em dois posts online após disputa comercial entre as duas empresas. Discutiu-se que a Sioux tinha poucas atividades em Arkansas, o estado natal da XPO, o que inviabilizaria a jurisdição de seus tribunais. A XPO argumentou que as postagens da Sioux, respondendo às postagens da XPO, contavam como contatos deliberados com o Arkansas, o que apoiaria o exercício de sua jurisdição.

Em vez de recorrer ao teste da Zippo, a corte examinou criticamente esse precedente e o considerou inadequado para a internet hodierna:

> 'A internet passou por uma tremenda mudança desde que a Zippo foi decidida em 1997', afirmou o tribunal. 'A computação em nuvem eliminou a necessidade de baixar arquivos em muitas situações, a tecnologia baseada em localização fez interações on-line que anteriormente existiam apenas no ciberespaço mais intimamente ligado a localizações geográficas específicas e o nível de interação do usuário com sites explodiu com

22 CALDER, Petitioner, v. JONES, Respondent. Nº. 82-1401. *Appeal from the Court of Appeal of California*. 20/03/1984. Acessado em: 26/03/2018. Disponível em: <https://goo.gl/wff9c2>

23 SIOUX TRANSPORTATION, INC, Plaintiff, v. XPO LOGISTICS, INC. ET AL, Defendants. Nº. 5:2015cv05265. *Memorandum Opinion and Order granting Motion to Dismiss Case Without Prejudice*. 22/12/2015. Acessado em: 26/03/2018. Disponível em: <https://goo.gl/sLEYdz>

mídia social. Tudo isso põe em dúvida a utilidade moderna da estrutura simplista tripartite do teste Zippo: a transmissão de arquivos de computador pela internet talvez não seja mais uma medida precisa do contato de um site com um estado do foro.'[24]Como observado no gráfico, a situação do Brasil, em termos de adoção do IPv6 é similar a de países com considerável penetração da internet e pertencentes ao grupo de países desenvolvidos do hemisfério norte e países em desenvolvimento do hemisfério sul. Em estimativa semelhante, o Asia-Pacific Network Information Centre aponta uma capacidade de 20,97% de IPv6 para o Brasil, o que posiciona o país em 14º lugar no ranking desse tipo de conexão[25].

4.2. A localização dos servidores: o caso *United States v. Microsoft Inc.* (Microsoft - Ireland)

O caso Estados Unidos/Microsoft (também conhecido como "Microsoft Irlanda") foi levado à apreciação da Suprema Corte dos EUA em 2017 e está previsto para ser julgado em junho de 2018. Nele, buscará responder se um mandado (*warrant)*, emitido com base nas normas do *Stored Communication Act* (SCA)[26], obrigaria as empresas dos EUA a fornecer informações sob seu controle, mas que estão armazenadas fora do país, especificamente em unidades de guarda e processamento de dados (data centers), localizados na Irlanda.

A disputa iniciou-se em 2013 quando um juiz federal (*Southern District of New York)* concedeu um mandado (*warrant*), com base no Parágrafo 2703[27] do *Stored Communications Act* (SCA) de 1986, para que autoridades de investigação obtivessem os conteúdos de emails e dados associados de um usuário da Microsoft suspeito de tráfico de drogas. Após esta decisão, a empresa forneceu somente os metadados relativos à conta do usuário, pelo fato de eles estarem armazenados nos EUA. Contudo, a Microsoft alegou que não poderia fornecer o conteúdo dos emails, porque ditas informações estavam localizadas em um servidor na Irlanda, e que as normas da SCA não teriam aplicação extraterritorial.

A recusa da empresa de fornecer o conteúdo dos *emails* não foi aceita pelo tribunal acionado em primeira instância, que condenou a Microsoft por desobediência a uma ordem judicial (*civil contempt*).[28] A Requerida então recorreu da decisão ao Tribunal de Apelações para o Segundo Circuito (*United States Court of Appeals for the Second Circuit),* que deu provimento ao recurso afirmando que: (1) a SCA era silente quanto ao seu alcance extraterritorial, devendo, portanto, ser interpretada restritivamente, conforme já estabelecido na jurisprudência da Suprema Corte[29]; e que (2) o elemento territorial

24 Ibid, em tradução livre.

25 Ranking produzido pela Asia-Pacific Network Information Centre. Informações disponíveis em: <https://stats.labs.apnic.net/ipv6>. Também disponibilizadas pelo site do ipv6.br: <http://ipv6.br/>.

26 O *Stored Communication Act* é o Título II da Lei *Electronic Communications Privacy Act* (ECPA) ,que foi aprovada em 1986. A EPCA buscou atualizar as normas de proteção às comunicações privadas realizadas por meio de computadores e outros meios eletrônicos de comunicação. US DEPARTMENT OF JUSTICE. *Justice Information Sharing - Electronic Communications Privacy Act of 1986 (ECPA)*. 30/07/2013. Acessado em: 01/03/2018. Disponível em: <https://goo.gl/hdv2on>

27 Esta seção protege comunicações privadas armazenadas eletronicamente de serem acessadas indiscriminadamente por autoridades públicas, estabelecendo critérios como a exigência de mandado judicial (warrant).18 U.S. Code § 2703 - Required disclosure of customer communications or records. Acessado em: 01/03/2018. Disponível em: <https://goo.gl/ojNv2A>

28 "Even when applied to information that is stored in servers abroad, an SCA Warrant does not violate the presumption against extraterritorial application of American law. Accordingly, Microsoft's motion to quash in part the warrant at issue is denied." UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK. Juiz James C. Francis IV. p. 26. Acessado em: 01/03/2018. Disponível em: https://goo.gl/7YrorZ

29 Ver os casos in *United States v. Morrison;*, *Kiobel v. Royal Dutch Petroleum Co.;* and *RJR Nabisco v. European Community*.

relevante para se determinar qual o alcance do mandado seria o de verificar onde os dados requisitados estavam armazenados. Assim, um mandado emitido nos EUA e que busca dados na Irlanda acabaria por operar neste país, sendo portanto uma aplicação extraterritorial da lei.[30]

a. Alegações do Departamento de Justiça dos EUA à Suprema Corte

Após o julgamento de segunda instância, o *Department of Justice* (DoJ) questionou a interpretação dada ao *Stored Communications Act* de 1986 mediante interposição de recurso de revisão junto à Suprema Corte (*judiciary review*), que aceitou o caso em outubro de 2017. Tendo em vista a relevância do caso para a compreensão das questões de repercussão constitucional na ADC 51/2017, pendente de julgamento pelo STF, as linhas a seguir objetivam explicitar alguns pontos relevantes relacionados à determinação da jurisdição.

O DoJ argumenta em sua petição (*merits brief*)[31] que o Parágrafo 2703 do SCA de 1986 regula a divulgação/quebra de sigilo da informação eletrônica (*disclosure*) e que este ato deve ocorrer no território dos EUA, e não na Irlanda. Assim, o acesso ao servidor localizado em outro país configuraria "mera conduta acessória", que não seria o objeto principal de regulação da referida lei. Para embasar esse ponto, o DoJ menciona que o termo "*disclosure*" é usado frequentemente ao longo do texto normativo, e que a análise histórica do processo legislativo da SCA também concentrar-se-ia no ato de exibição/divulgação, e não no ato de armazenamento. Igualmente, o DoJ acrescenta que a Microsoft poderia, inclusive, cumprir com o mandado por meio ações que acontecem exclusivamente nos EUA[32], por intermédio de seus softwares de gerenciamento de dados.

Além disso, o Departamento de Justiça busca rebater a interpretação utilizada pela *Court of Appeals* de que a Microsoft Inc., ao cumprir um mandado para quebra de sigilo de comunicação eletrônica, estaria a cometer uma violação de privacidade extraterritorial. O argumento da instância recursal baseou-se na ideia de que a Microsoft agiria como agente governamental que apreende (*seize)* dados armazenados em jurisdição estrangeira.

Contrariamente, o DoJ proclama que a Microsoft não age como agente governamental porque ela somente teria acesso a uma informação armazenada em seus próprios arquivos. E acrescenta que, mesmo que se pudesse considerá-la como agente do governo, o ato de acessar o servidor localizado no estrangeiro não poderia ser considerado uma apreensão (*seizure*) extraterritorial[33], porque os dados já estão sobre a custódia e controle da empresa. E que nem mesmo se configuraria como uma busca (*search*) extraterritorial, no sentido de uma violação de privacidade considerada razoável[34], porque não ocorre violação de privacidade em relação ao ato de transferência dos dados de seus servidores de um país a outro, algo que a empresa já faz rotineiramente para viabilizar seus serviços. Assim, mesmo que venha a ocorrer uma violação de privacidade,

30 United States Court of Appeals for The Second Circuit. Docket No. 14- 2985 - In the Matter of a Warrant to Search a Certain E- Mail Account Controlled and Maintained by Microsoft Corporation. 14 de Julho de 2016.Acessado em: 01/03/2018. Disponível em: https://goo.gl/Kz7hWp

31 USA, Petitioner v. MICROSOFT CORPORATION, Respondent. *Brief for the United States* - Nº 17-2.Acessado em: 01/03/2018. Disponível em: <https://goo.gl/X5kVUj>

32 Ações que representantes da Microsoft realizariam para acessar o servidor da empresa e transferir os dados requeridos às autoridades.

33 'For purposes of the Fourth Amendment, a 'seizure' of property occurs where 'there is some meaningful interference with an individual's possessory interests in that property'." Ibid, p. 30.

34 A "search" is an infringement on "an expectation of privacy that society is prepared to consider reasonable." Jacobsen, 466 U.S. at 113. Ibid, p.31.

essa conduta seria realizada pela autoridade governamental no território dos EUA, no momento de exibição do conteúdo dos dados.

O DoJ afirma que, caso prevaleça tese da localização do dado como critério determinante de jurisdição, este entendimento será prejudicial às capacidades de investigação e julgamento das autoridades dos EUA. Como a localização dos dados é decidida exclusivamente pela empresa, um decisão de viés econômico poderia inutilizar as previsões do *Stored Communications Act*, mesmo que o fato investigado envolva uma comunicação entre dois cidadãos residentes nos Estados Unidos. Além disso, o DoJ ressalta que outros modelos de negócio poderiam ser prejudicados se a teoria da localização do dado fosse adotada, como o caso da Google Inc., que pode armazenar os dados de um único usuário em diversos servidores espalhados pelo mundo, podendo, até mesmo, distribuir o armazenamento de um único email em servidores diferentes, com o texto arquivado em um local e os anexos em outro.

Acrescenta que os mecanismos de cooperação jurídica internacional estabelecidos em MLATs não seriam uma alternativa efetiva. Primeiro, porque esses acordos não são universais, tendo os EUA assinado MLATs com menos da metade de todos os países do mundo. Segundo, porque o processo, na maioria dos casos, é: (1) lento, podendo levar meses ou anos; e (2) incerto, pois o Estado receptor do pedido tem certa discricionariedade[35] para recusá-lo. E (3), porque um provedor de serviços online pode ter a prática de mudar constantemente a localização dos dados dos usuários, tornando difícil ou até impossível determinar a qual país deve ser encaminhado o pedido de cooperação em determinado momento[36].

O DoJ defende, ainda, que a aplicação do Parágrafo 2703 da SCA respeita os tratados internacionais dos quais os EUA são signatários. A Convenção de Budapeste sobre Cibercrime, em seu art. 18, estabelece que os estados partes devem empoderar suas autoridades competentes para que obriguem um fornecedor de serviços a entregar dados informáticos que estejam sobre sua posse ou controle.[37]

O DoJ alega, por fim, que diversos países não restringem sua capacidade de demandar dados armazenados digitalmente em outra jurisdição, citando um estudo comparativo de Maxwell & Wolf, de 2012. Essa pesquisa afirma que, entre Estados Unidos, Austrália, Canadá, Japão e outros seis países europeus, somente dois deles estabelecem, em alguns casos, a localização física dos dados como critério limitador do acesso de autoridades à informações eletrônicas.[38] E que, para os demais países do estudo, a exigência de quebra de sigilo dos dados localizados no estrangeiro é permitida desde que haja algum elemento que conecte o caso à jurisdição do país demandante,

35 Cabe acrescentar que a discricionariedade mencionada não se resume a mera decisão arbitrária do Estado receptor do pedido - a recusa mostra-se possível em casos nos quais o cumprimento do pedido viole a Ordem Pública do Estado receptor. Nesse sentido, enuncia o Artigo V, 3, do Decreto nº 3.810/2001: "As solicitações serão executadas de acordo com as leis do Estado Requerido, a menos que os termos deste Acordo disponham de outra forma. O método de execução especificado na solicitação deverá, contudo, ser seguido, exceto no que tange às proibições previstas nas leis do Estado Requerido". Decreto nº 3.810, de 2 de maio de 2001. Disponível em: <https://goo.gl/oiE1G3>

36 É importante ressaltar que, no Direito Internacional Privado, há mecanismos para sancionar ou dissuadir a escolha indiscriminada de foro, ou o deslocamento de jurisdição com efeito de elisão ou fraude à lei. No caso da fraude à lei, quando detectada como conduta das partes, leva à desconsideração do Direito estrangeiro aplicável.

37 "Artigo 18º - Injunção. Cada Parte adoptará 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 controlo 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 controlo, relativos aos assinantes e respeitantes a esses serviços". CONVENÇÃO SOBRE O CIBERCRIME - Budapeste, 23/11/2001. Acessado em: 05/03/2018. Disponível em: <https://goo.gl/twrwQu>

38 " MAXWELL, Winston; WOLF, Christopher. *A Global Reality: Governmental Access to Data in the Cloud 2* (July 18, 2012). A Hogan Lovells White Paper (international law firm). 18/07/2012. Acessado em: 05/03/2018. Disponível em: <https://goo.gl/TA33bN>

como a presença da empresa no seu território.

b. Defesa apresentada pela Microsoft à Suprema Corte

A Microsoft alega, em suas contrarrazões (*brief in opposition*),[39] que a Suprema Corte não deveria admitir o caso, baseando-se em três argumentos. O primeiro estabelece que é competência do Congresso dos Estados Unidos decidir sobre a necessidade de modernização do *Stored Communications Act*, processo legislativo este que já está em curso. O segundo sustenta que o tribunal de segunda instância decidiu corretamente, seguindo o teste, desenvolvido pela própria Suprema Corte em seus precedentes, sobre critérios definidores da aplicação extraterritorial de determinada lei[40]. E o terceiro refere-se ao fato de que ainda não existem julgados dos tribunais (Courts of Appeals) com interpretações divergentes quanto à aplicação extraterritorial da SCA, a fim de que se configure um dos requisitos normalmente utilizados pela Suprema Corte antes de aceitar um caso, o que é denominado de *circuit split*.

Em breve análise histórica do contexto de elaboração legislativa da SCA na década de 1980, a Microsoft afirma que o Congresso não teria como prever o crescimento exponencial que internet sofreu nos últimos anos, e tampouco vislumbraria o surgimento de atuais serviços de armazenamento em nuvem, com o estabelecimento de servidores em diversos países. Não seria possível conceber que o legislador tivesse a intenção de atribuir efeitos extraterritoriais às normas da SCA.

Acrescenta a defesa da empresa que, ao se utilizar o teste do caso *Morisson v. National Australia Bank* - que estabelece que as leis federais estadunidenses devem ser interpretadas de forma restritiva, caso não seja explícita a sua aplicação extraterritorial -, verifica-se que o critério adotado pela SCA é do local de **armazenamento** dos dados e de sua proteção, e não o local no qual ocorrerá o ato de divulgação ou de quebra de sigilo/revelação dos dados pelas autoridades. Essa interpretação fora justamente a adotada pelo Tribunal de Apelações para o Segundo Circuito (*Second Circuit Court of Appeals*). Assim, se o escopo da lei é a de alcançar comunicações privadas armazenadas eletronicamente, a conduta relevante seria o ato de **apreensão** das comunicações, que ocorre justamente sob a jurisdição onde está localizado o servidor.

Segundo a Microsoft, estaria correta a decisão da segunda instância que evitou posteriores tensões internacionais que acabaram por se manifestar quando da prolação da decisão do juiz federal de primeira instância, que se posicionou pela aplicação extraterritorial da SCA de 1986. Isso, porque o Comissário Europeu de Justiça, o governo da Irlanda e alguns membros do Parlamento Europeu se pronunciaram publicamente denunciando violações de soberania acarretadas pela decisão.

A empresa afirma ser precipitado levar o caso até a Suprema Corte, pois ainda não há nenhum outro julgado semelhante nos demais tribunais federais que represente uma divergência jurisprudencial, um dos principais requisitos para que um caso seja admitido pela Suprema Corte. Seria necessário, portanto, aguardar novos casos envolvendo inclusive outras empresas de tecnologia, para que a Corte tivesse subsídios suficientes para avaliar a extraterritorialidade do *Stored Communications Act*.

Por fim, a Microsoft enfatiza que o Congresso dos EUA debate projetos de lei que

39 UNITED STATES OF AMERICA, Petitioner v. MICROSOFT CORPORATION, Respondent. *Brief in Opposition*. 2017. Acessado em: 05/03/2018. Disponível em: <https://goo.gl/pnz1Wo>

40 SUPREME COURT OF THE UNITED STATES .*MORRISON et al. v . NATIONAL AUSTRALIA BANK LTD. et al.* 561 U.S. 247 (2010).18/07/2012. Acessado em: 05/03/2018. Disponível em: <https://bit.ly/2GbTd08>

solucionarão a questão, como o I*nternational Communications Privacy Act,* o *Email Privacy Act* e o *Cloud Act*. Desse modo, faria mais sentido que o Poder Legislativo tomasse a iniciativa de adotar soluções inovadoras, quando em comparação com os remédios jurisdicionais disponíveis. Assim, processo legislativo teria maior capacidade de estabelecer equilíbrio entre as necessidades das forças policiais estadunidenses e os interesses de outros países soberanos.

c. The Clarifying Overseas Use of Data Act (CLOUD ACT)

É relevante apontar que tanto os representantes do governo quanto os da Microsoft indicaram concordar, na audiência para sustentações orais na Suprema Corte[41], que o Congresso dos EUA seria o mais apto a solucionar a questão. Ademais, as partes indicaram que ambas apoiam o projeto de lei denominado *CLOUD Act*, *Clarifying Overseas Use of Data*, que foi apresentado em fevereiro por senadores democratas e republicanos.[42] Este projeto foi apressadamente aprovado pelo Congresso em 23/03/2018, e assinado pelo presidente Trump no mesmo dia, devido ao fato de ter sido inserido em conjunto com a lei orçamentária anual de 2018 (*omnibus spending bill*)[43], que, caso não fosse aprovada, ameaçava gerar uma crise no governo federal por falta de recursos.

