UNIVERSIDADE DE BRASÍLIA – UnB
FACULDADE DE DIREITO – FDD
CURSO DE GRADUAÇÃO EM DIREITO

VICTOR HUGO PINHEIRO CASCAIS MELEIRO

OS DESAFIOS DA COLETA DE DADOS ELETRÔNICOS NO EXTERIOR E A COOPERAÇÃO INTERNACIONAL PARA ACESSO A PROVAS

BRASÍLIA,

2018

VICTOR HUGO PINHEIRO CASCAIS MELEIRO

OS DESAFIOS DA COLETA DE DADOS ELETRÔNICOS NO EXTERIOR E A COOPERAÇÃO INTERNACIONAL PARA ACESSO A PROVAS

Monografia apresentada ao Programa de Graduação da Faculdade de Direito da Universidade de Brasília (UnB) como requisito parcial à obtenção do grau de Bacharel em Direito.

Orientador: Pedro Felipe de Oliveira Santos

BRASÍLIA,

2018

VICTOR HUGO PINHEIRO CASCAIS MELEIRO

OS DESAFIOS DA COLETA DE DADOS ELETRÔNICOS NO EXTERIOR E A COOPERAÇÃO INTERNACIONAL PARA ACESSO A PROVAS

Monografia apresentada no Programa de Graduação da Faculdade de Direito da Universidade de Brasília (UnB) como requisito parcial para a obtenção do título de Bacharel em Direito. Aprovada em 29 de junho de 2018 pela **Banca Examinadora** constituída pelos seguintes professores:

Me. Pedro Felipe de Oliveira Santos
(Orientador – Presidente)

Dr. João Costa Ribeiro Neto
(Membro)

Dr. Alexandre Kehrig Veronese
(Membro)

BRASÍLIA,
2018

Agradeço aos meus pais, que nunca pouparam esforços para investir em minha educação;
e ao meu orientador, sempre muito dedicado e atencioso.

RESUMO

O presente estudo aborda as complexidades que envolvem a coleta de dados eletrônicos armazenados no exterior, para fins de investigação ou instrução criminal, e divide-se em quatro partes. Primeiro, descreve-se o fenômeno do crescente acesso da população às plataformas eletrônicas de comunicação, com relação causal direta na produção de novos tipos de dados, os quais, nesta etapa do trabalho, são examinados consoante o paradigma do Marco Civil da Internet. Segundo, analisa-se o conflito entre as autoridades públicas e as empresas de tecnologia a respeito das metodologias mais eficientes ou legítimas para a coleta de dados no exterior, seja por meio da requisição direta a filiais de empresas no Brasil, seja por meio da cooperação jurídica internacional. Terceiro, são analisadas as propriedades jurídicas da cooperação internacional em matéria penal, com alicerce em dados empíricos do funcionamento do *Mutual Legal Assistance Treaty* (MLAT) entre Brasil e Estados Unidos, quando destinado à coleta de dados telemáticos. Quarto, apresentam-se soluções alternativas para a controvérsia no cenário internacional, com especial atenção ao *CLOUD Act* nos EUA, e outras técnicas controversas de investigação e acesso a dados.

Palavras-chave: Coleta de dados eletrônicos. Dados de comunicação privada. Investigação de crimes modernos. Provedores de serviços de Internet. Cooperação jurídica internacional. Privacidade e segurança.

ABSTRACT

The present study addresses the complexities involved in the collection of electronic data stored abroad, for purposes of criminal investigation or prosecution, and is divided into four parts. First, the phenomenon of increasing access of population to electronic communication platforms is described, with a direct causal link to the creation of new types of data, which, at this stage of the paper, are examined according to the *Marco Civil da Internet*'s paradigm. Second, the conflict between public authorities and technology companies is analyzed, regarding the most efficient or legitimate methods for international data collection, either through direct requisitioning to branch offices in Brazil or through international legal cooperation. Third, the legal properties of international cooperation in criminal matter are analyzed, based on empirical data on the operation of the Mutual Legal Assistance Treaty (MLAT) between Brazil and the United States, when used for telematic data gathering. Fourth, alternative solutions to international controversy are presented, with special attention to US' CLOUD Act, and other controversial investigation and data access techniques.

Keywords: Electronic data collection. Private communication data. Modern crime investigation. Internet service providers. International legal cooperation. Privacy and security.

SUMÁRIO

INTRODUÇÃO

Em março de 2016, o vice-presidente do Facebook na América Latina, Diego Dzodan, foi preso preventivamente[1]. A medida fora determinada pela Justiça de Sergipe, após a rede social descumprir prévia decisão judicial que determinava a entrega do conteúdo de mensagens privadas trocadas no aplicativo WhatsApp por usuários suspeitos da prática do crime de tráfico de drogas.

Segundo a Polícia Federal em Sergipe, o representante descumpriu ordens de repassar à Justiça informações armazenadas em serviços do Facebook, imprescindíveis para produção de provas a serem utilizadas em uma investigação de crime organizado e tráfico de drogas. A empresa, por sua vez, considerou a medida extrema e desproporcional, defendendo que a subsidiária no Brasil não seria tecnicamente capaz de fornecer os dados requeridos.