Não houve discussão acerca do Cloud Act, como projeto individual, em nenhuma das casas do Congresso. Desse modo, ainda é incerto se a recente aprovação terá um revés, ou se ela fará com que a Suprema Corte deixe de julgar o caso *United States v. Microsoft*. Apesar disso, ainda é de suma importância que expliquemos como essa lei busca solucionar o problema de jurisdição discutido na Suprema Corte.

O CLOUD Act lida com duas questões básicas: (1) se autoridades estadunidenses podem acessar dados armazenados no exterior; (2) e em quais condições outros países podem requisitar dados de empresas sediadas nos EUA.

Quanto à primeira questão, o PL propõe alterar a *Stored Communications Act* para que um provedor de comunicações eletrônicas ou serviço de computação remota tenha a obrigação de fornecer os dados armazenados sob sua posse, custódia ou controle (*possession, custody or control*), em caso de mandado judicial, independentemente de onde os dados estejam armazenados. Alguns juristas afirmam que, antes da aprovação, o projeto estava em consonância com a jurisprudência da Suprema Corte, principalmente em relação ao caso *United States v. Bank of Nova Scotia*, o qual permitiu com que bancos nos EUA sejam intimados para apresentar documentos (*subpoen*a) que estão no exterior, desde que eles estejam sobre sua posse, custódia ou controle.[44]

A lei também cria mecanismos para que as empresas possam contestar ou alterar os mandados judiciais das autoridades estadunidenses, caso o alvo da quebra de sigilo não seja um cidadão dos EUA e haja risco relevante de que o ato viole as leis de outro país. Adicionalmente, a lei busca reforçar mecanismo já existente no ordenamento jurídico, denominado *comity analysis*[45], o qual estabelece que os tribunais devem buscar

41 UNITED STATES, Petitioner, v. MICROSOFT CORPORATION, Respondent. Nº. 17-2. *Oral argument before the Supreme Court of the United States*.27/02/2018. Acessado em: 20/02/2018. Disponível em: <https://goo.gl/aDrz8q>

42 115th CONGRESS - THE SENATE OF THE UNITED STATES. S.2383/H.R. 4943. *The Clarifying Overseas Use of Data* (CLOUD ACT). 2018. Acessado em: 22/03/2018. Disponível em: <https://goo.gl/4gn81j>

43 WATTLES,Jackie. *Microsoft's epic court battle with DOJ is coming to an end*. CNN Tech. 23/03/2018. Acessado em: 27/03/2018. Disponível em: <https://cnnmon.ie/2DZeKXV>

44 WOODS, Andrew Keane; SWIRE Peter. *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems.* Lawfare Blog. 06/02/2018. Acessado em: 22/03/2018. Disponível em: <https://bit.ly/2HW2kCo>

45 "Comity, in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other […] it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of

medir os possíveis impactos de um ato ou decisão extraterritorial, na soberania e nas relações entre os países, caso a medida seja aplicada.

Já em relação à segunda questão, quanto aos pedidos de quebra de sigilo feitos por governos estrangeiros, a lei busca facilitar a cooperação internacional. A legislação americana atual impede que as empresas estadunidenses obedeçam certos pedidos feitos pelas autoridades judiciárias de países estrangeiros. A lei alterada diversas partes do *Electronic Communications Privacy Act*, permitindo que as empresas dos EUA obedeçam ordens judiciais estrangeiras de quebra de sigilo de dados, interceptações telemáticas, entre outros. Contudo, essa previsão só será válida para países que firmarem um acordo internacional com EUA, cumprindo certos requisitos estabelecidos pelo Executivo.

O Cloud Act estabelece como condições[46], resumidamente, que o Estado estrangeiro deve ter garantias processuais e materiais robustas de proteção à privacidade, aos direitos civis, e aos demais direitos humanos de seus cidadãos; que os procedimentos sejam supervisionados pelo Poder Judiciário, ou outra autoridade independente; que não seja violada a liberdade de expressão; e que o Estado adote procedimentos para prevenir com que cidadãos, pessoas naturais com residência permanente, ou pessoas jurídicas localizadas nos EUA sejam alvo de coleta de dados das autoridades governamentais.

Na hipótese de um país se qualificar para o acordo, não seria necessário que todo mandado de quebra de sigilo, ou outra ordem judicial semelhante, emitida por um tribunal competente, tivesse que passar pelo mecanismo de cooperação de MLAT, sendo cumprido diretamente pela empresa. O que atenderia a demanda de muitas autoridades de investigação que alegam ter dificuldades com os atuais mecanismos de cooperação. Contudo, não se sabe, caso a lei seja aprovada, quais e quantos países serão aceitos como elegíveis ao referido acordo com EUA, principalmente porque alguns do requisitos são conceitos abertos, e que podem variar quanto a sua significação para sistemas jurídicos diferentes. Acrescenta-se que, caso este mecanismo fique restrito a poucos aliados do EUA, como o Reino Unido por exemplo, os problemas de jurisdição continuariam nos diversos países que também têm forte presença de empresas estadunidenses de tecnologia, como o caso do Brasil.

Deve-se destacar, por fim, que há diversos grupos da sociedade civil dos EUA[47] (*American Civil Liberties Union*; *Human Rights Watch*; *Electronic Frontier Foundation*, entre outros) que criticavam o projeto de lei por ele aumentar unilateralmente os poderes de investigação das forças policiais para casos envolvendo elementos transnacionais. Elas têm demonstrado preocupações quanto à proteção à privacidade e o enfraquecimento do sistema de cooperação de MLATs. Em carta conjunta endereçada ao Congresso[48], uma das críticas feitas é que o sistema MLAT, apesar de enfrentar vários problemas de aplicação, ainda garante uma maior proteção aos direitos humanos, pois os pedidos de governos estrangeiros devem ser revistos pelo DoJ e julgados por um juiz estadunidense, que atenderia a padrões rigorosos estabelecidos no ordenamento jurídico dos EUA.

---

another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws." Hilton v. Guyot, 159 U.S. 113, 163–64 (1895). In: BREWER, David. *Obtaining Discovery Abroad: The Utility of the Comity Analysis in Determining Whether to Order Production of Documents Protected by Foreign Blocking Statutes*. Houston Journal of International Law. Vol. 22, nº 3. 2000. Acessado em: 22/03/2018. Disponível em: <https://goo.gl/dxRbwp>

46 Para mais detalhes, ver: "'(b) EXECUTIVE AGREEMENT REQUIREMENTS". S.2383/H.R. 4943 .The Clarifying Overseas Use of Data Act. p. 13. Acessado em: 23/02/2018. Disponível em:<https://bit.ly/2G3laqY>

47 *Coalition Letter Opposing the CLOUD Act*. 12/03/2018. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/qYB2EG>

48 Ibid.

A *Electronic Frontier Foundation* (EFF) afirma[49] que o PL, na prática, permite que autoridades dos EUA tenham acesso aos dados de qualquer pessoa de outro país, independentemente de sua localização ou de onde estão os dados. De forma semelhante, autoridades de um país estrangeiro que tenham feito o acordo com o Executivo estadunidense poderiam requisitar informações sobre um terceiro, independentemente de sua localização ou nacionalidade, desde que ele não seja nacional estadunidense, nem tenha residência permanente nos EUA. Essas prerrogativas acabariam por ferir a soberania de diversos países e os direitos de privacidade de inúmeros usuários ao redor do globo.

4.3. O LOCAL ONDE A EMPRESA QUE FORNECE OS SERVIÇOS FOI CONSTITUÍDA (SEDE);

O critério de localização da sede da empresa que fornece os serviços é um dos critérios de definição de jurisdição e de lei aplicável reminiscentes do *princípio da territorialidade*. Sob o princípio da territorialidade, a jurisdição e/ou a lei aplicável são definidos de acordo com a localização dos envolvidos e de seus atos. A aplicação do princípio em casos envolvendo a Internet, entretanto, é sempre bastante complicada pela dificuldade em se localizar satisfatoriamente um ato como sendo de um ou outro Estado.[50]

Especialmente na internet, o princípio territorial como critério de definição da jurisdição se revela falho, uma vez que a localização geográfica de um ato jurídico realizado pela internet é de difícil precisão. O ato pode ser cometido por uma pessoa em um país X, por meio de uma plataforma cujos servidores estão localizados no país Y, e afetar outro indivíduo no país Z, resultando em uma concorrência entre diversos Estados com reivindicações igualmente legítimas no que diz respeito a critérios de conexão territoriais.[51] Identificar a localização ideal de uma atividade online que resulte em fato jurídico relevante é, portanto, uma questão difícil e complexa.

Uma série de casos discutiram a possibilidade de se definir a jurisdição e/ou a lei aplicável de acordo com o local de sede da empresa envolvida no litígio em questão. Em poucos casos paradigmáticos, entretanto, um tribunal nacional optou por afastar a jurisdição ou legislação nacional em favor de institutos estrangeiros. A opção pelo local de sede da empresa geralmente ocorre por meio de cláusulas de eleição de foro inclusas unilateralmente nos contratos de adesão (Termos de Serviço, em inglês *Terms of Service - ToS*), baseadas em um modelo contratual anglo-saxônico que dificilmente encontra respaldo nas instituições de direito continental protetivas aos direitos do consumidor. As cláusulas de eleição de foro que chamam a jurisdição e a lei aplicável para o local de incorporação da empresa geralmente são consideradas nulas, em grande parte das jurisdições, quando invocadas pela empresa para argumentar a incompetência de um tribunal local.[52]

Um dos casos paradigmáticos não para o Direito de Internet, mas também para a questão da jurisdição e lei aplicável neste contexto, é o caso LICRA (La Ligue Contre Le Racisme et L'Antisemitisme) v. Yahoo!, iniciado em 2000 e concluído por volta de 2006.

49 FISCHER, Camille - Electronic Frontier Foundation, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data*. 08/02/2018. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/R9zNKh>

50 KUNER, Christopher, *Internet Jurisdiction and Data Protection Law*: An International Legal Analysis (Part 1). International Journal of Law and Information Technology, Vol. 18, 2010. p. 176.

51 KOHL, Uta. Jurisdiction and the Internet: Regulatory Competence over Online Activity, Cambridge: Cambridge University Press, 2007, p.24.

52 RIS. Competência Internacional dos Tribunais Domésticos e Litígios de Internet, 2018. p. 20. Disponível em: <https://goo.gl/7RveQq>

No caso, a Liga Contra o Racismo e Antissemitismo francesa processou a Yahoo! por disponibilizar em seu site de comércio eletrônico o leilão de memorabilia nazista, conduta tipificada no Código Penal Francês. Os fatos não foram contestados durante o caso, mas a empresa americana se defendeu alegando que os leilões foram conduzidos sob jurisdição dos Estados Unidos, e que portanto a corte francesa não teria competência para adjudicar o caso. O caso teve procedimentos paralelos também nos Estados Unidos.

No julgamento Francês, a corte reafirmou a competência da corte francesa, alegando que: i) os leilões estavam abertos a usuários de qualquer país, incluindo a França; ii) a exibição e visualização destes objetos causaram perturbação pública e eram contra o Código Penal Francês; e iii) a empresa americana estava ciente do acesso de usuários franceses ao serviço, pois disponibilizava um site na língua Francesa, com publicidade direcionada a cidadãos franceses e possuía uma filial em solo Francês. Condenou a Yahoo! a tomar medidas para impedir o acesso de cidadãos Franceses ao leilão. Quando a empresa americana se recusou, a Corte então passou a multá-la no valor de 100.000 francos por dia.

Em 2001, a Yahoo! optou por não recorrer da decisão. Em vez disso, levou o caso à Corte Distrital do Norte da Califórnia solicitando que julgasse a ordem Francesa como inefetiva em território Americano. Na primeira instância,[53] o tribunal julgou a condenação Francesa como conflitante com a Primeira Emenda da Constituição Americana. A instância superior do Nono Circuito, entretanto, reverteu a decisão alegando que a Corte Distrital não tinha jurisdição sobre a LICRA. O critério utilizado foi o de "contatos mínimos" que, segundo o Nono Circuito, não estavam presentes entre a LICRA e o Estado da Califórnia.

O desenvolvimento mais relevante para o caso veio em 2006,[54] quando o Nono Circuito novamente adjudicou um pedido de sentença declaratória que julgasse inefetiva em solo Americano a condenação da Corte Francesa. Mais uma vez, o tribunal de segunda instância Americano julgou improcedente o pedido da Yahoo!, tecendo comentários relevantes sobre a questão do conflito de leis e soberania gerado pelo caso. O juiz Fletcher teria dito: *"A Yahoo! está necessariamente arguindo que possui, sob a Primeira Emenda, um direito constitucional de violar a Lei Penal Francesa e de facilitar a violação desta por terceiros. [...] a existência de tal direito extraterritorial sob a Primeira Emenda é incerto."*

A consideração do juiz é relevante ao se considerar os paradoxos de soberania e os conflitos de lei gerados pela Internet: até que ponto a aplicação da legislação nacional garante um "direito" à violação da legislação de outro país?

a. Decisões favoráveis à localização da sede da empresa como critério de definição da lei aplicável

A Corte Administrativa de Hamburgo, Alemanha, recentemente derrubou uma ordem da Autoridade de Proteção de Dados (DPA) de Hamburgo contra o Facebook. A Corte decidiu que a lei de proteção de dados aplicável seria a Irlandesa, e não a Alemã, em função da localização da sede da filial europeia da empresa ser naquele país. [55]

53 USA, Yahoo! Inc. v. LA LIGUE CONTRE LE RACISME ET, 145 F. Supp. 2d 1168 (N.D. Cal. 2001). Disponível em: <https://goo.gl/wM5dZQ>

54 USA, Yahoo! Inc., a Delaware Corporation, Plaintiff-appellee, v. La Ligue Contre Le Racisme et L'antisemitisme, a French Association; L'union Des Etudiants Juifs De France, a French Association, Defendants-appellants, 433 F.3d 1199 (9th Cir. 2006) Disponível em: <https://goo.gl/E41b4H>

55 The Hamburg Commissioner for Data Protection and Freedom of Information. Facebook's real name policy remains in force for the time being. 2016. Disponível em: <https://goo.gl/eWwhZN>

O litígio se iniciou quando a Autoridade de Proteção de Dados recebeu uma reclamação de uma usuária após o Facebook ter bloqueado sua conta por usar um pseudônimo, exigir uma cópia de sua identidade e unilateralmente mudar seu nome de usuária para seu nome real. A DPA de Hamburgo decidiu que o Facebook não poderia mudar unilateralmente os nomes escolhidos por seus usuários para seus nomes verdadeiros, tampouco exigir-lhes sua identificação oficial, uma vez que a lei de proteção de dados Alemã garantiria um 'direito ao pseudônimo' em perfis online.

Rejeitando a decisão da DPA, a Corte de Hamburgo decidiu que as operações das empresas Facebook Irlanda e Facebook Alemanha constituem "estabelecimentos" dentro do significado do Artigo 4 (1)(a) da Diretiva de Proteção de Dados 95/46/EC.[56] Entretanto, sustentou que se diversas leis de proteção de dados nacionais poderiam ser aplicadas apenas pelo fato de que controlador dos dados está estabelecido em diversos Estados Membros da União Européia, então deve ser aplicada lei do Estado Europeu com o qual a operação dos dados está mais associada. No caso, a Corte de Hamburgo entendeu que, por ser a Facebook Irlanda a controladora desses dados e também o centro de operações do grupo na Europa, a Lei Irlandesa deveria ser aplicada.

A Corte se recusou a fazer uma interpretação abrangente do termo "estabelecimento" no Artigo 4(1)(a) da Diretiva. Para a Corte de Hamburgo, o caso se diferencia do caso julgado pela Corte de Justiça da União Européia (CJEU) no caso envolvendo a DPA Espanhola e a empresa Google Espanha, pois os dados em questão estão sob tutela de um controlador estabelecido em um dos Estados da União Europeia. Sendo assim, não haveria risco de que cidadãos europeus fossem privados da proteção da Diretiva, enquanto que no caso Espanhol, o controlador do sistema de busca estava localizado fora da União Europeia.

A interpretação do Artigo 4(1)(a) da Diretiva dada pela Corte Alemã indica que empresas multinacionais como a Facebook podem se escusar de observar uma miríade de diferentes legislações nacionais conflitantes, pelo menos no âmbito da União Europeia. Embora os conflitos de lei encontrados pelos tribunais brasileiros estejam em um contexto significativamente diferente no qual não existem orientações supranacionais tais quais a Diretiva 96/45/EC, o caso ainda sim pode trazer luz ao conflito de leis envolvendo controladores de dados localizados em solo estrangeiro.

b. Decisões contrárias à localização da sede da empresa como critério de determinação da lei aplicável

A própria decisão, entretanto, contrasta com outras decisões europeias envolvendo questões jurisdicionais parecidas. Uma interpretação mais abrangente do Artigo 4(1)(a) utilizada pela CJEU nos casos Google Espanha v. Mario Costeja[57] e Weltimmo.[58]

No caso Google Espanha, a CJEU decidiu que a lei europeia se aplicaria normalmente a um controlador de dados estrangeiro estabelecido fora das fronteiras da União. A corte entendeu que o Artigo 4(1)(a) não necessariamente exige que o processamento dos dados pessoais seja conduzido pelo próprio estabelecimento relevante, sendo suficiente que fosse conduzido no "contexto das atividades" deste estabelecimento. Assim,

56 UE, Diretiva 95/46/EC, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Disponível em: <https://goo.gl/BnhbK1>

57 CJUE, *Caso C-131/12*. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Disponível em: <https://goo.gl/Hyk4XM>

58 CJUE, *Caso C-230/14*. Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság. Disponível em: <https://goo.gl/aSfaEJ>

a corte entendeu que as vendas feitas pelo estabelecimento da Google na Espanha estariam "inerentemente ligadas" ao processamento de dados conduzido pelo braço da empresa nos Estados Unidos.

No caso Weltimmo, a CJEU reiterou a noção abrangente de "estabelecimento" na Diretiva. A Corte decidiu que se um controlador de dados exerce "[...]atividade real e efetiva, mesmo que mínima[...]" através de "instalações estáveis" no território do Estado, considerará-se como tendo um "estabelecimento" no território daquele Estado. Weltimmo era uma empresa registrada na Eslováquia, mas a quem a Autoridade de Proteção de Dados da Hungria queria multar por violar diversos dispositivos da Lei de Proteção de Dados Húngara. A CJEU considerou que a Weltimmo estava estabelecida na Hungria por operar um website na língua húngara, com propagandas em húngaro, representação, endereço e conta bancária no país.

5. MLATs - Dificuldades de sua Utilização e Possíveis Soluções

A utilização dos acordos de cooperação jurídica, "MLATs", apresenta, atualmente, uma série de dificuldades de eficiência e de efetividade. De modo geral, esses mecanismos foram pensados para casos excepcionais, em um contexto histórico no qual crimes transnacionais eram uma exceção. Contudo, com a crescente utilização da internet no mundo, as relações transnacionais passaram a ser cada vez mais comuns, estando presentes em diversos aspectos do cotidiano dos cidadãos.

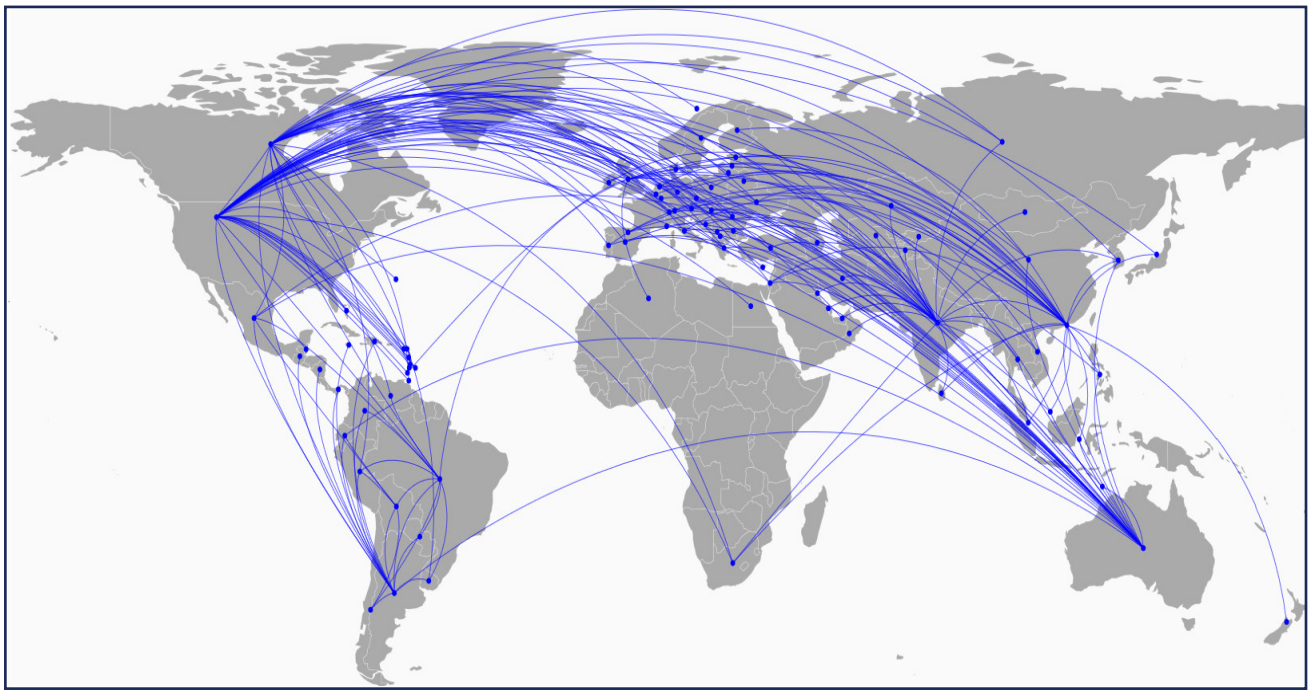
Chapelle e Fehlinger (2016) resumem os problemas estruturais enfrentados na implementação dos MLATs, nos diversos países, em 4 pontos[59]:

> **1. Celeridade:** MLATs são mal adaptados à velocidade trazida pela internet e à capacidade viral de disseminação da informação. No melhor cenário um pedido de cooperação por MLAT leva vários meses para ser processado, podendo levar até 2 anos entre determinados países. Os seus intrincados mecanismos de validação, apesar de buscarem promover garantias processuais robustas, no fim, acabam por tornar o sistema como um todo impraticável.
>
> **2. Escopo:** MLATs são frequentemente limitados à exigência de que o ato, objeto de cooperação, seja um ilícito na legislação dos dois países envolvidos (*dual incrimination*). Assim, a relevância dos MLATs acaba sendo reduzida devido a disparidade de legislações nacionais, principalmente em questões sobre liberdade de expressão, como nos casos de discurso de ódio e difamação. Eles também têm sido ineficazes nos casos em que a localização do dado requisitado é desconhecida pelos agentes estatais.
>
> **3. Assimetria:** Na prática, os MLATs impõem o sistema jurídico do país que recebe o pedido de cooperação, em detrimento daquele que faz o pedido, mesmo que não haja nenhuma conexão territorial com o país requisitado para além da sede do operador de um serviço online. Esses acordos também acabam por desconsiderar o local de ocorrência do ilícito, ou mesmo quem são as partes envolvidas. Desse modo, um número crescente de países têm criticado o sistema MLAT, principalmente quan-

59 LA CHAPELLE, Bertrand de; FEHLINGER, Paul. Ibid. p. 12 -13.

do se considera o papel dominante no mercado de empresas sediadas nos Estados Unidos.

4. Escalabilidade: O sistema tradicional de MLATs dificilmente consegue abarcar a escala da internet. Um grande número de países não possuem esses acordos de cooperação e estabelecer relações bilaterais entre 190 países iria requerer mais de 15.000 acordos.



Acordos MLAT entre os países, confome mapa interativo da ong internacional *Access Now.*[60]

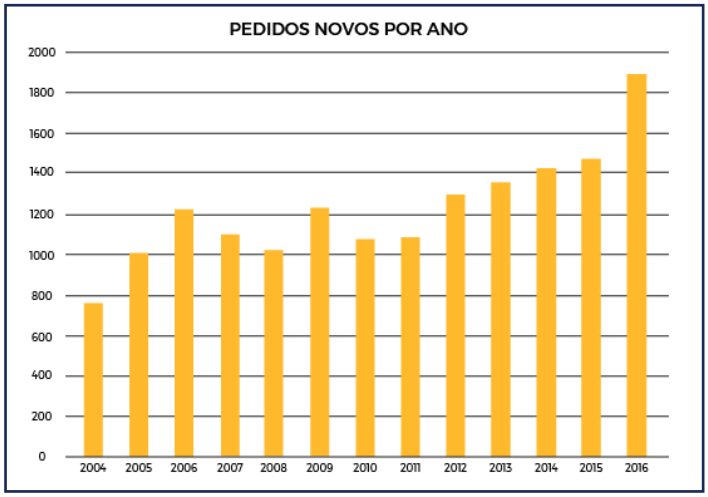
Assim, os autores acreditam que são necessárias soluções inovadoras que superem a limitações estruturais dos MLATs, a fim de se garantir o devido processo legal e a eficiência dos acordos. Contudo, eles reconhecem que o processos de reforma não serão fáceis e que, na sua visão, ainda não há uma solução simples no horizonte próximo.

Esse diagnóstico sobre a eficiência da cooperação internacional parece se confirmar no Brasil. Esta hipótese torna-se mais clara ao se comparar os números dos pedidos de cooperação na área criminal feitos pelo *Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional*, com os dados dos relatórios de transparência de determinadas empresas de tecnologia da informação, e com os dados sobre pedidos de escutas telemáticas realizadas pelas autoridades brasileiras.

No tocante aos dados do *Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional*[61] (DRCI), órgão do Ministério da Justiça, o Coordenador Geral de Recuperação de Ativos, Isalino Giacomet, estima que um processo de cooperação criminal entre o Brasil e outros países demore em média 7 meses para se concretizar, podendo este tempo ser reduzido em algumas situações emergenciais. Ele também informa que em em 2016 houve cerca de 1.900 novos pedidos na área criminal, sendo cerca de dois ativos para cada um passivo (2:1). Os EUA figuraram entre os 3 maiores demandados, atrás somente do Uruguai e Paraguai, respectivamente.

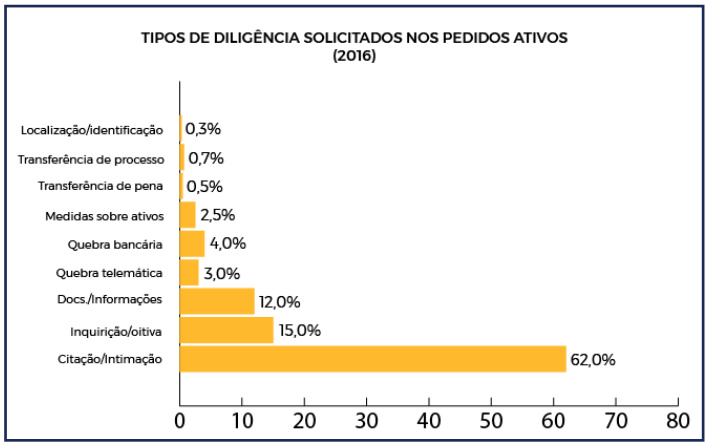
60 Para os acordos específicos entre cada país, ver: <https://www.mlat.info/>

61 Instituto de Referência em Internet e Sociedade (IRIS). Workshop: Jurisdição e cooperação jurídica internacional nos conflitos da internet - Parte 3. Novembro de 2017. Entre 00:00 e 26:00 minutos. Acessado em: 15/02/2018. Disponível em: <https://goo.gl/QZyv3H>

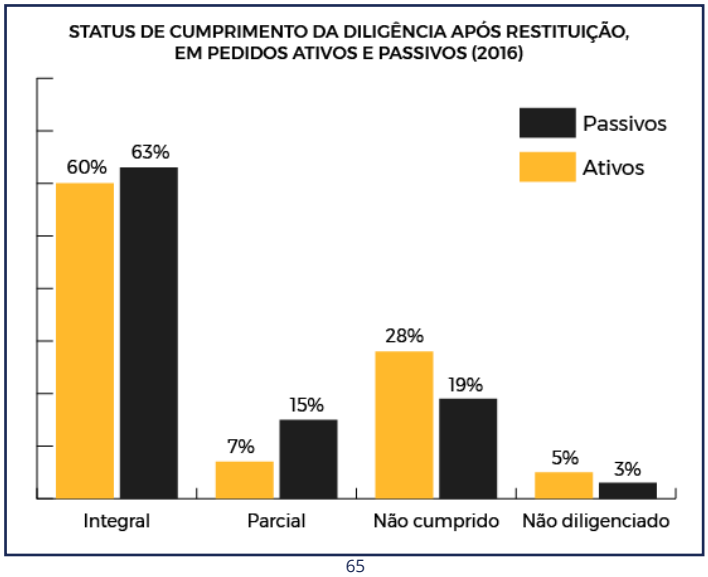


62

Acrescenta, ainda, que as diligências telemáticas[63] (obtenção de dados cadastrais, quebra de sigilo de comunicações, etc) representaram cerca de 3% dos pedidos criminais ativos em 2016; e que a taxa de cumprimento integral para todos os pedidos chegou a 60%.



64



65

62 Ibid, 8:10 - 9:30.
63 Não se refere exclusivamente a crimes cibernéticos.
64 Ibid, 14:32 - 15:00.
65 Ibid, 16:00 - 17:00.

Comparativamente, o relatório de transparência da Google de 2016 para pedidos de informações de usuários brasileiros, entre Janeiro e Junho, apresenta 874 solicitações, tendo sido atendidas 59%; enquanto que entre julho e dezembro houve 1.011 solicitações, tendo sido atendidas 60%. Apesar de não haver discriminação quanto ao tipo de dado requisitado ("escuta" em tempo real, comunicações privadas de e-mails, mensagens, etc), pode-se inferir que parte expressiva dos 1.885 pedidos de 2016, que envolviam quebra de sigilo de comunicações privadas e interceptações telemáticas, provavelmente estão entre as solicitações não atendidas (desconsiderando eventuais exceções relacionadas a emergências), já que a empresa utiliza o mesmo argumento exposto da ADC 51/2017 quanto à necessidade de procedimento por MLAT para esses casos[66].

Já o relatório de transparência do Facebook, referente somente a pedidos referentes a processos criminais no Brasil, entre janeiro e junho de 2016[67], afirma ter recebido 1.736 solicitações de informações de usuários, tendo fornecido algum dado às autoridades em 50,58% dos pedidos. Subsequentemente, entre julho e dezembro do mesmo ano, foram feitas 1.808 solicitações, tendo sido fornecido algum dado em 50.58% delas. No relatório, também são categorizados os pedidos emergenciais, dos quais cerca 12 entre 26 foram atendidos para o ano de 2016. Como o relatório também não discrimina quais tipos de dados foram requisitados, a lógica aplicado acima ao relatório da Google também pode ser aplicada ao do Facebook. Assim, é provável que os pedidos relativos a comunicações privadas estejam, em sua maioria, entre os não atendidos, já que a empresa também afirma em suas *guidelines* que, para conteúdos armazenados em conta, como mensagens, é necessário um mandado de busca (*search warrant*) emitido conforme a lei americana.[68]

Quando se compara o número de requisições feitas às empresas, com o percentual de somente 3% de pedidos criminais ativos de quebra de sigilo telemática, registrados pelo DRCI em 2016, infere-se que parte expressiva das solicitações de comunicações privadas às empresas não chegou a se converter em um procedimento de cooperação internacional por MLAT.

Finalmente, a fim de fortalecer a hipótese de que há uma demanda reprimida quanto às pedidos de fornecimento de comunicações privadas de usuários à provedores de aplicação, analisa-se brevemente os números de escutas telefônicas no Brasil. O site do Conselho Nacional de Justiça, na seção de dados relativos à escutas telefônicas de 2016 para a justiça estadual, constata que 239.222 telefones e 18.251 telefones utilizando VOIP (Voz sobre *Internet Protocol*) foram monitorados naquele ano. [69] Esses dados

66 "De que forma a Google responde a solicitações de organismos governamentais fora dos Estados Unidos? Por meio dos Tratados de Assistência Jurídica Mútua (MLATs) e de outros acordos diplomáticos e de cooperação, os organismos fora dos EUA podem trabalhar com o Departamento de Justiça do EUA para recolher provas no âmbito de investigações legítimas. Em alguns casos, a Comissão Federal do Comércio dos EUA pode prestar assistência.

Se a lei dos EUA estiver implicada na investigação, um organismo dos EUA pode abrir a sua própria investigação e fornecer as provas recolhidas aos investigadores fora dos EUA. A Google também pode divulgar dados em resposta a solicitações de divulgação urgentes se acreditar que é necessário fazê-lo para evitar ferimentos graves ou a morte de alguém.

De forma voluntária, podemos fornecer dados dos utilizadores em resposta a um processo jurídico proveniente de organismos governamentais fora dos EUA, se essas solicitações estiverem em conformidade com as normas internacionais, a legislação dos EUA, as políticas da Google e a legislação do país requerente." GOOGLE Inc. Perguntas frequentes sobre o processo jurídico para solicitações de dados de utilizadores. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/4FfVKz>

67 FACEBOOK Inc. Relatório de Transparência. 2016. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/aLZQZh>

68 "É necessário um mandado de busca emitido conforme os procedimentos descritos no Código Federal de Processo Penal dos Estados Unidos, ou um mandado estadual equivalente mediante comprovação de justificativa provável para forçar a divulgação de conteúdos armazenados em qualquer conta, incluindo mensagens, fotos, vídeos, publicações na Linha do Tempo e informações de localização." FACEBOOK Inc. Guidelines - Informações para Autoridades Policiais. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/uYDvfX>

69 CONSELHO NACIONAL DE JUSTIÇA. Relatórios Quantitativos - Interceptações Telefônicas. 2016. Tabelas 5 e 6. Acessado

demonstram como a prática de monitoramento de telefones ainda tem sido ferramenta constante de investigação no país, necessidade essa que não parece estar sendo substituída por outros instrumentos conforme a telefonia tradicional vem cedendo espaço para formas de comunicação via internet. Assim, é evidente como, para 2016, o pequeno número de pedidos de cooperação internacional realizados pelo Ministério da Justiça contrasta expressivamente com o volume de interceptações telefônicas realizadas. Este fato fortalece a afirmação de Chapelle e Fehlinger quanto aos problemas estruturais enfrentados pelas autoridades na tentativa de se utilizar do sistema atual de MLATs. Assim é no mínimo questionável afirmar que tal arranjo institucional tem funcionado de forma eficiente no Brasil.

Apesar disso, deve-se ressaltar que relevantes atores envolvidos com o debate sobre jurisdição e internet defendem que o sistema MLAT, apesar dos atuais problemas, deve ser fortalecido por meio de reformas. A *Electronic Frontier Foundation*, por exemplo, recomenda o aperfeiçoamento do sistema MLAT[70], pois acredita que ele estabelece garantias processuais mais robustas, e uma maior proteção à privacidade, já que uma autoridade buscando um dado no exterior precisa respeitar as proteções legais dos dois países envolvidos. Os problemas de eficiência, alega a EFF, poderiam ser resolvidos, em parte, através de uma maior atribuição de recursos ao órgãos de cooperação, uma simplificação dos procedimentos, e um melhor treinamento das forças policiais e do judiciário quanto aos mecanismo de cooperação.

Desse modo a falta de cooperação entre os países pode acabar por incentivar a adoção de soluções diversas, como a invasão de dispositivos eletrônicos feita diretamente pelas forças policiais, a qual apresenta graves riscos à privacidade e à violação da soberania de terceiros. Ou mesmo a imposição de que os dados sejam armazenados na jurisdição do país (*data localisation*), a qual possui efeitos temerários quanto à eficiência e à liberdade econômica do setor de tecnologia.

A título ilustrativo, Ahmed Ghappour, da Boston University, alerta para o fato de que invasões de dispositivos informáticos (*network investigative techniques* ou *hacking*) feitas pelo FBI em investigações na *dark web*, envolvem, em grande parte dos casos, pessoas localizadas em outros países como alvos dos inquéritos. Assim, ele acredita ser plausível afirmar que esse fenômeno pode estar levando a maior expansão de aplicação extraterritorial da jurisdição estadunidense (*enforcement jurisdiction*) já realizada na história do FBI.[71]

6. Confusões conceituais intencionais: identificação de usuários e anonimato

Nas breves manifestações de direito material aportadas pela **Sociedade de Usuários de Tecnologia - SUCESU Nacional**, nos autos da ADC 51/2017, parece haver patente confusão entre a sistemática de identificação de usuários online e o conceito de anonimato. Segundo a SUCESU, a aplicação de dispositivos do Decreto No 3.810/2001 (que incorpora o Acordo de Assistência Mútua entre Estados Unidos e República Federativa do Brasil) "feriria" a vedação ao anonimato, do art. 5º, inciso IV, da Constituição

em: 23/02/2018. Disponível em: <https://goo.gl/kE5ZAU>

70 JAYCOX, Mark; e TIEN, Lee. Reforms Abound for Cross-Border Data Requests. Electronic Frontier Foundation. 27/12/2015. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/2WJAfV>

71 GHAPPOUR, Ahmed.*Searching places unknown: law enforcement jurisdiction on the dark web*. Stanford Law Review. 69.4. Abril de 2017.p.3. Acessado em: 25/03/2018. Disponível em: <https://stanford.io/2pIBCGa>

Federal.