Essa situação é apenas um capítulo de uma problemática mais complexa, que descortina um profícuo debate: como devem ser coletados dados eletrônicos armazenados no exterior para fins de produção de evidências criminais?

A arquitetura técnica da Internet foi concebida como uma plataforma transfronteiriça e não territorial, que permite acesso a conteúdos independentemente da localização física do usuário. Sua natureza tem gerado incontáveis benefícios para a humanidade, sejam eles políticos, econômicos ou sociais. Em especial, permite o efetivo cumprimento do artigo 19 da Declaração Universal dos Direitos Humanos, no que tange ao acesso irrestrito à informação "sem consideração de fronteiras".

Apesar disso, como qualquer outra ferramenta humana, a Internet está suscetível ao mau uso e, como consequência, os meios eletrônicos de comunicação são cada vez mais utilizados para o planejamento e para a prática de crimes. Nesse contexto, mais crimes são investigados a partir de mecanismos digitais, de modo que o acesso aos dados relacionados a tais comunicações, armazenados pelos provedores dos serviços de Internet em outros países, torna-se peça fundamental nas investigações.

---

[1] Polícia prende vice-presidente do Facebook na América Latina em SP. Disponível em: <http://g1.globo.com/sao-paulo/noticia/2016/03/policia-prende-representante-do-facebook-na-america-do-sul-em-sp.html>. Acesso em: 18/06/2018.

A partir de uma perspectiva histórica, as interações transfronteiriças eram raras e as ferramentas de cooperação internacional foram pensadas para solucionar esses casos excepcionais. Contudo, com o desenvolvimento da Internet, as interações além das fronteiras são cada vez mais comuns, gerando conflitos entre usuários, as empresas provedoras dos serviços por eles utilizados e as autoridades públicas. Em face dessa problemática, urge questionar: como determinar as leis aplicáveis quando as relações extrapolam as fronteiras geográficas em um sistema internacional baseado em jurisdições definidas exclusivamente pela territorialidade?

Em relação à coleta de dados eletrônicos, há diferentes fatores territoriais que podem determinar a lei aplicável, como a localização do usuário de Internet, a localização dos servidores que armazenam os dados ou o local que a provedora do serviço de Internet está incorporada. Esses critérios territoriais conflitantes tornam a aplicação de leis no ambiente virtual e a resolução de disputas relacionadas à Internet difíceis e ineficientes, alargando tensões conforme a Internet se expande para usuários em mais de 190 países.

No Brasil, a discussão acerca do procedimento correto para acesso a dados no exterior tem se intensificado consideravelmente, fruto de posicionamentos díspares na jurisprudência e punições aplicadas às empresas de tecnologia pelo não cumprimento de decisões judiciais, como nos famosos casos de bloqueios do WhatsApp[2]. Essas decisões não são cumpridas pelas empresas sob alegação de impossibilidade técnica, pois não teriam acesso aos dados, e jurídica, em razão de lei americana proibir o fornecimento das informações requeridas sem prévia autorização da Justiça daquele país (várias das pessoas jurídicas empreendedoras de aplicativos eletrônicos encontram-se sediadas nos Estados Unidos).

Assim, as empresas provedoras de serviços de Internet encontram-se posicionadas entre duas normas domésticas conflitantes e com risco de responsabilização em ambos os países. Apesar das empresas defenderem a utilização da cooperação jurídica internacional para coleta de dados, as autoridades brasileiras têm dado preferência a alternativas mais agressivas (como a requisição direta às subsidiárias no Brasil, acompanhadas da fixação de astreintes), em razão da frustração gerada pela frequente demora e inefetividade do sistema de auxílio internacional.

---

[2] WhatsApp bloqueado: Relembre todos os casos de suspensão do app. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html>. Acesso em: 09/05/2018.

Cria-se, então, um debate entre as perspectivas da legalidade e da eficiência, isto é, entre os meios colaborativos que protegem os direitos a privacidade e segurança, e as técnicas mais agressivas, que valorizam a eficiência das autoridades em obter os dados almejados.

As soluções mais agressivas, apesar de aparentarem ser mais eficientes de imediato, põem em risco a segurança dos usuários de serviços de Internet e sacrificam direitos fundamentais de privacidade. Conforme será defendido no trabalho, as autoridades públicas devem dar preferência às técnicas de cooperação internacional para a coleta de dados no exterior, ainda que, por vezes, mostrem-se mais demoradas, pois tais métodos observam adequadamente os direitos fundamentais, notadamente o devido processo legal, bem como as normas do país em que a prova é produzida.

Para embasar essa hipótese, o presente trabalho parte do exame da doutrina especializada em relação ao tratamento e coleta de dados eletrônicos, bem como da regulação dada ao tema pela legislação brasileira, em especial, pelo Marco Civil da Internet. Em seguida, analisa casos judiciais para mostrar como a Justiça brasileira tem enfrentado a problemática, além do posicionamento jurídico dos diferentes atores envolvidos. Ainda, são examinadas as proteções e restrições trazidas pela legislação americana à coleta de dados telemáticos e, por fim, analisam-se comparativamente institutos e mecanismos adotados por outros países.