Em diversas disputas judiciais em matéria de internet e novas tecnologias, essa é uma associação comum que se faz, apesar de equivocada, entre as possibilidades técnicas de sigilo e de proteção de dados pessoais, em detrimento da liberdade de expressão desde que identificada, conforme determina nossa Constituição. Em certo trecho da peça da SUCESO Nacional, chega-se a afirmar que "*fazer valer o entendimento preconizado pela Autora da demanda, afastar-se-á a vedação constitucional ao anonimato*", o que simplesmente não condiz com a realidade argumentativa e dos fatos.

Defensores dos direitos de usuários e da sociedade civil organizada, como é o caso do **Instituto de Referência em Internet e Sociedade - IRIS**, ao exigir o cumprimento de salvaguardas e procedimentos legalmente instituídos para a quebra de sigilos telemáticos e identificadores, como aqueles previstos pelo Marco Civil da Internet (arts. 22 e art. 3º, parágrafo único) e pelos Acordos de Assistência Mútua entre Estados, de forma alguma propõem violações à ordem constitucional, ou à vedação ao anonimato. Ao contrário, a submissão feita pelo IRIS, admitido como 'Amicus Curiae" na ADC nº 51, objetiva proteger justamente os direitos e garantias do art. 5º da Constituição Federal, entre eles a intimidade, a privacidade e o sigilo das comunicações. Para tanto, propõe-se a tutela de instrumentos próprios de acesso a esses dados, legalmente previstos e em conformidade com a ordem jurídica vigente, e a afirmação da observância do direito internacional pelo STF.

O suposto antagonismo do binômio liberal "privacidade" x "segurança" é frequentemente criticado pela doutrina nacional[72] e internacional[73], já que em diversas ocasiões direitos fundamentais foram flagrantemente "flexibilizados" em favor de uma pretensa necessidade de resposta social (e, por vezes, política e midiática) à questões de segurança. Ocorre que privacidade e segurança não são mutuamente excludentes, assim como a proteção aos dados pessoais de usuários não significa, necessariamente, direito ao anonimato. Ademais, deve-se ter em mente que a condição de "anônimo" na internet não é um fenômeno binário e estanque, mas que compreende diversos graus de caracterização, conforme a maior ou menor dificuldade técnica para que um usuário seja identificado. Esta caracterização gradativa, inclusive, é reconhecida na Lei Geral da Proteção de Dados Pessoais, tanto brasileira (art, 5º, III, PLC 53/2018[74]) quanto europeia (recital 26, *General Data Protection Regulation*[75]), que buscam incentivar o tratamento de dados pessoais anonimizados, a fim de se promover uma maior privacidade e proteção do usuário, sem prejuízo ao desenvolvimento tecnológico.

As novas tecnologias envolvidas em plataformas de comunicação e computação

72 DONEDA. Danilo. A proteção dos dados pessoais como um direito fundamental. In: Espaço Jurídico.v. 12, n. 2, p. 106, jul./dez. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>, acesso em 16 de julho de 2018.

73 SOLOVE, Daniel J. *Nothing to Hide:* The False Tradeoff between Privacy and Security. Yale University Press, 2011, p. 207.

74 "Art. 5º Para os fins desta Lei, considera-se: [...] III – dados anonimizados: dados pessoais relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;"

75 "Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação." Regulamento(UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: <https://bit.ly/2LsogHg>

em nuvem, como as que suscitam o debate em comento, potencializaram o armazenamento de dados pessoais (de identificação e de comunicação) cada vez mais para fora do Estado de residência habitual dos cidadãos, ao contrário do que era a praxe quando se começa a discutir o direito à privacidade[76]. O próprio conceito de privacidade evolui para acompanhar as transformações sociais que o estabelecem e modulam (privacidade de crianças e adolescentes, responsabilidade na manutenção de grandes bancos de dados, alocação de salvaguardas para a condução de transações online - bancárias, processos judiciais eletrônicos, etc.). Isso não significa, por essa razão, que esses dados não estariam sujeitos aos adequados regimes legais de proteção à privacidade, especialmente a um conceito de privacidade compatível com a realidade das novas tecnologias, que é também transnacional, que envolve diferentes atores e que exige múltiplas formas de proteção.

Segurança e privacidade são ideias que ocasionalmente podem ser ponderadas, mas não de forma similar a um jogo de soma-zero. É possível, **honesta e racionalmente**, retomar um debate intelectual sem propor este antagonismo, justamente pelos instrumentos legais (leis nacionais e acordos internacionais) cuja constitucionalidade aqui se procura assegurar. O próprio Marco Civil da Internet, em seu art. 3º, elenca a **privacidade** e a **segurança** como princípios disciplinadores, e não concorrentes ou excludentes, do uso da internet no Brasil, o que é reforçado em seu artigo 8º[77]. Parece um contrassenso, dentre alguns dos argumentos ventilados na Manifestação da SUCESO Nacional, que privacidade e segurança sejam destacados como se fossem pretensões irreconciliáveis, como se representassem uma panaceia da era digital.

Ao contrário, a sociedade em rede, característica do momento atual, somente se estrutura graças ao aperfeiçoamento dos padrões societários do longo - e fatídico- século XX e que cimentaram o respeito ao valor do Estado Democrático de Direito. Suas instituições devem preservar conquistas em termos de direitos humanos, como mesmo representa a privacidade online e a segurança das interações, comunicações, negócios e operações na Internet.

O que se propõe, por meio da afirmação e declaração da constitucionalidade do Decreto No 3.810/2001, e da aplicação imediata das normas de direitos humanos previstos nos tratados de que o Brasil é parte (ainda por força dos Arts. 5, §§1, e 2, da Constituição e Art. 3, parágrafo único, do Marco Civil) não é, portanto, a prevalência do anonimato sobre a possibilidade de identificação dos usuários, mas sim a observância dos procedimentos vigentes para que a identificação e a quebra de sigilos telemáticos possam ocorrer.

Nesse quadro, caso manifestações em procedimentos constitucionais como na ADC 51/2017 não confiem pedidos e demandas dessa natureza à legislação vigente e aos compromissos internacionalmente assumidos, o Brasil estaria a recorrer à posição contraditória em relação às garantias que institucionalmente construiu no que se refere à Internet. De modo mais grave, dispensar os mecanismos que favorecem o devido

76 SOLOVE, Daniel J. A Brief History of Information Privacy Law. In: *Proskauer on Privacy,* PLI, 2006, p. 5. Disponível em: <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications>, acesso em 16 de julho de 2018.

77 No que tange especificamente à privacidade e à intimidade no Marco Civil da Internet, Giacchetta e Meneguetti afirmam que: "O Marco Civil da Internet reafirmou a garantia constitucional à inviolabilidade da intimidade e da vida privada, como princípio e também como direito dos usuários da rede mundial de computadores, como reação aos feitos internacionais relacionados à coleta e utilização não autorizada de dados pessoais e de comunicação de usuários brasileiros, mesmo que prescindível ante as disposições da Constituição Federal de 1988". Cf. GIACCHETTA, André; MENEGUETTI, Pamela. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: *Marco Civil da Internet.* LEITE, George Salomão; LEMOS, Ronaldo (coord.). São Paulo: Atlas, 2014, p. 390.

processo transnacional, como apontado no item 8 a seguir, poderia implicar riscos de submeter a sociedade brasileira aos procedimentos de vigilância massiva, censura e infrações à privacidade e à liberdade de expressão online (art. 8º, do Marco Civil da Internet).

Esses procedimentos também são adotados - em escala maior e com profundidade distinta, mas não de forma que deslegitima a comparação - em países como Rússia, China, Irã, Síria e Arábia Saudita[78]. Neles, o anonimato também não é permitido, em detrimento de garantias e liberdades individuais, mas também e especialmente em defesa de uma pretensa segurança nacional que, diga-se de passagem, não é atingida por meio de ainda mais vigilância[79]. Dessa forma, observa-se que o combate ao anonimato não é justificativa a ser acolhida pelo STF a fim de afastar os instrumentos de cooperação internacional, incorporados ao ordenamento jurídico brasileiro.

7. Marco Civil da Internet Art. 3º, parágrafo único, e Art. 11

Há entre certos advogados, juízes e acadêmicos, a impressão de existir aparente "conflito de leis" entre o Marco Civil da Internet, com seus dispositivos de aplicação unilateral da lei brasileira (Artigo 11), e o Decreto nº 3.810 de 2001, que determina o processo a ser adotado em casos de cooperação jurídica internacional. Esse conflito, entretanto, é apenas aparente, sobretudo quando analisados mais a fundo os dispositivos e a estrutura de relacionamento ou interação entre normas estabelecidas pelos próprios instrumentos legislativos.

Ao rejeitar o cumprimento de pedidos de fornecimento ou entrega de dados por parte da Justiça brasileira em função da restrição imposta pela lei estadunidense (*Stored Communications Act)*, empresas provedoras de aplicações com atuação transnacional não estão violando a soberania brasileira, nem entrando em conflito com o ordenamento jurídico brasileiro. Isso, porque o próprio direito brasileiro, integrado por normas do Marco Civil da Internet, do Decreto nº 3.810 e da Constituição, prevê a observância do procedimento de cooperação internacional mediante apoio dos *Mutual Legal Assistance Treaties* - MLATs (ou Acordos Mútuos de Cooperação Jurídica, em português), sem margem discricionária para o juiz nacional. Para além das obrigações legais, existem obrigações de caráter internacional bilateral e multilateral, fundadas em tratados, cujo desumprimento levaria o Brasil à responsabilidade internacional por violação positiva.

O equívoco inicial parece estar baseado na análise isolada do Artigo 11 do Marco Civil da Internet,[80] que determina a aplicação da legislação brasileira a quaisquer casos de coleta, armazenamento, guarda e tratamento de registros nos quais um dos terminais esteja situado no Brasil. O parágrafo 2º novamente apenas acentua o equívoco

78 A esse respeito, cf. os indicadores e resultados de análise em FREEDOM HOUSE. *Freedom on the Net Report 2017*: manipulating Social Media to Undermine Democracy. Disponível em: <https://freedomhouse.org/report/freedom-net/freedom-net-2017>, acesso em 16 de junho de 2018. Sobre o tema, ver ainda Relatório de 2015 da Assembleia de Estados do Conselho da Europa, sobre Vigilância em Massa e Ameaça aos Direitos Humano, disponível em: https://pt.scribd.com/document/253848295/Mass-Surveillance-Report

79 BARTLETT, Jamie.The online surveillance debate is really about whether you trust governments or not. In: *The Telegraph***,** em 06/11/2015. Disponível em: <https://www.telegraph.co.uk/technology/internet-security/11979682/The-online-surveillance-debate-is-really-about-whether-you-trust-governments-or-not.html>, acesso em 16 de junho de 2018.

80 "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."

sobre um aparente conflito[81], uma vez que estabelece que a lei brasileira (material) se aplica mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior e que possua, no mesmo grupo econômico, estabelecimento no Brasil.

A partir desses dois blocos de regras, fica evidente que o objetivo das fórmulas legislativas foi apenas submeter unilateralmente, ao direito brasileiro, a regência (ou disciplina) de certas relações jurídicas envolvendo empresas de internet e usuários ("coleta, armazenamento, guarda e tratamento de registros nos quais um dos terminais esteja situado no Brasil"). Ou seja, trata-se de um problema de lei material aplicável; ele não se confunde com questões jurisdicionais, especificamente quanto à definição da competência dos tribunais nacionais para solucionar um litígio envolvendo aquelas partes. Levada a análise para a precisa delimitação dos objetos do direito internacional privado, como observa o Professor Jacob Dolinger, a questão ali subjacente é uma questão de direito aplicável ao caso com conexão internacional[82]. A natureza e a classificação da regra contida no Art.11 do Marco Civil, por sua vez, apontam para uma regra de conflito do tipo "unilateral" (quanto à estrutura), vale dizer, regra que designa uma única solução de direito aplicável, a qual refere-se, na espécie analisada, à lei brasileira[83]. Evidentemente, a solução de política legislativa ali contida parece estar baseada em um critério espacial muito específico: "local de atividade de coleta, armazenamento, guarda ou tratamento" de dados no Brasil.

Restaria claro, portanto, que a lei brasileira aplicar-se-ia a qualquer ato relativo à coleta, ao armazenamento, guarda ou tratamento de dados na presença de um elemento de conexão objetivo (ao menos um dos terminais situados no Brasil) e, portanto, qualquer oposição a estes dispositivos em função de restrição por lei americana configura uma violação da soberania e das normas brasileiras. No entanto, o próprio ordenamento jurídico brasileiro **rejeita essa noção para o caso específico da requisição de dados, informações ou, no extremo, provas localizadas sob jurisdição estrangeira.**

Importante destacar que existem outros dispositivos no Marco Civil da Internet, no Decreto nº 3.810 de 2001 (Acordo de Cooperação Brasil-Estados Unidos) e na Constituição Federal que validam a necessidade de uso dos MLATs para os casos envolvendo a internet. Não se deve confundir, entretanto, os dados referentes ao **conteúdo das comunicações** ou conversas entre usuários com os chamados **metadados** de acesso, que também são exigidos pela Lei 12.965/14. A *Stored Communications Act* apenas impede que as empresas entreguem os primeiros, decidiu jurisprudência Americana.[84]

Segundo Pontes de Miranda, o Direito é um sistema metódico de regras e que satisfaz exigências de **coerência e de consistência**. Ao analisar intrínseca e extrinsecamente as relações sociais que são timbradas pela ordem jurídica, o autor explica:

81 "§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil."

82 DOLINGER, Jacob. *Direito Internacional Privado.* Parte Geral, 10.ed. Rio de Janeiro: Forense, 2011, pp.20 e ss.

83 Exemplo típico de uma norma unilateral de conflito é a contida no Art.7, §1 da LINDB ("Realizando-se o casamento no Brasil, será aplicada a lei brasileira quanto aos impedimentos dirimentes e às formalidades da celebração"). Nas palavras de DOLINGER (Direito Internacional Privado, cit., p.213), a tendência do DIP brasileiro é a de formular normas bilaterais, sendo excepcionais os casos de unilateralismo. Para ele, os defensores do unilateralismo sustentam que o legislador somente tem competência legislativa sobre "a aplicação de suas próprias leis, não lhe cabendo atribuir competência à lei de outro legislador, pois só este dirá do alcance de sua lei. Segundo essa escola, o legislador apenas determina quando se aplicará sua própria lei".

É exatamente o que ocorre com a solução do Art.11 do Marco Civil, cujo alcance normativo fica adstrito à submissão, à lei brasileira, das relações jurídicas emergentes da "coleta, armazenamento, guarda ou tratamento" de dados, quando pelos menos um deles tenha ocorrido ou sido realizado no Brasil.

84 "Metadata is not 'content' under Stored Communications Act." ESI Case Law, Março de 2013. Disponível em: <https://www.ilsteam.com/metadata-is-not-content-under-the-stored-communications-act>

> As regras jurídicas hão de construir sistema. Nenhuma regra jurídica é sozinha, nenhuma é gota, ainda quando tenha sido o artigo ou parágrafo único de uma lei. [...] Essa exigência de sistematicidade do direito atende à necessidade de coerência e consistência, na conduta humana, máxime no que concerne à vida de relação[85].

O artigo 3º, parágrafo único[86] do Marco Civil da Internet situa a legislação internacional dentro do ordenamento jurídico brasileiro, e seu respeito a princípios outros que aqueles estabelecidos na própria lei, introduzindo assim uma regra de abertura à sistemática de tratados e convenções. Igualmente, incorpora obrigações de caráter processual, como o dever de estabelecer cooperação jurídica no curso do processo civil transnacional. **Cooperação jurídica, portanto, não pode ser concebida como ato de mera discricionariedade por parte da autoridade administrativa e judiciária brasileira.** Ela se estabelece como comando direto dos tratados, pelo Código de Processo Civil, pela Constituição, e no interesse de consecução de objetivos de justiça.[87] É preciso, ainda, analisar a Constituição da República, em seu Título I, relativo aos **princípios fundamentais.**

O Artigo 4º[88] da CR/88 elenca os princípios que regem as relações internacionais da República, e portanto oferece a base principiológica sob a qual os casos de cooperação jurídica devem ser analisados. Entre eles, está o chamado **Princípio da Cooperação Internacional**, estabelecido pelo inciso IX deste artigo como "cooperação entre os povos para o progresso da humanidade". Sobre este princípio, Hildebrando Accioly afirma:

> O principal, dentre os deveres morais dos Estados, é o **de assistência mútua**, o qual se manifesta sob várias formas. Entre estas, podem citar-se as seguintes: [...] d) a assistência e cooperação para a administração da justiça, tanto em matéria civil, quanto em matéria penal, compreendendo-se nesta última a adoção de medidas próprias para facilitar a ação social contra o crime[89].

Igualmente, é preciso observar a eficácia imediata da norma contida no parágrafo 2º do Artigo 5º da Constituição,[90] que ressalta a **não exclusão de outros princípios decorrentes**, bem como dos **tratados internacionais** com os quais o Brasil se comprometeu.

Sendo assim, por observância ao princípio da cooperação internacional, bem como outros princípios de direito internacional e direito dos tratados (como explicado no capítulo anterior), nenhuma interpretação consistente do Marco Civil pode ir de encontro ao estabelecido no Decreto nº 3.810 de 2001, que estabelece em diversos momentos o respeito à legislação do Estado Requerido. Isto porque: (i) O Decreto incorpora, ao

85 PONTES DE MIRANDA, Francisco Cavalcanti. *Comentários à Constituição de 1967*, Vol. I (arts. 1º - 7º). São Paulo : Editora Revista dos Tribunais, 1967, p. 39.

86 "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [..] Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte."

87 POLIDO, Fabrício. *Brasil, cooperação jurídica internacional e Internet*. Jota, 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/brasil-cooperacao-juridica-internacional-e-internet-31072017#_ftn1>

88 "Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios: IX - cooperação entre os povos para o progresso da humanidade;"

89 ACIOLY, Hildebrando. Tratado de Direito Internacional Público. Volume I. São Paulo : Quartier Latin, 2009, pp. 314-315.