O trabalho se desenvolve da seguinte forma. O primeiro capítulo trata do crescente acesso da população às plataformas eletrônicas de comunicação, com direta relação na produção de diferentes tipos de dados, os quais são analisados sob a ótica do Marco Civil da Internet. O segundo capítulo trata do conflito brasileiro entre as autoridades públicas e as empresas de tecnologia, no tocante ao modo adequado para coleta de dados eletrônicos no exterior, além de expor quais são os obstáculos técnicos e jurídicos enfrentados pelos provedores de serviços de Internet e analisar casos judiciais acerca do tema. O terceiro capítulo analisa a cooperação jurídica internacional em matéria penal, munido de dados empíricos acerca do funcionamento do tratado de assistência legal (MLAT) entre Brasil e Estados Unidos quando destinado à coleta de dados eletrônicos. Por fim, o quarto capítulo apresenta alternativas para a solução do debate a partir da análise de técnicas utilizadas em outros países, com especial atenção ao *CLOUD Act*, dos EUA, e outros mecanismos controversos de investigação.

1. OS DADOS ELETRÔNICOS SOB A ÓTICA DO MARCO CIVIL DA INTERNET E OS CRIMES MODERNOS

1.1 O objeto do estudo: os dados de comunicação privada

Neste capítulo, pretende-se expor detalhadamente *o quê* vai ser analisado ao longo do trabalho e *o porquê* dessa análise. Além disso, serão trazidos conceitos mais técnicos dentro do universo da Internet, muitas vezes desconhecidos pelos operadores do Direito.

Inicialmente, cumpre realizar um corte metodológico: o objeto principal de estudo consiste nos dados de comunicação privada. Para tanto, é importante destrinchar as diferentes categorias de dados trazidas no Marco Civil da Internet e os requisitos legais para a violação de seu sigilo constitucionalmente garantido.

A Lei nº 12.965/2014, também conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil, gerando um verdadeiro marco regulatório de enorme repercussão social.

Apesar de o texto não passar isento de críticas, especialmente quanto às suas contradições internas de redação ou imprecisões de conceitos técnicos empregados, o diploma legal tem sido considerado como um avanço pela maior parte da doutrina, em razão de seu viés claro de proteção à liberdade de expressão, à neutralidade da rede e à privacidade dos dados e informações dos usuários[3].

O escopo do presente estudo, contudo, não é analisar a integralidade do diploma legal, senão seus desdobramentos a respeito da proteção garantida aos usuários e seus dados. Os dados dos usuários, cuja distinção é feita ao longo da Lei, variam entre *registro de cadastro*; *registro de conexão e acesso*; e o *conteúdo das comunicações privadas*.

Primeiro, os *registros cadastrais* consistem nas informações pessoais fornecidas pelo usuário ao provedor de serviços de Internet, tais como nome, endereço, números de documentos pessoais ou empresariais e demais informações necessárias à instalação, funcionamento e cobrança dos serviços.

---

[3] ARTESE, Gustavo (coord.). Marco Civil da Internet: Análise Jurídica sob uma Perspectiva Empresarial. São Paulo: Quartier Latin, 2015, p. 120.

Segundo, os *registros de conexão e acesso* consistem nos endereços IP (*Internet Protocol*) utilizados durante o acesso à Internet, bem como em outras informações relativas ao uso da rede, tais como datas e horários de *login* e *logout*, nome de usuário utilizado e demais informações técnicas que tenham por objetivo identificar determinado usuário. São armazenados tanto pelos provedores de acesso à Internet, quanto pelos provedores de conteúdo, englobando os dados vinculados à identidade do usuário ao acessar um serviço *online*[4].

Os provedores de acesso são empresas prestadoras de serviços de conexão à Internet, por meio da habilitação de um terminal para envio e recebimento de dados, mediante a atribuição ou autenticação de um endereço IP[5]. Já os provedores de conteúdo ou de aplicação consistem em terminais conectados à Internet, cuja funcionalidade e conteúdo são acessíveis pelos usuários através de outro terminal. É o caso, por exemplo, do Facebook, do Gmail, do Twitter, entre outros.

Para essas empresas de tecnologia, o armazenamento de dados não é mais visto de forma estática e de utilidade limitada ao propósito da sua coleta. O registro e a guarda de *logs* de acesso e de navegação se inserem no modelo de negócio em que estas empresas se baseiam[6]. Assim, as receitas das empresas de tecnologia se originam, principalmente, na publicidade oferecida através de suas plataformas, de forma que a coleta de informações é necessária para o direcionamento de ofertas a usuários com mais propensão de interessarem por elas.