90 "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte."

ordenamento brasileiro, **tratado** ao qual o Brasil se comprometeu a seguir; (ii) O Marco Civil determina, em seu Art 3º o **respeito a outros princípios vigentes** no ordenamento jurídico Brasileiro, neste caso, o da cooperação internacional; e (iii) O Decreto por si só **é parte do direito brasileiro**, para o qual o Marco Civil - Lei nº 12.965/14 - determina a observância para casos envolvendo dados coletados no Brasil.

O Decreto nº 3.810 de 2001 estabelece a observância das leis do Estado Requerido (E.R.) em três pontos:

(i) no Artigo I, 2., h),[91] para restringir formas de assistência proibidas pelas leis do E.R.;

(ii) no Artigo V, 3.,[92] para determinar que as solicitações de cooperação sejam executadas de acordo com as leis do E.R.; e

(iii) no artigo XIV, 1.,[93] para determinar que a execução de mandados de busca e apreensão sejam justificadas segundo as leis do E.R.

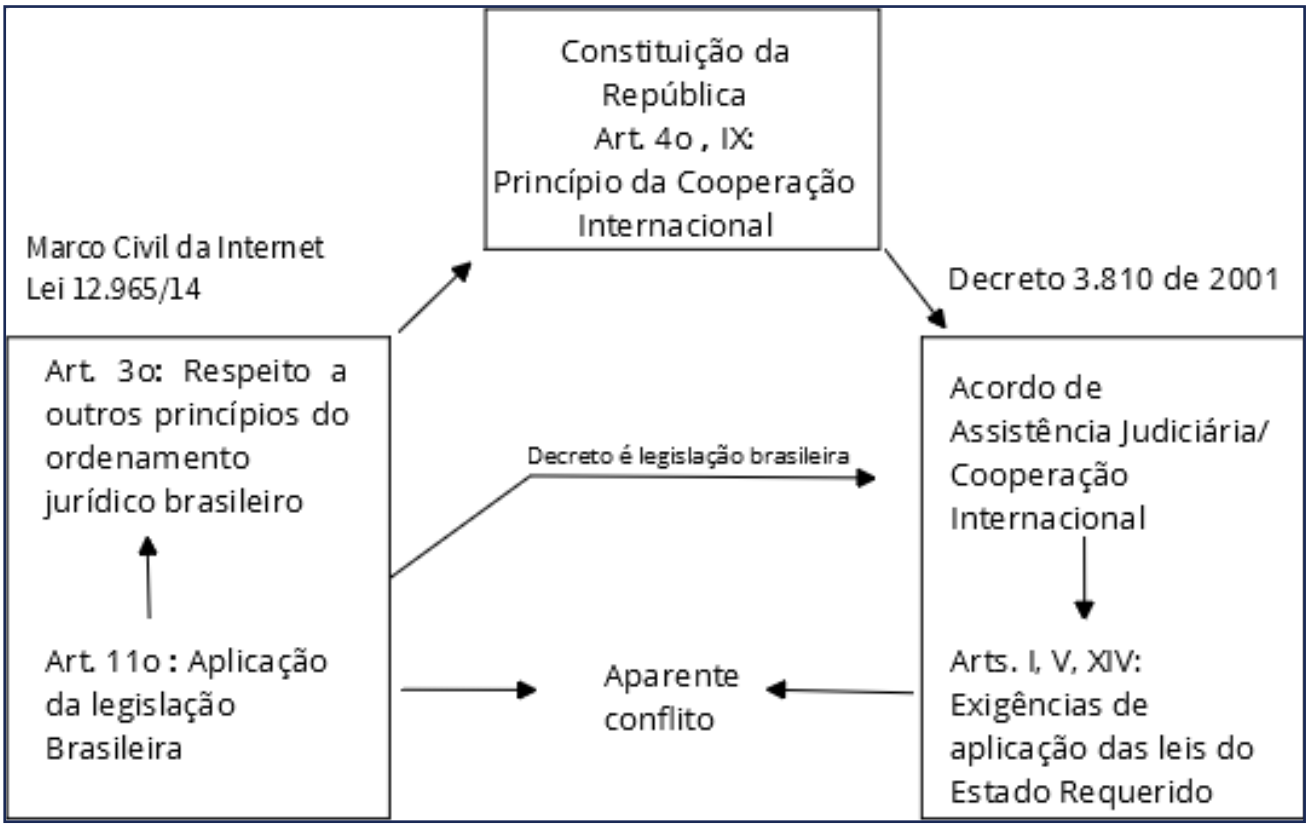


Figura I - Conflito Aparente entre a Lei 12.965/14 e o Decreto 3.810/01

No esquema acima, podemos observar a submissão da regra do artigo 11 do Marco Civil da Internet a outros dispositivos da mesma lei, da Constituição e do Decreto nº 3.810/2001. Não se trata, portanto, de um caso em que a legislação brasileira é omissa e uma empresa estrangeira estaria se beneficiando dessa omissão. O Estado brasileiro assumiu um compromisso, qual seja, o de cooperar por assistência mútua e o de respeitar a legislação do Estado requerido; não poderia agora dele se eximir por conveniência de autoridades de investigação ou persecução criminal e em submissão à

91 Artigo I. 2. A assistência incluirá: [...] h) qualquer outra forma de assistência não proibida pelas leis do Estado Requerido.

92 Artigo V. 3. As solicitações serão executadas de acordo com as leis do Estado Requerido, a menos que os termos deste Acordo disponham de outra forma. O método de execução especificado na solicitação deverá, contudo, ser seguido, exceto no que tange às proibições previstas nas leis do Estado Requerido.

93 Artigo XIV, 1. O Estado Requerido executará o mandado de busca, apreensão e entrega de qualquer bem ao Estado Requerente, desde que o pedido contenha informação que justifique tal ação, segundo as leis do Estado Requerido.

legislação infraconstitucional.

Como será examinado mais adiante (cf. item 4), as normas interpretadas sistematicamente - da Constituição, do Acordo Brasil-Estados Unidos e do Marco Civil - também apontam para a observância de direitos e garantias processuais às partes no contencioso transnacional civil e penal, igualmente incidentes em litígios pluriconectados da Internet.

8. Defesa dos direitos e garantias fundamentais dos usuários

Outro aspecto bastante relevante para a consideração da constitucionalidade do Decreto No 3.810/2001, que incorpora o Acordo de Assistência Mútua em Matéria Criminal entre Estados Unidos e República Federativa do Brasil, diz respeito à necessidade de os tribunais nacionais de garantir direitos dos usuários online.

Não é por outro motivo que a Lei 12.965/2014 é frequentemente denominada a "constituição da internet" no Brasil. Sem a pretensão de exaurir as salvaguardas contempladas por essa legislação aos usuários, o Marco Civil da Internet reforça importantes direitos e garantias fundamentais, como o direito à privacidade, à proteção dos dados pessoais (objeto inclusive de legislação recém-aprovada no Congresso Nacional, na figura do PLC 53/2018), a inviolabilidade e sigilo das comunicações online, a acessibilidade, a liberdade dos modelos de negócio, bem como **outros princípios "previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte**" (art. 3º, parágrafo único).

Ou seja, a própria "constituição da internet" no Brasil, assim como a Constituição Federal, admite a adequação do regime jurídico nacional à ordem internacional, bem como a incorporação de tratados internacionais em seu rol de instrumentos legislativos. Assim como o Acordo de Assistência Mútua entre Estados Unidos e República Federativa do Brasil pode ser incluído nessa categoria e de acordo com seu processo de internalização, também podem ser gradualmente incorporadas, ao ordenamento brasileiro, declarações como a que trata o acesso à internet como um direito humano[94], do Conselho de Direitos Humanos da Organização das Nações Unidas, do qual o Brasil fazia parte.

Parte significativa da doutrina também considera o modelo adotado na elaboração do Marco Civil da Internet como garantista, que pressupõe a subordinação do poder público e privado às normas superiores que estabelecem direitos fundamentais, como seriam aquelas constantes dos artigos 7º e 8º do Marco Civil da Internet[95]. Nesse contexto, o reconhecimento dos direitos elencados como garantias fundamentais implica sua primazia na adequação dos atos formais às questões materiais, conforme observa também o jurista italiano Luigi Ferrajoli[96], em um claro rompimento com o positivismo jurídico tradicional, e em benefício da interpretação sistemática do ordenamento jurídico, atenta aos conceitos de validade, vigência material e democracia substantiva das leis.

94 ONU. Conselho de Direitos Humanos, *Resolução n A/HRC/32/L.20*, de 30 de junho de 2016. Disponível em: <https://www.article19.org/data/files/Internet_Statement_Adopted.pdf>, acesso em 16 de julho de 2018.

95 COPETTI, Alfredo; FISCHER, Ricardo Santi. A natureza dos direitos e das garantias dos usuários de internet: uma abordagem a partir do modelo jurídico garantista. In:. LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014, p. 350-351.

96 FERRAJOLI, Luigi. *Derechos y garantías*: la ley del más débil. Madrid: Editorial Trotta, 2010, p. 499.

9. Respeito ao devido processo legal transnacional

Em linha com as abordagens teóricas e doutrinárias, procedimentos de cooperação internacional vinculam o Estado brasileiro, desde a perspectiva da Constituição, do Código de Processo Civil e dos tratados de que o Brasil é parte.

O art. 26, *caput*, do CPC determina a abertura da sistemática processual brasileira para o direito internacional, estabelecendo a **primazia de tratados e convenções na regulação dos atos e medidas de cooperação jurídica**, em sintonia com os princípios ali oferecidos. Entre eles, importante destacar que o legislador expressamente previu a observância de **garantias do devido processo legal** no Estado requerente (art. 26, inciso I), que pode ser o Brasil, quando formula os pedidos ativos, ou o Estado estrangeiro, quando ele endereça os pedidos às autoridades judiciárias e administrativas brasileiras para cumprimento (pedidos passivos). A observância do devido processo deve conter tanto o direito das partes envolvidas na disputa quanto ao direito de formular suas pretensões (direito de ação), como a ampla defesa e contraditório, além das garantias de que os procedimentos no foro e no estrangeiro se desenvolvam com respeito aos "direitos fundamentais do processo"[97].

Em concorrência com essas garantias, asseguradas pela lei interna (Constituição Federal e leis processuais), encontram-se os direitos assegurados pelos tratados de que o Brasil é parte em matéria de direitos humanos, como a Convenção Americana de Direitos Humanos de 1969 - Pacto de San José. Em seu artigo 8º, a Convenção Americana assegura o devido processo legal no curso de procedimentos civis, criminais, administrativos perante os tribunais nacionais dos Estados partes, incluído como garantia judicial a ser estabelecida nos ordenamentos jurídicos internos.

Nesse sentido, a Corte Interamericana de Direitos Humanos- CIDH, a cuja jurisdição se submete o Estado brasileiro, já se manifestou em torno da concreção e alcance normativo do art. 8º, como nos casos *Castillo Petruzzi/Peru*[98], *Baena Ricardo/Panamá*[99] e *Camba Campos/Equador*[100]. Como conjunto de precedentes relevantes, as sentenças proferidas pela Corte apontam para a compreensão da observância do devido processo como componente dos direitos fundamentais das partes em disputa ou em controvérsias adjudicadas pelos tribunais nacionais; referem-se ao conjunto de regras também delineadoras do "direito de defesa processual", com pretensões que podem ser invocadas pelas partes demandadas não apenas no contencioso penal, mas também em outras matérias (civil, trabalhista, comercial, administrativa), em que haja incidência de garantias processuais[101].

Em cotejo com a interpretação consistente com as normas internacionais de direitos humanos, incluindo as decisões proferidas pela Corte Interamericana envolvendo matéria concernente ao art. 8º do Pacto de San José, cuja hierarquia no ordenamento

97 Cf. POLIDO, Fabrício B. P. Fundamentos, estruturas e mecanismos da cooperação jurídica internacional e o Código de Processo Civil brasileiro. In: Cooperação Jurídica Internacional. Revista dos Tribunais vol.990. Caderno Especial. Abril de 2018, p.37 ss.

98 CIDH. *Castillo Petruzzi y otros Vs. Perú. Fondo, Reparaciones y Costas*. Sentencia de 30 de mayo de 1999. Serie C No. 52.

99 CIDH. *Baena Ricardo y otros Vs. Panamá. Fondo, Reparaciones y Costas*. Sentencia de 2 de febrero de 2001. Serie C No. 72, § 125.

100 CIDH. Caso del Tribunal Constitucional (Camba Campos y otros) Vs. Ecuador. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 28 de agosto de 2013. Serie C No. 268, § 167.

101 Segundo a CIDH, "el individuo tiene el derecho al debido proceso entendido en los términos del artículo 8.1 y 8.2, tanto en materia penal como en todos otros órdenes"(Caso Baena Ricardo y otros Vs. Panamá, 2001).

brasileiro, a despeito da orientação majoritária do STF, é de caráter constitucional (art. 5o, parágrafo 2º, CF/88), ao menos algumas consequências podem ser observadas. A aplicação imediata de normas de direitos fundamentais de usuários da internet - nacionais ou estrangeiros residentes no Brasil-, na esteira do art. 5º, parágrafo 1º da Constituição, e do Marco Civil, não exclui, evidentemente, normas previstas em tratados e convenções de que o Brasil é parte; ao contrário, incluem as que prevêem garantias processuais, como o devido processo (*ex vi* o art. 8º do Pacto de San José), e que também dizem respeito à integridade do processo civil/criminal instaurado perante os tribunais brasileiros Se eles envolverem, igualmente, questões relativas à Internet, como busca, retenção ou fornecimento de dados telemáticos, também em processos civis/comerciais, penais, administrativos, ditas garantias devem ser observadas. De outra medida, a cooperação jurídica internacional também se organiza a partir da observância dos direitos e garantias das partes no contencioso transnacional.

O próprio ordenamento jurídico brasileiro, integrado por normas da Constituição Federal, do Decreto nº 3.810/2001 e do Marco Civil da Internet, prevê a observância de procedimentos de cooperação internacional mediante recurso a MLATs, como o Acordo Brasil-Estados Unidos ou Acordo Brasil-Suíça[102], sem margem discricionária para mera opção ou dispensa pelo juiz nacional. A constelação normativa ali existente - e vigente - para regulação material e procedimental de fatos, situações e relações jurídicas emergentes da Internet - admitidas em seus elementos de conexão, de internacionalidade-, não afasta o cumprimento ou adimplemento de obrigações internacionais bilaterais e multilaterais fundadas em tratados de que de que o Brasil é parte. Ao contrário, o cumprimento das obrigações convencionais é reforçado, especialmente, pela vinculação expressa da República Federativa do Brasil a princípios de cooperação internacional em todas suas relações com Estados estrangeiros.

10. Argumento da sede da empresa não é suficiente para solucionar a demanda

Conforme foi demonstrado anteriormente, a intensificação do uso da internet pelo cidadão comum nos últimos 25 anos tem questionado de forma única as regras tradicionais de determinação da jurisdição. A digitalização das sociedades, por sua vez, acompanha a intensificação dos fluxos de dados entre os territórios dos Estados, em suas respectivas jurisdições. Nesse quadro, é cada vez mais comum a frequência de demandas administrativas e judiciais relacionadas ao acesso a dados de usuários e que envolvem mais de uma jurisdição. As soluções jurídicas para casos típicos do "conflito de jurisdições" têm sido duas: (1) a cooperação internacional, principalmente por meio dos MLATs; e (2) os pedidos de dados feitos diretamente a intermediários.[103]

A ADC 51/2017 discute exatamente qual deve ser o mecanismo de solução predominante a ser aplicado pelo judiciário brasileiro. Independente de qual seja a solução defendida, parece ser necessário definir quais devem ser os critérios de determinação da jurisdição, seja ela referente a qual lei deve ser aplicada (*applicable law*), ou a qual jurisdição compete executar determinada decisão (*enforcement jurisdiction*).

A insuficiência dos atuais paradigmas para resolução de conflitos de jurisdição

102 Tratado de Cooperação Jurídica em Matéria Penal entre a República Federativa do Brasil e a Confederação Suíça, celebrado em Berna, em 12 de maio de 2004. Incorporado ao ordenamento jurídico brasileiro pelo Decreto 6.974/2009.

103 *INTERNET & JURISDICTION. Data & Jurisdiction Program: Cross-Border Access to User Data - Problem Framing*. França. Maio de 2017. p.5. Acessado em:14/04/2018. Disponível em: <https://bit.ly/2J7yZ8O>

em **litígios transfronteiriços da Internet** fica evidente quando são observadas as dificuldades enfrentadas pelos tribunais ao redor do mundo - vide os casos já apresentados neste trabalho e a própria ADC - quando confrontados com a necessidade de eleger um critério determinante de competência para entrega de dados pessoais de usuários. Nesse sentido, é importante ressaltar que discussões internacionais mais intensas têm sido feitas em relação à **entrega de dados de conteúdo** (como comunicações privadas, fotos, e-mails, etc.) dos usuários, havendo, por outro lado, maior consenso em relação ao **fornecimento de dados cadastrais** e **dados sobre o tráfego das informações/ metadados** (números de IP, portas lógicas, etc.)[104].

A essa altura de análise empreendida pelo STF nas controvérsias suscitadas pela ADC nº 51, as distinções entre **fornecimento ou retenção de dados de conteúdo** e **fornecimento de dados cadastrais de usuários e dados de tráfego** devem ser muito bem delimitadas, especialmente porque regimes distintos são aplicáveis, desde a perspectiva da vigência da Constituição, do Marco Civil da Internet e dos tratados de que o Brasil é parte.

O problema de determinação da jurisdição, em sentido amplo, contudo, parece se agravar quando os tribunais analisam uma demanda pelo viés estrito, tomado apenas em função de um dos critérios possíveis de determinação de lei aplicável e da execução de medidas e as decisões judiciais (*enforcement jurisdiction*). Assim, é importante apontar as insuficiências que se apresentam quando da escolha da sede da sociedade empresária como único critério de jurisdição.

Um dos principais problemas suscitados pela escolha da "sede da empresa" como critério de jurisdição reside no fato de de que, muitas vezes, ela não tem qualquer relação com a localização das partes e dos bens envolvidos no litígio, com o local onde foi cometido o ilícito, ou mesmo com o local no qual foram sentidos os efeitos do ato ilícito. Conforme observam La Chapelle e Fellinger:

> Independentemente da localização física das ações ou das partes envolvidas, o sistema MLAT impõe de fato a lei do país receptor do pedido sobre a lei do solicitante, mesmo que não haja conexão territorial com aquele para além do fato de ser a sede empresarial da plataforma ou operador.[105]

A adoção da sede da empresa como único critério de jurisdição tem gerado frustrações em inúmeros órgãos de investigação e de aplicação da lei ao redor do globo (as chamadas "law enforcement authorities - LEAs"), principalmente quando se considera que a maior parte dos serviços online ou digitais do globo concentra sua sede ou origem de fornecimento nos EUA.