Terceiro, há o *conteúdo propriamente dito das comunicações privadas* realizadas por meio dos referidos provedores de conteúdo, que compreendem, por exemplo, o texto enviado

---

[4] ARTESE, Gustavo (coord.). Marco Civil da Internet: Análise Jurídica sob uma Perspectiva Empresarial. 1. ed. São Paulo: Quartier Latin, 2015, p. 281.

[5] Ibid., p. 123.

[6] Fato que se tornou notório após a publicização do recente escândalo do Facebook. A rede social permitia que aplicativos de jogos e testes psicológicos colhessem dados dos usuários e de todos seus amigos. Por meio destes, a Cambridge Analytica, empresa americana de análise de dados, comprou do Facebook o acesso a tais dados e foi capaz de criar um sistema que permitiu prever e influenciar as escolhas dos eleitores nas eleições americanas de 2016 e no plebiscito que determinou a saída do Reino Unido da União Europeia, por meio dos dados colhidos na rede social. Contratada pelo time responsável pela campanha do republicano Donald Trump e pelo grupo que promovia o Brexit, a empresa se aproveitou de uma brecha no política do Facebook para colher dados de cerca de 50 milhões de usuários (na maioria, eleitores americanos) sem autorização, para catalogar o perfil dessas pessoas de acordo com suas inclinações políticas e direcionar, de forma mais personalizada, materiais pró-Trump e mensagens contrárias à sua adversária, Hillary Clinton, àqueles usuários que ainda estavam em dúvida em relação à sua intenção de voto. Essa brecha foi levada ao conhecimento do Facebook pela primeira vez há cerca de dois anos, mas a plataforma só suspendeu o acesso da Cambridge Analytica aos dados recentemente, após reportagens que procuraram a empresa para pedir respostas acerca do caso. O CEO do Facebook, Mark Zuckerberg, foi chamado para prestar esclarecimentos perante comitês legislativos nos Estados Unidos e no Reino Unido. A rede social, por sua vez, teve seu valor encolhido em mais de US$ 35 bilhões na bolsa de valores de tecnologia dos EUA após o escândalo. Assim, fica a reflexão: nós, como usuários da rede social, somos os clientes ou o próprio produto da plataforma?

nas mensagens privadas ou o corpo de e-mails. Com esse tipo de dado, pretende-se coletar o conteúdo da conversa que o remetente teve a intenção de enviar ao seu destinatário, por meio de texto, foto, vídeo, áudio etc.

Finalizadas as distinções a respeito dos diferentes tipos de dados, cumpre analisar as questões atinentes ao sigilo e sua inviolabilidade.

Segundo o art. 5º, XII, da Constituição Federal de 1988, "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal". Assim, o sigilo foi imposto como regra, sendo exceção a sua quebra, que somente poderá ser autorizada mediante ordem judicial fundamentada.

O sigilo das comunicações, além de consequência da garantia da livre expressão de pensamento, exprime também aspecto fundamental do direito à privacidade e à intimidade. Com efeito, a quebra da confidencialidade da comunicação significaria frustrar o direito do emissor de escolher o destinatário do conteúdo de sua comunicação[7].

Os dados informáticos, conforme visto anteriormente, consistem em informações particulares e íntimas dos indivíduos, capazes de os identificarem ou os tornarem identificáveis. Dessa forma, é evidente que os dados ora analisados estão incluídos sob o manto da inviolabilidade constitucional.

A controvérsia nasce, contudo, na interpretação da expressão "salvo, no último caso", incluído na redação do inciso XII pelo legislador originário, que abriu margem para três correntes distintas[8]: os que defendem que somente pode ser quebrado o sigilo de comunicações telefônicas, com observância restrita dos critérios legais; aqueles que entendem haver dois grupos, o da correspondência, cujo sigilo é absoluto, e o das comunicações telegráficas, de dados e comunicações telefônicas, em que o sigilo seria relativo; e a corrente que entende que o sigilo absoluto abrangeria o grupo das comunicações telegráficas e de correspondência, havendo sigilo relativo quanto ao grupo das comunicações telefônicas e de dados.

[7] NETO, M. F.; SANTOS, J. E. L.; GIMENES, E. V. *Crimes na Internet e Inquérito Policial Eletrônico*. 1. ed. São Paulo: EDIPRO, 2012, p. 111.
[8] Ibid., p. 111-112.

Nessa toada, há autores que entendem ser absoluta a vedação de quebra do sigilo de correspondência, das comunicações telegráficas e de dados pessoais, somente podendo ser admitida a quebra do sigilo de comunicações telefônicas na forma da lei[9].

No mesmo sentir, seria inconstitucional o parágrafo único do art. 1º da Lei nº 9.296/1996, que regulamenta a parte final do inciso XII, da CF/1988. Isso porque o dispositivo legal prevê a expansão dos meios de prova aos fluxos de comunicações estabelecidos em sistemas de informática e telemática, em equiparação à escuta telefônica[10].

Por outro lado, há acadêmicos que se posicionam no sentido de ser possível a quebra judicial de dados pessoais, desde que a limitação da tutela do sigilo seja justificável através do princípio da proporcionalidade, em casos em que o interesse público prevaleça em detrimento do interesse do particular[11].