O prof. Paul Berman, da George Washington Law School, também critica a utilização da sede da empresa como critério único de jurisdição. Ele afirma que este elemento pode ser arbitrário em certos casos, apesar de ainda poder ser relevante em um contexto mais amplo. Berman teme que o critério da sede da empresa, por si só,

104 Sobre o tema ver, excelentes estudos de *REIDENBERG, Joel R. Technology and Internet jurisdiction. In: University of Pennsylvania Law Review, vol.153, n.6, 2005, p. 1951-1974; KUNER, Christopher. Data protection law and international jurisdiction on the Internet (part 1). In: International Journal of Law and Information Technology*, vol.18, n.2, 2010, p.176-193, 2010. Entre nós, cf. POLIDO, Fabrício B.P. Direito Internacional Privado nas Fronteiras do Trabalho e Tecnologias, cit. esp. p.86 ss.

105 *"Regardless of the physical location of actions or involved parties, the MLAT system de facto imposes the law of the recipient country over the law of the requesting one, even if there is no territorial connection to the latter other than the incorporation of the targeted platform or operator.". LA CHAPELLE, Bertrand de; FELLINGER, Paul. Jurisdiction on the internet: How to move beyond the legal arms race. Observer Research Foundation. 14/10/2016.* Acessado em: 10/04/2018. Disponível em: <https://bit.ly/2Hxy84k>

possa ser utilizado para evitar o acesso a determinadas jurisdições, a partir de uma estratégia deliberada das partes (*forum shopping*), de forma análoga à utilização exclusiva do critério de jurisdição do local onde se armazenam os dados:

> No entanto, em certos casos, o local de incorporação [sede] é tão arbitrário e manipulável quanto à localização dos dados ou do servidor. Indivíduos sem conexão com os Estados Unidos podem facilmente criar uma empresa nos EUA e, em seguida, reivindicar a proteção da lei dos EUA (e dos tribunais dos EUA), embora nada sobre a disputa em questão realmente evidencie uma conexão com os Estados Unidos. [...] **Assim, se a jurisdição estiver automaticamente vinculada ao local de incorporação da empresa, sem uma análise mais aprofundada da realidade social ou econômica subjacente, podem ocorrer distorções**.[106] (destaque nosso)

A construção de uma solução passa por reconhecer que é possível, e muitas vezes necessário, a análise de mais de um critério de determinação da jurisdição, em sentido amplo, a depender do caso concreto com o que juízo se deparar. A doutrina e a jurisprudência internacional têm apontado os seguintes critérios para se determinar que um Estado tem uma conexão substancial e um legítimo interesse ao requer determinados dados armazenados por um provedor de aplicação estrangeiro (empresa), portanto, dentro da categoria de **fornecimento ou retenção de dados de usuários no estrangeiro**:

1. Nacionalidade das vítimas e dos investigados/suspeitos;[107] [108]
2. Residência habitual das vítimas e dos investigados/suspeitos;[109]
3. O local onde foram sentidos os efeitos do ato ou crime;[110]
4. Se o serviço online é direcionado ou acessível a determinado território[111]
5. Localização da sede da empresa;[112]

106 *"Yet, sometimes, place of incorporation is just as arbitrary and manipulated as data or server location. Individuals with no connection with the United States can easily create a U.S. company and then claim protection of U.S. law (and U.S. courts) even though nothing about the dispute at issue really evinces a connection with the United States.[...] Thus, if jurisdiction is automatically tied to place of incorporation without any further analysis of the underlying social or economic reality, distortions may result." BERMAN, Paul Schiff. Legal Jurisdiction and the Deterritorialization of Data. GWU Legal Studies Research Paper Nº.* Maio de 2018. Acessado em:14/04/2018. Disponível em: <https://bit.ly/2EUqdsq>

107 *INTERNET & JURISDICTION. Data & Jurisdiction Policy Options: Cross-Border Access to User Data - Input Document for Workstream I of the Second Global Internet and Jurisdiction Conference . França.* Novembro de 2017. p.6. Acessado em:19/04/2018. Disponível em: <https://bit.ly/2F4o7X2>

108 *"(3) COMITY ANALYSIS.— For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate — [...] (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States[...];". 115th UNITED STATES CONGRESS. The Clarifying Lawful Overseas Use of Data Act (H.R. 4943). 2018.* Acessado em: 22/04/2018. Disponível em: <https://bit.ly/2qXL0WQ>

109 Ibid.

110 Ibid.

111 "O Tribunal de Justiça [*Court of Appeals*] considerou que o Yahoo está territorialmente presente na Bélgica, através da sua participação ativa na economia belga, submetendo-se voluntariamente à jurisdição das autoridades belgas. Em particular, o Tribunal de Justiça manteve o entendimento de que a Yahoo! participa na economia belga através do uso do nome de domínio "www.yahoo.be", da utilização das línguas locais belgas neste site, dos anúncios de pop-up ligados à usuários localizados na Bélgica, e da acessibilidade na Bélgica de serviços ao cliente voltados ao público belga. O Tribunal de Justiça concluiu, assim, que a recusa do Yahoo em fornecer endereços IP dos investigados criminalmente violou a lei do processo penal belga [...] Por seu turno, o Supremo Tribunal Belga confirmou todas as considerações do Tribunal de Apelação, ligando-as essencialmente ao princípio da territorialidade objetiva [*objective territoriality principle*]."(tradução nossa).*L'ECLUSE, Peter; D'HULST, Thibau. Belgium: Supreme Court Condemns Yahoo For Failure To Cooperate With Belgian Law Enforcement Officials. Mondaq.* 11 de janeiro de 2016. Disponível em: <https://bit.ly/2LDFNAO>. Ver também: <https://bit.ly/2O18iVZ>

112 Ibid.

6. Localização dos dados (servidores);[113]

7. A localização dos responsáveis pelo registro de nomes de domínio (*registrars* e *registries*).

Essa variedade de critérios, não exaustiva, foi desenvolvida ao longo de cerca de 30 anos desenvolvimentos doutrinários e jurisprudenciais na Europa e EUA, desde a expansão comercial da internet a partir dos anos 90, o que demonstra que a dificuldade de se determinar a jurisdição, se não é relativamente nova, permanece ainda como um tema controvertido[114]. A falta de consenso ressalta como litígios envolvendo a internet possuem múltiplas dimensões que não podem ser ignoradas por uma adoção pragmática de um único critério de jurisdição a curto prazo.

11. Medidas adicionais para resolução do problema

Os diversos atores que têm debatido o tema da internet e a transferência internacional de dados afirmam existir, basicamente, dois pólos de solução para o problema da jurisdição, as quais têm variado em diferentes matizes de aplicação e combinação.

Um conjunto de soluções têm buscado retomar o poder de regulação e aplicação da jurisdição nacional dos estados soberanos, seja por meio da extensão extraterritorial da sua soberania, ou pela reimposição de fronteiras nacionais na internet. Esta tendência, chamada por La Chapelle e Fehlinger de corrida armamentista jurídica (*legal arms race*) traduz-se na prática por meio de leis estabelecendo localização de servidores em território nacional (*data localisation*); bloqueio de aplicações por meio de provedores de conexão; *enforcement* de decisões nacionais com efeitos extraterritoriais (p. ex. direito ao esquecimento - *Google Spain v González*); regimes jurídicos mais rígidos de responsabilização de intermediários (p. ex. os projetos de lei de uma Diretiva e um Regulamento da União Europeia a obrigar empresas de internet com sede no estrangeiro à designação de um representante legal na UE para processamento de pedidos de dados feitos por autoridades[115]); entre outros.[116]

O outro pólo de soluções tem como objetivo o de fomentar maior cooperação internacional entre os países. Em um extremo desse pólo encontram-se poucos defensores de um tratado internacional de alcance global que regulasse substancialmente o tema, à semelhança da Convenção das Nações Unidas sobre o Direito do Mar de 1982 e o Tratado do Espaço Exterior.[117]

A organização *Internet* & *Jurisdiction* acredita que a solução mais viável seria a criação de um ambiente institucional multissetorial permanente (Estados, empresas, sociedade civil, comunidades técnica e acadêmica) que permita que representantes dos

113 *SUPREME COURT. United States, Petitioner v. Microsoft Corporation*. 27/06/2017. Acessado em: 25/06/2018. Disponível em: <https://bit.ly/2o42Jhl>

114 Do ponto de vista do próprio direito internacional privado, as questões transnacionais da internet oferecem o desenvolvimento do chamado "pluralismo dos métodos", a afetar as distintas variações de determinação da lei aplicável e jurisdição, particularmente pela tendência de modernização das regras de conexão, como ocorre em matéria de obrigações contratuais e extracontratuais (torts) pluriconectadas. Esse movimento tem sido criticamente revisitado pelos excelentes trabalhos da Professora Horatia MUIR WATT, da Escola de Direito da Sciences Po, França. Sobre isso, cf. sumário em *CONFLICT OF LAWS.NET, Guest Editorial: Muir-Watt on Reshaping Private International Law in a Changing World. In*: http://conflictoflaws.net/2008/guest-editorial-muir-watt-on-reshaping-private-international-law-in-a-changing-world/ Acessado em: 25/06/2018.

115 *KATITZA, Rodriguez. A Tale of Two Poorly Designed Cross-Border Data Access Regimes. Electronic Frontier Foundation. 25 de abril de 2018.*

116 *CHAPELLE, Bertrand de la; FEHLINGER. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. Abril de 2016. pp. 10-11.* Acessado em: 26/04/2018. Disponível em: <https://bit.ly/2uh34Li>.

117 *Ibid*, p. 11 e 17.

diversos grupos afetados, a nível global, criem, em conjunto, padrões e mecanismos de cooperação internacional eficientes, indo além dos atuais modelos.[118] A organização baseia seu posicionamento inspirada no processo de governança, aberta, multissetorial e transnacional da camada técnica da internet (IPs, nomes de domínio, protocolos, etc), a qual permitiu a expansão exponencial da rede por meio da adoção de padrões universais.

Por entender que uma harmonização do direito material é pouco realista, a propósito dos mecanismos tradicionais do direito internacional, a organização defende que o enfoque da rede multissetorial deve ser o de buscar (1) padrões processuais comuns, de forma a garantir um mínimo de interoperabilidade entre as jurisdições;[119] e (2) e garantir um devido processo legal transnacional quanto aos pedidos de cooperação, com enfoque em responder "como os pedidos devem ser submetidos" e "como os pedidos devem ser julgados"[120]. Nesse sentido, as normas e procedimentos criados por meio de consensos multissetoriais teriam o *status* de padrões normativos de política pública (*policy standards*) que podem ser adotados de forma escalar; e implementados tanto por meio de simples guias de melhores práticas, como por meio obrigações normativas em leis nacionais ou tratados internacionais. Conforme concluem La Chapelle e Fehlinger:[121]

> Abordar questões relacionadas à governança "sobre" a Internet requer uma mudança de paradigma: da cooperação internacional apenas entre os estados, para a cooperação transnacional entre todas as partes interessadas; de simples tratados intergovernamentais a padrões de política pública multissetoriais; e de instituições intergovernamentais a redes de governança baseadas em questões específicas [*issue-based*]. Longe de rejeitar a cooperação internacional tradicional, no entanto, nossa proposta dá-se como uma extensão construtiva àquela - uma maneira de olhar as práticas atuais sob uma nova luz [...] Ambas têm suas respectivas zonas de validade. Do mesmo modo, o tipo de cooperação transnacional que sugerimos não suprime nem reduz a relevância e a autoridade das instituições e modelos de governança existentes, em particular dos governos nacionais. Pelo contrário, processos multissetoriais podem produzir padrões de políticas públicas [*policy standards*] que sirvam de subsídio a possíveis reformas dos atuais mecanismos de cooperação entre Estados, e podem, posteriormente, ser ainda implementados por organizações multilaterais tradicionais. **A comunidade global precisa intensificar seus esforços para evitar as conseqüências negativas de um corrida armamentista legal [*legal arms race*], a fim de se preservar a natureza global da Internet e abordar adequadamente seus usos indevidos. Precisamos de mecanismos de cooperação inovadores que sejam tão transnacionais quanto a própria Internet** [...].[122] (grifo nosso)

118 *EUROPEAN COMMISSION. Improving cross-border access to electronic evidence.* Acessado em: 03/05/2018. Disponível em: <https://bit.ly/2wiGgBl>

119 *CHAPELLE, Bertrand de la; FEHLINGER. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. Abril de 2016. pp. 21-22.* Acessado em: 26/04/2018. Disponível em: <https://bit.ly/2uh34Li>.

120 Ibid, pp. 23.

121 Ibid, pp. 24.

122 *"Addressing issues related to governance "on" the Internet requires a paradigm shift: from international cooperation only between states, to transnational cooperation among all stakeholders; from pure intergovernmental treaties to policy standards; and from intergovernmental institutions to issue-based governance networks. Far from a rejection of traditional international cooperation, however, this is proposed as a constructive extension – a way to look at current practices in a new, generalized light.[...] Both have their respective zones of validity. Likewise, the type of transnational cooperation envisioned here in no way suppresses or reduces the relevance and authority of existing governance frameworks, in particular national governments. On the contrary, multi-stakeholder processes can produce policy standards that inform the reform of existing interstate cooperation mechanisms, and policy standards can even later be enshrined by traditional mul-*

Ainda circunscrita ao pólo de cooperação internacional, surgem iniciativas que se concentram no fomento a uma maior cooperação bilateral entre os países, como os tratados bilaterais para fornecimento de dados diretamente pelas empresas à autoridades estrangeiras, como estabelecido pela recém aprovada *CLOUD Act*.

As questões suscitadas na ADC 51/2017 refletem claramente as preocupações existentes quanto à tomada unilateral de soluções pelos países ao redor do mundo. Caso a ADC seja julgada procedente no mérito, garantir-se-á, duplamente, segurança jurídica para empresas atuantes no segmento de internet no Brasil e maiores níveis de proteção às comunicações privadas dos usuários brasileiros, particularmente em vista da natureza e da localização dos dados acessados.

Contudo, ainda permanecerão dilemas enfrentados na obtenção de comunicações digitais pelos órgãos jurisdicionais em investigações criminais, que em muitos casos decorrem de necessidades legítimas. O cenário muito realista poderia levar tais órgãos a adotar técnicas de invasão direta aos dispositivos eletrônicos dos investigados, em outras palavras, técnicas de *hacking* ou obtenção clandestina de conteúdo de comunicações, como forma de contornar os problemas de cooperação e obtenção de provas, já que os atuais mecanismos de cooperação internacional chegam a ser ineficientes em muitos casos. Ditas técnicas investigativas não contam com específica regulação no Brasil, podendo, dessa forma, representar mais uma porta para diversos abusos institucionais, caso não sejam acompanhadas de contrapesos e de uma adequada supervisão judicial.

O receio de organizações dedicadas a questões regulatórias e sociais da Internet, como é o caso do IRIS, é de que práticas unilaterais de autoridades de persecução criminal no Brasil escancarem a negativa tendência e abusos de criminalização de legítimos usos da internet e punição de cidadãos-usuários, sem o devido processo, todos ainda presentes na realidade brasileira e de outros países do globo.

Por outro lado, caso a ADC 51/2017 seja rejeitada no mérito - adotando-se o entendimento de que acordos de cooperação internacional seriam somente uma opção para os casos de quebra de sigilo envolvendo dados de brasileiros no estrangeiro em virtude de atos alegadamente criminosos praticados no Brasil - corre-se o risco duplo: de um lado, a imputação de responsabilidade do Estado brasileiro em relação à violação positiva do direito internacional por práticas unilaterais adotadas, inclusive pela não observância de direitos e garantias das partes no processo judicial; de outro, o risco de imposição de obrigações às empresas que violem leis estrangeiras. Isso porque elas estariam suscetíveis a condutas de desconformidade com leis nacionais dos Estados envolvidos e em cujas jurisdições os dados são alcançados e acessados. Ademais, a insegurança jurídica pode ser um de fator de desestímulo a investimentos dessas empresas no país, podendo ser também um barreira de entrada para pequenas e médias empresas.[123]

Devido à natureza transfronteiriça e multissetorial da internet, é provável que qualquer **tentativa unilateral de solução das questões em torno da obtenção de dados seja ineficiente** no médio e longo prazos. Assim, será necessária a atuação tanto dos três poderes, representando o Estado, como dos outros diversos setores envolvidos (sociedade civil, empresas, comunidade acadêmica e organizações internacionais) na

tilateral organizations.The global community needs to step up efforts to avoid the negative consequences of a legal arms race, preserve the global nature of the Internet and address its misuse. We need innovative cooperation mechanisms that are as transnational as the Internet itself and the necessary policy networks and ongoing dialogue processes to produce them.". Ibid. p. 24.

123 Ibid. p. 15.

busca por uma solução, independente de qual dos pólos o Brasil se aproxime na tentativa de endereçar a matéria da ADC 51/2017.

12. Perspectivas de modernização e complementaridade do engajamento internacional dos três poderes

Apesar de reconhecido em diversos âmbitos da ordem jurídica interna brasileira, o debate sobre a relação entre direito internacional e direito interno carece de revisão, como a provocada pela ADC 51/2017 Em tempos da chamada "governança global", Estados, organizações internacionais, organizações não-governamentais, empresas e indivíduos são crescentemente vinculados à observância de normas internacionais. Enquanto destinatários de direitos e de obrigações na ordem internacional, esses sujeitos ocupam posição de destaque no cumprimento, no respaldo, e na garantia de aplicação do direito internacional pelos órgãos dos Estados.

Especialmente no que diz respeito à Constituição Federal de 1988, é necessário revisar os papéis atribuídos aos três poderes da organização do Estado brasileiro nas relações internacionais, de forma a aproximá-los da ideia de um constitucionalismo global. Ainda que o Brasil privilegie contemporaneamente uma solução consentânea com a aceitação e com a observância de normas internacionais, em particular no domínio do Direito Internacional dos Direitos Humanos, as divergências entre monismo e dualismo ainda despertam incongruências.