Quanto a esse posicionamento, a restrição de direitos fundamentais pode ocorrer mesmo sem autorização expressa do constituinte, sempre que se fizer necessária a concretização do princípio da concordância prática entre ditames constitucionais. Não havendo direitos absolutos, o sigilo de correspondência, de comunicações telegráficas e de dados também são passíveis de restrições em casos recomendados pelo princípio da proporcionalidade[12].

Em que pese ao debate doutrinário, o art. 1º, parágrafo único, da Lei nº 9.296/96 é vigente no ordenamento jurídico, de tal modo que o texto constitucional é interpretado para incluir os dados de comunicações em fluxo, em sistemas de informática e telemática, no rol de inviolabilidades relativas.

Nesse ponto, segundo Carina Quito, há um descompasso entre a proteção das comunicações eletrônicas em fluxo em relação às armazenadas[13]. Em termos práticos, os usuários dos meios de comunicação armazenados observam uma vulnerabilidade muito grande de sua privacidade por ausência de uma regulamentação específica.

Assim, defende que falta de regulamentação possibilita que o Judiciário acesse essas informações de forma indiscriminada, com base no argumento de que os requisitos bastante

---

[9] NETO, M. F.; SANTOS, J. E. L.; GIMENES, E. V. *Crimes na Internet e Inquérito Policial Eletrônico*. 1. ed. São Paulo: EDIPRO, 2012, p. 116.
[10] Ibid., p. 116.
[11] Ibid., p. 118.
[12] MENDES, G. F.; BRANCO, P. G. G. Curso de direito constitucional. 7. ed. São Paulo: Saraiva, 2012, p. 421.
[13] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Acesso a comunicações eletrônicas e criptografia: garantias, prerrogativas e devido processo legal. 2017. (2h29m). Disponível em: <https://www.youtube.com/watch?v=W_b2Jr9wFXk>. Acesso em: 09/05/2018.

restritivos da Lei nº 9.296/1996 são aplicáveis apenas às comunicações em fluxo, não sendo extensíveis aos dados armazenados. No mais, sustenta que essa interpretação é corroborada pela leitura do art. 7º do Marco Civil da Internet, que estipula que basta uma ordem judicial fundamentada para acessar o conteúdo das comunicações armazenadas, sem que haja parâmetros autorizadores, como a elevada gravidade do crime investigado.

Com efeito, diferentemente do que acontece com as comunicações telefônicas, marcadas por uma característica de instantaneidade, as comunicações eletrônicas que predominam atualmente no contexto de interações sociais e profissionais são, por sua própria natureza, um tipo de comunicação que gera registros.

Dessa forma, é comum que as ordens de quebra de sigilo e entrega de conteúdo aos provedores de aplicações abranjam longos intervalos de tempo e grande quantidade de conteúdo, muito além do necessário à investigação ou instrução criminal. Por esses motivos, Quito argumenta que deve ser dada interpretação ampliativa ao art. 5, XII, da CF/1988, para proteger não só as comunicações em fluxo, mas também as armazenadas, evitando assim a quebra indiscriminada do sigilo em razão da falta de regulamentação específica.

Seguindo à análise de dispositivos do Marco Civil da Internet, o diploma legal impõe aos provedores o dever geral de manter em sigilo todos os dados cadastrais, de conexão e o conteúdo de suas comunicações privadas, estabelecendo inclusive punições em caso de violação da privacidade dessas informações.

Mais especificamente, no tocante aos diferentes tipos de dados elencados anteriormente, cabe menção ao art. 10 do Marco Civil, como se observa:

> *Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*
>
> *§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.*

> *§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.*
>
> *§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.*
>
> *(...)*

O *caput* reitera os princípios elencados no art. 3º, que, por sua vez, já se encontravam dispostos na Constituição Federal. Além disso, faz distinção entre os dados de conexão, os dados de cadastro e o conteúdo das comunicações privadas, que também foram especificamente tratados nos parágrafos subsequentes.

O § 1º trata dos dados de conexão, estipulando a responsabilidade do provedor, seja de acesso à Internet ou ao conteúdo, de guardar e disponibilizar os registros de dados pessoais que possam contribuir para a identificação do usuário ou do terminal, mediante autorização judicial.

O § 2º, por sua vez, trata do conteúdo das comunicações privadas, que, da mesma forma, poderá ser disponibilizado apenas mediante ordem judicial.

O § 3º, que trata dos dados cadastrais, traz uma abordagem mais branda a essa categoria de dados. Autoridades administrativas, policiais e investigativas podem requisitar diretamente aos provedores, sem a necessidade de autorização judicial prévia, dados cadastrais referentes a registros eletrônicos que dispõem, como qualificação pessoal, filiação e endereço[14].

Assim, em consonância com a proteção da privacidade do usuário, a disponibilização dos registros de acesso à conexão e a aplicações, como também do conteúdo das comunicações privadas, somente poderá ser realizada mediante ordem judicial.