Além da interdisciplinaridade que o tema da aplicação dos tratados apresenta (ciência política, relações internacionais e direito constitucional), também se evidencia a falta de diálogo entre poderes constituídos no Estado. Como ocorre também em outros ordenamentos, essa relação controvertida parece ser um problema, igualmente, de conflito ou de concorrência entre atribuições políticas e constitucionais, com efeitos tanto em relação ao cumprimento de obrigações do Estado no plano internacional (do que decorrem questões de responsabilidade do Estado), quanto à aplicação das normas internacionais pelos tribunais internos. Não havendo, portanto, equilíbrio ou complementaridade de atribuições, é possível que haja distorções e que esse modelo não seja desejável ou conveniente a países que reclamam espaço e inserção nas relações internacionais, como é o caso do Brasil.

As normas de direito interno são criadas segundo competências e procedimentos reconhecidos pelas constituições domésticas dos Estados (portanto, de acordo com dispositivos constitucionais), e são destinadas à regulamentação dos fatos e das relações jurídicas submetidas a uma supremacia territorial. As normas de direito internacional, por sua vez, são elaboradas e produzidas, desde uma perspectiva tradicional, pelos Estados e pelas organizações internacionais, destinadas a regular as relações internacionais, e de acordo com as respectivas competências atribuídas a esses sujeitos na ordem internacional, como as competências atribuídas pelas constituições domésticas (Estados) e as competências atribuídas por estatutos constitutivos (organizações internacionais).

Da realidade social internacional, decorre a consequência mais importante da interação: Estados, organizações internacionais e indivíduos passam a ser **vinculados ao cumprimento das normas internacionais e fazê-las cumprir**, sobretudo enquanto sejam destinatários de direitos e obrigações na ordem internacional. A tendência con-

temporânea é rechaçar a teoria da transposição das normas internacionais, e admitir sua incorporação automática e eficácia obrigatória no ordenamento interno[124].

Há distinção entre normas de aplicação imediata (ou autoaplicáveis - *self-executing*) e normas de aplicação não imediata. Essa diferença sempre pressupõe estarem as normas internacionais aptas à produção de efeitos no ordenamento doméstico, de modo que o Estado se vê obrigado e vinculado, de acordo com os requisitos que estabelece sua Constituição e com os próprios dispositivos do ato internacional em consideração[125].

Essa matéria, especificamente, é muitas vezes deixada para a interpretação pelos tribunais superiores (ou de instância de revisão constitucional) nos Estados que admitam a incorporação automática dos tratados, divergindo, sobretudo, em relação ao momento em que aquela ocorre: (i) desde a ratificação do tratado, autorizada pelo órgão legislativo (minoritária); ou (ii) desde o momento do efetivo depósito do instrumento de ratificação pelo Poder Executivo na autoridade depositária, com o que o tratado entra em vigor no plano internacional. No entanto, observa-se que deve haver maior participação entre os diferentes Poderes no que diz respeito à elaboração, à assunção e à aplicação de obrigações internacionais. Nos tribunais, é necessário haver maior reflexão sobre as normativas internacionais e seu efetivo status no ordenamento jurídico nacional, bem como elaborar redes de cooperação entre tribunais, associações de magistrados e auxiliares da Justiça.

No âmbito do Poder Executivo, é necessário convocar maior envolvimento dos congressistas nas agendas de política externa brasileira. Isso pode ser realizado, inicialmente, por meio de iniciativas como o Livro Branco da Política Externa Brasileira, do Ministério das Relações Exteriores, que convocou membros da sociedade civil e de diversos setores do Poder Público em sua elaboração[126]. No Congresso Nacional, por sua vez, existe uma demanda clara em torno de projetos de lei que estejam em consonância com as atuais tendências de temas sensíveis da agenda internacional contemporânea. Nesse sentido, torna-se fundamental o acompanhamento das discussões em curso na Organização Internacional do Trabalho (OIT), no Conselho de Direitos Humanos das Nações Unidas, na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), Fórum de Governança da Internet (Internet Governance Forum -IGF) entre outros.

Por meio de ações coordenadas e simbióticas, e não meramente subordinadas, é possível promover efetiva participação dos três poderes na formulação da agenda internacional brasileira. O Poder Judiciário não pode se distanciar dos paradigmas

124 Sobre esse tema, Napoleão Miranda afirma que: "De modo como esse processo está ocorrendo, em particular pela vinculação crescente dos Estados aos organismos internacionais com poder de ingerência sobre a definição de políticas públicas internas, estaria se produzindo, na prática, uma limitação à soberania dos Estados, exigindo, portanto, uma redefinição do alcance da soberania dos Estados no plano internacional, de forma a dar conta da nova realidade. O exemplo mais significativo desse fenômeno, parece-nos, é aquele relativo ao longo processo de constituição da União Europeia, o qual há mais de uma década – desde o Tratado de Maastrich, em 1991, com a constituição do Banco Central Europeu, responsável pela formulação de uma política monetária única na zona de abrangência do euro – vem conformando um amplo conjunto de instrumentos jurídicos, políticos e econômicos que demandam dos Estados que a eles aderem uma limitação, embora não eliminação, da sua soberania para, de forma autônoma, definir os diversos mecanismos de gestão da ordem pública nacional". MIRANDA, Napoleão. Globalização, soberania nacional e direito internacional. In: Revista CEJ, 2004. Disponível em <http://www2.cjf.jus.br/ojs2/index.php/revcej/article/view/638/818>. Acesso em 29 de novembro de 2014.

125 Observando a técnica do Direito Internacional Público e Direito Constitucional, em matéria de tratados, exige-se manifestação expressa e formal da vontade do Estado, que se concretiza por meio de ato complexo exteriorizando a soberania interna no plano internacional. Em geral, o Poder Executivo, representado por Chefes de Estado, chefes de governo e ministérios das relações exteriores, negocia e conclui os tratados; ao Poder Legislativo (parlamento ou congresso) cabe autorizar a conclusão e ratificação do tratado convencionado pelo Estado em suas relações exteriores. Com relação à norma internacional consuetudinária, o respeito dá-se pela observância, prática dos órgãos internos ou aceitação, pelo silêncio, da prática dos demais.

126 Até o momento, contudo, não há informações sobre o lançamento da publicação pelo Ministério das Relações Exteriores, que tem sido sistematicamente cobrado desde 2014 por organizações da sociedade civil e entidades governamentais. Ver status em: http://www.ebc.com.br/livro-branco-da-politica-externa-brasileira.

contemporâneos do pluralismo jurídico e da legitimidade discursiva das normas internacionais. Ainda que a incorporação dos atos internacionais no ordenamento brasileiro leve à possibilidade de seu controle constitucional, as decisões devem considerar sua repercussão, para o Brasil, no sistema internacional. Dessa forma, é necessária simbiose entre os Três Poderes no tratamento das questões relacionadas às relações exteriores, para simplesmente evitar que um ato unilateral do Brasil possa repercutir no sistema internacional. As decisões, como esta da ADC 51, devem evitar expor o Estado brasileiro ao risco de descumprimento de obrigações internacionais e eventual imputação de responsabilidade, em âmbito internacional.

13. Recompreensão da soberania e compartilhamento de jurisdições

A Internet não apenas se representa por uma estrutura técnica aperfeiçoada fundada em modernos padrões de comunicação e conexão. Em sua evolução para uso civil e comercial, desde o final da década de 1990, ela tem constituído verdadeiro espaço transnacional da informação e tecnologias. Atores estatais e não-estatais, como organizações, empresas e indivíduos envolvem-se em distintas interações que se projetam para além das fronteiras meramente territoriais. Enquanto o Estado permanecer com determinados poderes regulatórios, adjudicatórios e executivos, é também possível verificar que a concepção tradicional de soberania, legada da ordem vestifaliana, sofre relativizações conceituais e operacionais muito concretas.

Estados não mais podem exercer pleno controle sobre comportamentos, práticas e transações sobre pessoas residentes e domiciliadas em seus territórios, sem recorrer à observância de obrigações internacionais e à cooperação com outros Estados e organizações. A noção de soberania imediatamente relacionada a este sistema vem sendo mitigada nos últimos trinta anos, com o avanço da globalização e das tecnologias de informação e comunicação, em favor de processos transnacionais centrados em atores outros que não o Estado[127].

Parte desse processo de transformação do paradigma tradicional de soberania decorre dos efeitos da globalização na organização e projeção de grupos econômicos multinacionais e das novas dinâmicas no fluxo de capitais e serviços. A estrutura tradicional destes grupos econômicos multinacionais sofreu uma transformação que a primeira vista pode parecer paradoxal. Ao mesmo tempo em que seu raio de expansão e projeção aumentaram consideravelmente ao redor do globo, diversas estruturas essenciais que se distribuiriam conjuntamente com a transnacionalização da empresa acabaram, ao contrário, a se concentrar enormemente em polos regionais de alta tecnologia, qualificação e serviços[128]. O alcance internacional das firmas torna-se, assim, inversamente proporcional à centralização de seus núcleos de produção de valor mais essenciais[129].

127 SASSEN, Saskia. "When national territory is home to the global: Old borders to novel borderings", In: *New Political Economy*, v. 10, n. 4, p. 523–541, 2005, p.524.

128 Sobre o tema, cf. SASSEN, Saskia. *Global city*. Princeton, NJ: Princeton University Press, 1991.

129 Do fenômeno de internacionalização da atividade empresarial de grupos econômicos - em especial, os que englobam provedores de aplicação de internet - pode-se observar o surgimento de diversos debates jurídicos. Dentre eles, um dos que parece mais controverso atualmente diz respeito à possibilidade de responsabilização de uma empresa pertencente a um grupo econômico - na maioria das vezes, uma subsidiária ou afiliada - em decorrência de conflito relativo, em verdade, à empresa que comanda aquele determinado grupo de sociedades empresárias. A jurisprudência nacional, desde a segunda instância até as decisões dos tribunais superiores, encontra-se em dissenso quanto ao tema, apresentando fundamentações muitas vezes discordantes para as decisões mesmo quando estas levam a um mesmo resultado fático. A título de exemplo, cita-se as decisões do Agravo de Instrumento nº 2184235-15.2016.8.26.0000, do TJ-SP, e do Mandado de Segurança Crime nº 1.396.365-4, do TJ-PR - essas decisões, diametralmente opostas em seus resultados, demonstram, em suma, o mérito central dessa divergência argumentativa.

No caso das empresas de Internet, estes núcleos tomam a forma de seus departamentos de pesquisa e desenvolvimento (P&D), de data centers e de centrais operação técnica, em detrimento das subsidiárias no estrangeiro que servem apenas de ponta de lança para a conquista e melhor aproveitamento de novos mercados. Uma analogia ilustrativa seria a comparação com os impérios coloniais da Era Moderna: embora suas extensões territoriais tivessem alcançado proporções dezenas de vezes maiores que seus territórios originais, e sua presença estivesse consideravelmente mais espalhada pelo globo, as riquezas e o poder político centralizaram-se quase completamente nas metrópoles. Diferentemente destes impérios, entretanto, os Estados são cada vez mais obrigados a cooperar mutuamente - e não se impor - como forma de resguardar seus interesses (e até mesmo sua soberania material) da melhor forma possível.

A essência de cooperar - e não simplesmente coexistir (como era característica da ordem internacional anterior à emergência das Nações Unidas em 1945, entre as razões planas da paz e segurança internacional) -, é que ainda hoje caracteriza a dinâmica das relações transnacionais. A esse fator associa-se a realidade de crescente interdependência jurisdicional - regulatória, adjudicatória e executiva, entre os atores estatais e não-estatais - e que ainda se fundamenta na **observância de tratados e convenções**, mas também no atendimento de certas expectativas legítimas envolvidas no trânsito econômico internacional[130]. Elas se manifestam em diversas áreas de intensa mobilidade de fatores: bens, capitais, serviços, tecnologias e informações - nos campos do comércio, meio ambiente, propriedade intelectual, tributação, investimentos, na proteção de direitos humanos e no combate global à corrupção.

A arquitetura da Internet, como é conhecida, desde uma natureza global, multiterritorial, de estrutura descentralizada e reticular, parece propugnar especificamente por uma mudança de concepção de soberania e jurisdição, em distintas perspectivas: política, econômica, jurídico-substantiva e procedimental. Espaços jurisdicionais entre Estados não mais são exclusivos ou em conflito; eles se organizam em compartilhamento. Esse compartilhamento é necessário para que autoridades administrativas e jurisdicionais domésticas e intracomunitárias (como é o caso da União Europeia) possam solucionar questões envolvendo o lado regulatório e conflitual (em sentido aqui litigioso, do contencioso) das interações entre governos, empresas e usuários na Internet[131].

Uma das manifestações mais concretas do **compartilhamento de jurisdições** é a decisão coordenada entre Estados e organizações por regular substantiva e processualmente as relações e interações que emergem da Internet, como em matéria de comércio e contratos eletrônicos, tratamento de dados, comunicações privadas e propriedade intelectual. A explicação parece mais intuitiva, pois é a opção fornecida pelo direito internacional e direito comunitário (e.g. direito da União Europeia) em facilitar e promover modelos de harmonização, uniformização, unificação do direito privado - civil e comercial -, sobretudo para fatos, situações e relações jurídicas que se vinculam a distintos sistemas jurídicos, afetando, pois, interações humanas que transcendem fronteiras e são de preocupação global.

Desde o final da década de 1990, com o advento da Internet, a Comissão das Nações Unidas para Direito do Comércio Internacional (UNCITRAL), por exemplo, intensificou os trabalhos de preparação de tratados, convenções e leis-modelo para

130 Cf. POLIDO, Fabrício B. P. *Direito internacional privado nas fronteiras do trabalho e tecnologias: ensaios e narrativas na era digital*. 1.ed. Rio de Janeiro: Lumen Iuris, 2018, p. 73 ss.
131 Idem, p.75.

aproximar as fórmulas legislativas em tema de comércio eletrônico, forma, certificação de assinaturas, segurança de dados e confiança em contratos eletrônicos[132]. A atuação dos Membros da ONU nesses campos, como revelado pelas competências da UNCITRAL , demonstra a necessidade de contínuos estudos e esforços em torno da compreensão sobre e maturação das tecnologias integradas de comunicação e informação no comércio eletrônico. Essas soluções ainda não poderiam permanecer unilaterais pelos modelos legislativos domésticos, sob o risco de fragmentação normativa.

O mesmo pode ser afirmado em relação aos limites que podem ser postos às tendências de unilateralização da aplicação da lei ou extensão de seus efeitos para alcançar fatos e situações ocorridas no estrangeiro (como a aplicação extraterritorial da lei doméstica). Eles devem guiar restritivamente as escolhas de jurisdição prescritiva/regulatória, porque há áreas de sensível regulação e interesse público que podem justificá-las (e.g. tributação, antitruste, meio ambiente, persecução criminal e violação transfronteiriça de direitos humanos). No entanto, essa escolha não poderia ser meramente adotada pelos estados sem um balanço ou fino equilíbrio a respeito das repercussões políticas, econômicas e sociais dentro de seus territórios e para além de suas fronteiras domésticas.

A outra expressão do compartilhamento jurisdicional decorre da vertente da **cooperação jurídica** para a aplicação das leis, atos e decisões pelas autoridades administrativas e tribunais domésticos dos estados e regionais/comunitários. Ela é peça-chave na compreensão de questões suscitadas em controvérsia na ADC 51/2017. No curso do processo civil transnacional (ou contencioso internacional privado), é possível verificar como os litígios transfronteiriços da Internet dependem do compartilhamento dos espaços jurisdicionais, particularmente para o adequado funcionamento da justiça e acesso à jurisdição por usuários e empresas da Internet.

Estados, não diferentemente, permanecem apoiados pelas estruturas de cooperação jurídica internacional, que se apresentam reguladas positivamente, a exemplo das fórmulas oferecidas por tratados e leis internas (no Brasil, a Constituição, códigos processuais e regulamentos) e centrados em modelos cartoriais-burocráticos, pois dependem da atuação autoridades centrais, tribunais e, residualmente, via diplomática; por outro, dependem também do entrosamento e participação de atores não-estatais para a solução judicial dos litígios, particularmente em domínios especializados, envolvendo organizações, indivíduos, sociedade civil e indústria.

No campo da Internet e jurisdição, as questões de governança também são centrais e hoje admitem a necessidade do diálogo multissetorial que não passaria distante do objetivo de discutir seriamente formas de controle e efetividade de mecanismos vigentes de cooperação jurídica internacional para solução de litígios transnacionais da Internet[133].

132 Ver, por exemplo, os produtos normativos desenvolvidos pela UNCITRAL, em tratados e também leis-modelos e princípios, recomendações: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html. Para evolução sobre o tema, ver ainda POLIDO, Fabrício B. P. e OLIVEIRA DA SILVA,, Lucas Savio. Contratos internacionais eletrônicos e o direito brasileiro: entre a insuficiência normativa doméstica e as soluções globais. In: *Seqüência: Estudos Jurídicos e Políticos* vol. 38 (2017), p.157-188.

133 LA CHAPELLE, Bertrand de; FEHLINGER, Paul. *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*. 2016, p 7; POLIDO, Fabrício B. P. *Direito internacional privado nas fronteiras do trabalho e tecnologias: ensaios e narrativas na era digital*. cit. esp. p.84-85.

14. Conclusões

Em vista do exposto, e como expressado pelo IRIS em sua participação como 'Amicus Curiae', observa-se a necessidade de que as controvérsias jurídicas ventiladas na ADC 51/2017 e a repercussão das questões constitucionais relevantes sejam escrutinadas pelo Egrégio Supremo Tribunal Federal com a devida premência e as precauções interpretativas relativamente às normas da Constituição e de tratados e convenções de que o Brasil é parte.

Com a ADC nº 51/2017, o STF tem a oportunidade, igualmente, de considerar questões emergentes da natureza multissetorial da regulamentação da Internet e observância de regimes de cooperação jurídica internacional no curso do contencioso transnacional – civil, comercial e criminal – envolvendo a rede mundial de computadores.

É verdade que a falta de coordenação das estruturas de cooperação jurídica internacional e de critérios uniformes de jurisdição para solução de litígios da internet poderia suscitar dificuldades ainda mais presentes no cotidiano dos tribunais e autoridades administrativas que lidam com o contencioso transnacional. Essas falhas, contudo, nunca poderiam servir de fundamento para denegação de justiça ou supressão de etapas fundamentais do processo com respeito aos direitos fundamentais das partes e daqueles que são diretamente afetados pelas pretensões aduzidas em juízo – os usuários da internet, seus dados pessoais e conteúdo das comunicações privadas.