Para tanto, o Marco Civil da Internet especifica que a ordem judicial deve considerar a existência de evidências suficientes da ofensa, a relevância do dado para a investigação em curso, em nome do princípio da proporcionalidade, e deve definir o período específico a que o dado se refere[15].

---

[14] MASSO, F. D.; ABRUSIO, J.; FILHO, M. A. F (coord.). Marco Civil da Internet: Lei 12.965/2014. 2. ed. São Paulo: Editora Revista dos Tribunais, 2014, p. 150-151.

[15] ARTESE, Gustavo (coord.). *Marco Civil da Internet: Análise Jurídica sob uma Perspectiva Empresarial.* 1. ed. São Paulo: Quartier Latin, 2015, p. 95.

Ainda, o art. 23 do diploma legal determina que cabe ao magistrado tomar medidas necessárias de precaução, de forma a assegurar a privacidade do indivíduo cujos dados tiveram o sigilo violado. Essa provisão inclui a possibilidade de o juiz decretar o segredo de justiça do processo e até mesmo da requisição de acesso a dados, de forma a proteger a privacidades dos envolvidos.

O fornecimento de dados de usuários da Internet, sem ordem judicial específica, portanto, representaria violação às normas constitucionais, que asseguram a privacidade e o sigilo de dados do indivíduo, como apontado anteriormente.

Além disso, a obtenção, sem ordem judicial, de dados de usuários supostamente envolvidos em atos ilícitos pode ser prejudicial à própria investigação, já que provas obtidas em desobediência à Constituição Federal e fora do devido processo legal podem ser consideradas inadmissíveis, ante o disposto no art. 5º, LVI, da CF/1988, no CPC e no CPP.

Note-se que o Marco Civil da Internet expressamente destaca, em seu art. 22, que o fornecimento de dados pode ocorrer para fins de formação de conjunto probatório em processo cível ou penal, em caráter incidental ou autônomo, e não apenas em caso de investigação criminal ou instrução processual penal, o que demonstra que o requisito básico da ordem judicial pode ser observado em procedimento de qualquer natureza[16].

Feitas as distinções acerca dos diferentes tipos de dados armazenados pelos provedores de serviços de Internet, além da conceituação técnica de elementos do Direito cibernético, também fica delimitado o escopo de análise do presente estudo.

Todas as categorias de dados podem ser úteis para a investigação dos crimes modernos, que serão melhor explicados no tópico a seguir. Contudo, será dada maior ênfase aos dados cujo *standard* de obtenção é mais elevado, quais sejam, os dados de conexão e o conteúdo das comunicações privadas, que necessitam de autorização judicial para terem seu sigilo violado.

Explicado *o que* está sendo analisado, passa-se à análise do *porquê* do estudo.

1.2 O motivo do estudo: os serviços de comunicação privada como meio de planejamento e cometimento de crimes modernos

[16] ARTESE, Gustavo (coord.). *Marco Civil da Internet: Análise Jurídica sob uma Perspectiva Empresarial*. 1. ed. São Paulo: Quartier Latin, 2015, p. 286.

É cada vez maior o número de pessoas conectadas à Internet no mundo, assim como o número de pessoas com acesso às plataformas de comunicação privada. Em pesquisa realizada no final de 2016 pelo IBGE, verifica-se que o Brasil tem 116 milhões de pessoas conectadas à Internet, número que corresponde a 64,7% de toda a população do país com idade acima de 10 anos[17]. Em outro estudo realizado em 2017, o IBGE aponta que 63,3% dos domicílios brasileiros têm acesso à Internet[18]. Ambas as pesquisas, ademais, apontaram que o celular é o principal meio de acesso a Internet no Brasil, sendo utilizado por 94,6% dos internautas.

Os dados analisados são de extrema importância para a visualização do constante crescimento da conectividade da população brasileira à Internet, especialmente porque, em 2013, menos da metade dos domicílios brasileiros tinham acesso à rede. Outro elemento interessante das pesquisas é que a principal atividade realizada pelos internautas brasileiros no celular, apontada por mais de 94% dos usuários, é a troca de mensagens de texto, voz ou imagens por aplicativos de bate-papo.

O incremento na quantidade de pessoas conectadas à Internet gera, indubitavelmente, maior acesso às redes sociais, plataformas digitais que trazem diversos benefícios à sociedade[19].

Destaca-se, inicialmente, o grande poder democratizante da Internet, que facilita a comunicação e cria possibilidades de interação, organização e mobilização social, geralmente por meio de serviços e plataformas gratuitas ou de baixo custo. Recentemente, há vários casos de manifestações organizadas por redes sociais, que culminaram, inclusive, até na queda de regimes totalitários em alguns países[20].

Além disso, as plataformas digitais promovem a liberdade de expressão, o acesso à informação, à educação e à cultura, uma vez que as pessoas podem expressar suas opiniões sem interferência, recebendo e compartilhando informações livremente. O conteúdo gerado

---

[17] Brasil tem 116 milhões de pessoas conectadas à internet, diz IBGE. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml>. Acesso em: 25/04/2018.

[18] Mais de 63% dos domicílios têm acesso à internet, aponta IBGE. Disponível em: <https://g1.globo.com/economia/noticia/mais-de-63-dos-domicilios-tem-acesso-a-internet-aponta-ibge.ghtml>. Acesso em: 25/04/2018.

[19] ARTESE, Gustavo (coord.). *Marco Civil da Internet: Análise Jurídica sob uma Perspectiva Empresarial.* 1. ed. São Paulo: Quartier Latin, 2015, p.278-280.

[20] Redes sociais desempenharam papel fundamental na queda de Mubarak, afirmam especialistas. Disponível em: <https://oglobo.globo.com/mundo/redes-sociais-desempenharam-papel-fundamental-na-queda-de-mubarak-afirmam-especialistas-2823615>. Acesso em: 25/04/2018.

pelos usuários e disponibilizado pelas plataformas digitais representa uma das principais formas de expressão do pensamento crítico.

Com efeito, um ambiente de insegurança jurídica e censura é caracterizado pela falta de debates e manifestação limitada ou inexistente de opiniões. Noutro giro, a democracia pode ser identificada pela vasta quantidade de debates políticos e manifestação crítica do pensamento, o que é facilmente visto nas redes sociais atualmente.

Por fim, no âmbito econômico, as plataformas digitais fomentam a criação de novos meios de negócio, em razão do amplo acesso de consumidores aos fornecedores. Assim, há um ambiente que permite maior inovação do mercado, a geração de novos empregos e tributos, e a redução tanto dos custos do empresário quanto dos preços do consumidor.

Contudo, também há um lado negativo do aumento do número de usuários da Internet e das plataformas digitais: a criação de um novo ambiente para o planejamento e o cometimento de atos ilícitos.

Com o aumento do acesso das pessoas à Internet, vieram à tona situações jamais enfrentadas pelo Direito Penal em nosso país. Há incertezas no tocante à interpretação das normas vigentes e pouca coisa foi pacificada pela jurisprudência dos Tribunais pátrios.

Há doutrina que distingue os tipos de delitos informáticos[21].Os delitos podem ser puros, quando o sujeito ativo visa especificamente o sistema de informática em todas suas formas, incluindo *software*, *hardware*, dados e sistemas, bem como meios de armazenamento; e podem também ser mistos, nos casos em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático.

Dentro da primeira categoria, destacam-se os ilícitos informáticos que violam a privacidade na *web*, como o uso de *spywares*, que são programas espiões que enviam informações do computador do usuário da rede para desconhecidos, e dos diferentes tipos de vírus de computador, que causam danos ou modificam programas e dados da máquina, obstaculizando o funcionamento normal do sistema[22].

Na segunda categoria, aparecem os crimes em que o computador e a Internet são apenas instrumentos, tendo em vista que o bem jurídico violado não é o sistema informático. Neste

[21] NETO, M. F.; SANTOS, J. E. L.; GIMENES, E. V. Crimes na Internet e Inquérito Policial Eletrônico. 1. ed. São Paulo: EDIPRO, 2012, p. 29.
[22] Ibid., p. 31-32.

grupo se destacam, por exemplo, os crimes de induzimento, instigação ou auxílio a suicídio; de ameaça; de calúnia, difamação e injúria; de furto mediante fraude e estelionato; de pornografia infantil e corrupção de criança ou adolescente; bem como outras condutas potencialmente danosas, ainda não disciplinadas pelo Direito Penal.

Além da possibilidade de cometimento de novos crimes por meio da Internet, as plataformas digitais também podem servir de instrumento para o crime organizado. Com efeito, criminosos podem facilmente se utilizar dos serviços comuns de bate-papo para planejar atos ilícitos.

A tecnologia da criptografia ponta-a-ponta nas conversas de WhatsApp, analisada com mais detalhes no capítulo seguinte, dificulta consideravelmente o acesso das autoridades de investigação ao conteúdo das mensagens, de forma que os criminosos têm, na prática, a certeza de estarem planejando seus atos em um ambiente "seguro".

Há, inclusive, Projeto de Lei[23] de autoria do deputado Francisco Floriano (DEM-RJ) que propõe alterar o Código Penal para incluir como agravantes de pena o uso de redes sociais ou serviços de mensagens via celular, como o WhatsApp, para divulgar cenas de crime ou para organizar a ação criminosa.

Assim, a produção de provas é indubitavelmente uma das maiores barreiras a serem transpostas no tocante à condenação pela prática e pelo planejamento dos crimes modernos.

A finalidade da prova é convencer o julgador a respeito de determinado fato, produzindo um estado de certeza na convicção do magistrado acerca da existência ou não de fato que se considera de interesse para a solução de um processo[24].

Com o surgimento e a disseminação da Internet, aumentaram exponencialmente a produção de dados de usuários. Tais dados, então, se tornam o meio de prova mais eficiente (quiçá o único) para o deslinde de investigações de crimes cometidos por meio da Internet.