Da mesma forma, como observado ao longo do Memorial, o ordenamento jurídico brasileiro, integrado por normas da Constituição Federal, do Código de Processo Civil, do Decreto nº 3.810/2001 e do Marco Civil da Internet, estabelece - e não afasta - a observância de procedimentos de cooperação internacional mediante recurso a acordos de cooperação e assistência mútua jurisdicional e administrativa, como mesmo representam o Acordo Brasil-Estados Unidos e o Acordo Brasil-Suíça. Na visão do IRIS, a constelação normativa ali existente - e vigente - para regulação material e procedimental de fatos, situações e relações jurídicas emergentes da Internet - admitidas em seus elementos de conexão, de internacionalidade-, **não derroga o cumprimento ou adimplemento de obrigações internacionais bilaterais e multilaterais fundadas em tratados de que de que o Brasil é parte**.

Ao contrário, o cumprimento das obrigações convencionais é enfatizado e assegurado pela vinculação expressa da República Federativa do Brasil a princípios de soberania, não ingerência em assuntos internos e cooperação internacional em todas suas relações com Estados estrangeiros, como estabelece o próprio Art.4º da Constituição. Assim como em outras áreas - meio ambiente, direitos humanos, combate global à corrupção, tributação, antitruste - com forte apelo à aplicação extraterritorial das leis nacionais (uma vertente excepcional da jurisdição), a Internet não estaria imune à incidência de regras de cooperação jurídica internacional. Isso porque, em suma, a cooperação é que assegura duplamente o diálogo entre, e o compartilhamento de, jurisdições na ordem global.

15. Referências

Livros e artigos

ACIOLY, Hildebrando. Tratado de Direito Internacional Público. Volume I. São Paulo : Quartier Latin, 2009.

BARTLETT, Jamie.The online surveillance debate is really about whether you trust governments or not. In: *The Telegraph***,** em 06/11/2015. Disponível em: <https://www.telegraph.co.uk/technology/internet-security/11979682/The-online-surveillance-debate-is-really-about-whether-you-trust-governments-or-not.html>, acesso em 16 de junho de 2018.

BREWER, David. *Obtaining Discovery Abroad: The Utility of the Comity Analysis in Determining Whether to Order Production of Documents Protected by Foreign Blocking Statutes*. Houston Journal of International Law. Vol. 22, nº 3. 2000. Acessado em: 22/03/2018. Disponível em: <https://goo.gl/dxRbwp>.

COPETTI, Alfredo; FISCHER, Ricardo Santi. A natureza dos direitos e das garantias dos usuários de internet: uma abordagem a partir do modelo jurídico garantista. In:. LEITE, George Salomão; LEMOS, Ronaldo (coord.). *Marco Civil da Internet*. São Paulo: Atlas, 2014.

COSETTI, Melissa Cruz. Facebook revela dados do Brasil na CPBR9 e WhatsApp 'vira ZapZap'. Techtudo. 28/01/2016. Acessado em 20/02/2018. Disponível em: <https://goo.gl/g7Pm5p>.

DOLINGER, Jacob. *Direito Internacional Privado.* Parte Geral, 10.ed. Rio de Janeiro: Forense, 2011

DONEDA. Danilo. A proteção dos dados pessoais como um direito fundamental. In: Espaço Jurídico**.**v. 12, n. 2, p. 106, jul./dez. 2011. Disponível em: <https://dialnet.unirioja.es/descarga/articulo/4555153.pdf>, acesso em 16 de julho de 2018.

FERRAJOLI, Luigi. *Derechos y garantías*: la ley del más débil. Madrid: Editorial Trotta, 2010

FISCHER, Camille - Electronic Frontier Foundation, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data*. 08/02/2018. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/R9zNKh>

GHAPPOUR, Ahmed.*Searching places unknown: law enforcement jurisdiction on the dark web*. Stanford Law Review. 69.4. Abril de 2017.p.3. Acessado em: 25/03/2018. Disponível em: <https://stanford.io/2pIBCGa>

GIANNATTASIO, Arthur. Roberto Capella. *O Direito Internacional entre Dois Pós-Modernismos: A Ressignificação das Relações entre Direito Internacional e Direito Interno*. In: *Revista Eletrônica do CEDIN*, v. 6, 2010, p. 42-90. Disponível em: <https://goo.gl/DCrJgT>

GIACCHETTA, André; MENEGUETTI, Pamela. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: *Marco Civil da Internet.* LEITE, George Salomão; LEMOS, Ronaldo (coord.). São Paulo: Atlas, 2014.

INTERNET & JURISDICTION. *Data & Jurisdiction Program: Cross-Border Access to User Data - Problem Framing*. França. Maio de 2017. p.5. Acessado em:14/04/2018. Disponível em: <https://bit.ly/2J7yZ8O>

INTERNET & JURISDICTION. *Data & Jurisdiction Policy Options: Cross-Border Access to User Data - Input Document for Workstream I of the Second Global Internet and Jurisdiction Conference* . França. Novembro de 2017. p.6. Acessado em:19/04/2018. Disponível em: <https://bit.ly/2F4o7X2>

IRIS. *Competência Internacional dos Tribunais Domésticos e Litígios de Internet*, 2018.. Disponível em: <https://goo.gl/7RveQq>. Acesso em: 25/03/2018.

JAYCOX, Mark; e TIEN, Lee. Reforms Abound for Cross-Border Data Requests. Electronic Frontier Foundation. 27/12/2015. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/2WJAfV>

KATITZA, Rodriguez. *A Tale of Two Poorly Designed Cross-Border Data Access Regimes*. Electronic Frontier Foundation. 25 de abril de 2018.

KOHL, Uta. Jurisdiction and the Internet: Regulatory Competence over Online Activity, Cambridge: Cambridge University Press, 2007, p.24.

KUNER, Christopher. Data protection law and international jurisdiction on the Internet (part 1). In: *International Journal of Law and Information Technology*, vol.18, n.2, 2010, p.176-193, 2010.

KUNER, Christopher, *Internet Jurisdiction and Data Protection Law*: An International Legal Analysis (Part 1). International Journal of Law and Information Technology, Vol. 18, 2010. p. 176.

LA CHAPELLE, Bertrand de; FEHLINGER, Paul. *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation*. Acessado em: 15/02/2018. 2016. p. 4. Disponível em: <https://goo.gl/uy7Fpe>.

L'ECLUSE, Peter; D'HULST, Thibau. *Belgium: Supreme Court Condemns Yahoo For Failure To Cooperate With Belgian Law Enforcement Officials*. Mondaq. 11 de janeiro de 2016. Disponível em: <https://bit.ly/2LDFNAO>. Ver também: <https://bit.ly/2O18iVZ>.

MAXWELL, Winston; WOLF, Christopher. *A Global Reality: Governmental Access to Data in the Cloud 2* (July 18, 2012). A Hogan Lovells White Paper (international law firm). 18/07/2012. Acessado em: 05/03/2018. Disponível em: <https://goo.gl/TA33bN>.

MILLS, Alex. Rethinking Jurisdiction in International Law. In: *British Yearbook of International Law*, volume 84, n. 1, 1 2014, pp. 187–239.

MIRANDA, Napoleão. Globalização, soberania nacional e direito internacional. In: *Revista CEJ*, 2004. Disponível em <http://www2.cjf.jus.br/ojs2/index.php/revcej/article/view/638/818>. Acesso em 29 de novembro de 2014.

POLIDO, Fabrício B. P. *Direito Internacional Privado nas Fronteiras do Trabalho e Novas Tecnologias*: ensaios e narrativas na era digital. Rio de Janeiro: Lumen Iuris, 2018.

POLIDO, Fabrício. *Brasil, cooperação jurídica internacional e Internet*. Jota, 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/brasil-cooperacao-juridica-internacional-e-internet-31072017#_ftn1>

POLIDO, Fabrício B. P. e OLIVEIRA DA SILVA, Lucas Savio. Contratos internacionais eletrônicos e o direito brasileiro: entre a insuficiência normativa doméstica e as soluções globais. In: *Seqüência: Estudos Jurídicos e Políticos* vol. 38 (2017), p.157-188.

POLIDO, Fabrício B. P. Fundamentos, estruturas e mecanismos da cooperação jurídica internacional e o Código de Processo Civil brasileiro. In: Cooperação Jurídica Internacional. Revista dos Tribunais vol.990. Caderno Especial. Abril de 2018.

PONTES DE MIRANDA, Francisco Cavalcanti. *Comentários à Constituição de 1967*, Vol. I (arts. 1º - 7º). São Paulo : Editora Revista dos Tribunais, 1967

REIDENBERG, Joel R. Technology and Internet jurisdiction. In: *University of Pennsylvania Law Review*, vol.153, n.6, 2005, p. 1951-1974.

SASSEN, Saskia. *Global city*. Princeton, NJ: Princeton University Press, 1991.

SASSEN, Saskia. "When national territory is home to the global: Old borders to novel borderings", In: *New Political Economy*, v. 10, n. 4, p. 523–541, 2005.

SOLOVE, Daniel J. A Brief History of Information Privacy Law. In: *Proskauer on Privacy,* PLI, 2006, p. 5. Disponível em: <https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications>, acesso em 16 de julho de 2018.

SOLOVE, Daniel J. *Nothing to Hide:* The False Tradeoff between Privacy and Security. Yale University Press, 2011.

THEODORO, Humberto Jr. *Curso de Direito Processual Civil - Volume 1*. 56ª edição .Rio de Janeiro: Editora Forense, 2015. p. 410.

WILSKE, Stephan; SCHILLER, Teresa. International Jurisdiction in Cyberspace: Which States May Regulate the Internet? Federal Communications Law Journal, vol. 50, issue 1, pp.117 – 178, 1997.

WOODS, Andrew Keane; SWIRE Peter. *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems.* Lawfare Blog. 06/02/2018. Acessado em: 22/03/2018. Disponível em: <https://bit.ly/2HW2kCo>

Leis e decisões

BRASIL, *Decreto nº 3.810*, de 2 de maio de 2001. Disponível em: <https://goo.gl/oiE1G3> Acessado em: 02/04/2018.

BRASIL, Decreto nº 6.974/2009, de 07 de outubro de 2009. <http://www.planalto.gov.br/CCIVil_03/_Ato2007-2010/2009/Decreto/D6974.htm>. Acesso em 16/07/2018.

BRASIL, Lei 12.965/2014, de 14 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 02/04/2018.

CIDH. *Castillo Petruzzi y otros Vs. Perú. Fondo, Reparaciones y Costas*. Sentencia de 30 de mayo de 1999. Serie C No. 52.

CIDH. *Baena Ricardo y otros Vs. Panamá. Fondo, Reparaciones y Costas*. Sentencia de 2 de febrero de 2001. Serie C No. 72,

CIDH. Caso del Tribunal Constitucional (Camba Campos y otros) Vs. Ecuador. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 28 de agosto de 2013. Serie C No. 268,

CJUE, *Caso C-131/12*. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Disponível em: <https://goo.gl/Hyk4XM> .

CJUE, *Caso C-230/14*. Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság. Disponível em: <https://goo.gl/aSfaEJ> .

CONVENÇÃO SOBRE O CIBERCRIME - Budapeste, 23/11/2001. Acessado em: 05/03/2018. Disponível em: <https://goo.gl/twrwQu>.

ONU. Conselho de Direitos Humanos, *Resolução n A/HRC/32/L.20*, de 30 de junho de 2016. Disponível em: <https://www.article19.org/data/files/Internet_Statement_Adopted.pdf>, acesso em 16 de julho de 2018.

STJ, *RMS 44.892/SP*, Rel. Ministro Ribeiro Dantas, Quinta Turma, acórdão de 5 de abril de 2016, DJe 15.04.2016.

STJ, *Recurso em Mandado de Segurança n. 55.109/PR*, Rel. Min.Joel Paciornik, acórdão de 17.12.2017 (MPF vs. Yahoo!, caso *Castanheira-Brasil 247*).

THE SENATE OF THE UNITED STATES. S.2383/H.R. 4943. *The Clarifying Overseas Use of Data*

(CLOUD ACT). 2018. Acessado em: 22/03/2018. Disponível em: <https://goo.gl/4gn81j>.

TJSP, *Agravo de Instrumento nº 2184235-15.2016.8.26.0000*, 35 Câmara Civil, Relator Desembargador Alcides Leopoldo e Silva Júnior, julgado em 21/02/2017.

TJPR, *Mandado de Segurança Crime nº 1.396.365-4*, 3ª Câmara Tribunal, Relator Desembargador Arquelau Araujo Ribas, julgado em 19/05/2015, DJe 04/12/2015.

UE, *Diretiva 95/46/EC*, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995. Disponível em: <https://goo.gl/BnhbK1>

USA, CALDER, Petitioner, v. JONES, Respondent. Nº. 82-1401. *Appeal from the Court of Appeal of California*. 20/03/1984. Acessado em: 26/03/2018. Disponível em: <https://goo.gl/wff9c2>.

USA, *Code § 2703* - Required disclosure of customer communications or records. Acessado em: 01/03/2018. Disponível em: <https://goo.gl/ojNv2A>.

USA, Court of Appeals for The Second Circuit. Docket No. 14 2985 - In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation. 14 de Julho de 2016.Acessado em: 01/03/2018. Disponível em: https://goo.gl/Kz7hWp.

US DEPARTMENT OF JUSTICE. *Justice Information Sharing - Electronic Communications Privacy Act of 1986 (ECPA)*. 30/07/2013. Acessado em: 01/03/2018. Disponível em: <https://goo.gl/hdv2on>.

USA, Disctrict Court Southern of New York. Juiz James C. Francis IV. p. 26. Acessado em: 01/03/2018. Disponível em: https://goo.gl/7YrorZ.

USA, Petitioner v. MICROSOFT CORPORATION, Respondent. *Brief for the United States* - Nº 17-2.Acessado em: 01/03/2018. Disponível em: <https://goo.gl/X5kVUj>.

USA, Petitioner, v. MICROSOFT CORPORATION, Respondent. Nº. 17-2. *Oral argument before the Supreme Court of the United States*.27/02/2018. Acessado em: 20/02/2018. Disponível em: <https://goo.gl/aDrz8q>.

USA, SIOUX TRANSPORTATION, INC, Plaintiff, v. XPO LOGISTICS, INC. ET AL, Defendants. Nº. 5:2015cv05265. *Memorandum Opinion and Order granting Motion to Dismiss Case Without Prejudice*. 22/12/2015. Acessado em: 26/03/2018. Disponível em: <https://goo.gl/sLEYdz>.

USA, Supreme Court. .*MORRISON et al. v . NATIONAL AUSTRALIA BANK LTD. et al.*

561 U.S. 247 (2010).18/07/2012. Acessado em: 05/03/2018. Disponível em: <https://bit.ly/2GbTd08>.

USA, Yahoo! Inc. v. LA LIGUE CONTRE LE RACISME ET, 145 F. Supp. 2d 1168 (N.D. Cal. 2001). Disponível em: <https://goo.gl/wM5dZQ> .

USA, Yahoo! Inc., a Delaware Corporation, Plaintiff-appellee, v. La Ligue Contre Le Racisme et L'antisemitisme, a French Association; L'union Des Etudiants Juifs De France, a French Association, Defendants-appellants, 433 F.3d 1199 (9th Cir. 2006) Disponível em: <https://goo.gl/E41b4H>.

USA, ZIPPO MANUFACTURING COMPANY, Plaintiff, v. ZIPPO DOT COM, INC., Defendant. Nº. 96-397. *Memorandum Opinion*. 16/01/1997. Acessado em: 26/03/2018. Disponível em: <https://goo.gl/DUXEbG> .

Outros documentos e notícias

Coalition Letter Opposing the CLOUD Act. 12/03/2018. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/qYB2EG>.

Com 50 milhões de usuários, Brasil é segundo no ranking do Instagram. Folha de S. Paulo. 28/10/2017. Acessado em 20/02/2018. Disponível em: <https://goo.gl/hgh3gol>.

CONFLICT OF LAWS.NET, *Guest Editorial:* Muir-Watt on Reshaping Private International Law in a Changing World. In: http://conflictoflaws.net/2008/guest-editorial-muir-watt-on-reshaping-private-international-law-in-a-changing-world/ Acessado em: 25/06/2018.

CONSELHO NACIONAL DE JUSTIÇA. Relatórios Quantitativos - Interceptações Telefônicas. 2016. Tabelas 5 e 6. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/kE5ZAU>.

EUROPEAN COMMISSION. *Improving cross-border access to electronic evidence*. Acessado em: 03/05/2018. Disponível em: <https://bit.ly/2wiGgBl>

FACEBOOK Inc. Relatório de Transparência. 2016. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/aLZQZh>.

FACEBOOK Inc. Guidelines - Informações para Autoridades Policiais. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/uYDvfX>.

FREEDOM HOUSE. *Freedom on the Net Report 2017*: manipulating Social Media to Undermine Democracy. Disponível em: <https://freedomhouse.org/report/freedom-net/freedom-net-2017>, acesso em 16 de junho de 2018

GOOGLE Inc. Perguntas frequentes sobre o processo jurídico para solicitações de dados de utilizadores. Acessado em: 23/02/2018. Disponível em: <https://goo.gl/4FfVKz>

How to fix MLATs — and a path toward resolving jurisdictional issues. Access Now. 23/05/2017. Disponível em: <https://goo.gl/JCNv5i>.

IRIS. Workshop: Jurisdição e cooperação jurídica internacional nos conflitos da internet - Parte 3. Novembro de 2017. Entre 00:00 e 26:00 minutos. Acessado em: 15/02/2018. Disponível em: <https://goo.gl/QZyv3H>

Metadata is not 'content' under Stored Communications Act. ESI Case Law, Março de 2013. Disponível em: <https://www.ilsteam.com/metadata-is-not-content-under-the-stored-communications-act>.

SYMANTEC CORPORATION. Norton Cyber Security Insights Report 2017 Global Results. 2018. Acessado em: 15/02/2018. Disponível em: <https://goo.gl/RC7q5i>

The Hamburg Commissioner for Data Protection and Freedom of Information. Facebook's real name policy remains in force for the time being. 2016. Disponível em: <https://goo.gl/eWwhZN>

The urgent need for MLAT reform. Access Now. 12/09/2014. Disponível em: <https://goo.gl/dcqCWi>.

USA, *Executive Agreement Requirements.* S.2383/H.R. 4943 .The Clarifying Overseas Use of Data Act. p. 13. Acessado em: 23/02/2018. Disponível em:<https://bit.ly/2G3laqY>.

WATTLES,Jackie. *Microsoft's epic court battle with DOJ is coming to an end*. CNN Tech. 23/03/2018. Acessado em: 27/03/2018. Disponível em: <https://cnnmon.ie/2DZeKXV>.

WhatsApp chega a 120 milhões de usuários no Brasil. O Estado de S. Paulo **.**29/05/2017. Acessado em 20/02/2018. Disponível em: <https://goo.gl/gJVGEF>.