Os denominados dados eletrônicos nada mais são que uma sequência de *bits* traduzidas por meio de determinado programa de computador, ou seja, é o documento que se encontra memorizado em forma digital, acessível somente por meio de computador[25].

---

[23] Projeto de Lei nº 9.688/2018.

[24] ZANIOLO, Pedro Augusto. *Crimes Modernos: o impacto da tecnologia no direito*. 3. ed. Curitiba: Juruá Editora, 2016, p. 48.

[25] FEROLLA, G.; NAVES, J. P. M.; ZUGAIBE, N. C. *Documento eletrônico como meio de prova no processo penal brasileiro*. Revista dos Estudantes de Direito da UnB. Brasília, 2016, p. 17.

Dessa forma, a esse novo modelo de prova transcende o entendimento tradicional acerca da materialidade e literalidade da prova documental, uma vez que se dá o nome de documento eletrônico àquele gerado ou arquivado por sistema computadorizado, em meio digital[26].

Conforme analisado no tópico anterior, o Marco Civil da Internet trouxe importantes inovações para a obtenção dos dados eletrônicos como meio de prova para investigações em processo de qualquer natureza.

No caso em análise, há destaque, evidentemente, ao processo penal. Assim, com o crescimento do número de crimes cometidos por meio da Internet, inerente ao aumento da acessibilidade da população ao serviço, os dados eletrônicos adquirem importância incontestável para a investigação desses ilícitos.

Fica claro, então, o motivo pelo qual a discussão acerca da coleta de dados eletrônicos em meio à investigação de crimes cometidos ou planejados por meio da Internet é tão importante, tendo em vista a atualidade da discussão e a consequente falta consentimento das autoridades investigadoras e dos Tribunais quanto à aplicação da legislação.

Elucidado o *porquê* do estudo, além do seu objeto, a discussão se torna um pouco mais complexa: passa-se a analisar os casos em que a empresa de tecnologia que detém a plataforma digital ou o serviço de comunicação é sediada e armazena os dados de seus usuários no exterior.

[26] FEROLLA, G.; NAVES, J. P. M.; ZUGAIBE, N. C. *Documento eletrônico como meio de prova no processo penal brasileiro*. Revista dos Estudantes de Direito da UnB. Brasília, 2016, p. 3-4.

2. AS COMPLEXIDADES DA COLETA DE DADOS ELETRÔNICOS ARMAZENADOS NO EXTERIOR

2.1 As empresas provedoras de serviços de Internet e a criptografia

No capítulo anterior, foi explicada a sistemática do Marco Civil da Internet quanto à regulamentação da coleta de provas eletrônicas, que se mostram muito úteis e necessárias na atual conjuntura. Isso porque, com o aumento considerável de pessoas conectadas à Internet, também cresce o número de crimes modernos – aqueles cometidos ou planejados através da rede.

Conforme examinado, para a obtenção de dados de conexão e do conteúdo propriamente dito das comunicações eletrônicas, é preciso que haja ordem judicial autorizando a violação de sua privacidade. O desafio que se apresenta agora, contudo, é analisar como deve se dar esse mesmo procedimento – de obtenção de dados eletrônicos – quando as empresas provedoras de serviços de Internet e detentoras dos dados em questão são estrangeiras.

De fato, trata-se de um tema que gera muito debate e que está longe de ser pacificado. Como devem proceder as autoridades locais para a obtenção de dados armazenados no exterior e detidos por empresas de tecnologia sediadas em outro país?

Não é raro as autoridades de investigação se depararem com a situação narrada, até porque a maioria das grandes empresas de tecnologia, e provedoras das plataformas de comunicações, são originárias de outros países, em especial, dos Estados Unidos.

A título de exemplificação, apenas alguns dos gigantes do Vale do Silício, como o Facebook (que também controla o Instagram e o WhatsApp), a Apple, a Google, a Microsoft, já são capazes de evidenciar o monopólio americano quando se trata de plataformas de Internet.

Tais companhias oferecem serviços de e-mail, de redes sociais, de bate-papo em chats individuais ou em grupo, de armazenamento de arquivos, de compartilhamento de fotos vídeos e inúmeros outros que já são de conhecimento da população em geral, devido à proximidade com a realidade de quem usa a Internet.

Por conseguinte, essas e outras empresas estrangeiras do ramo detém dados de milhões de usuários por todo o mundo. Dados de pessoas que, por ventura, podem utilizar das referidas

plataformas eletrônicas para o cometimento ou planejamento de crimes e, consequentemente, podem estar sob investigação criminal.

A controvérsia, embora recente, tem gerado respostas divergentes dos tribunais brasileiros, uma vez que envolve questões sensíveis sobre a proteção da privacidade, os poderes de investigação do Estado, a soberania nacional e as possibilidades de cooperação internacional.

A realidade brasileira, como não poderia ser diferente, apresenta complexidades que acirram a controvérsia. Quando as autoridades de investigação criminal requerem ao juiz responsável a coleta de dados de comunicação eletrônica armazenados por uma empresa estrangeira, o caminho a ser tomados pelos magistrados ainda não é claro. Isso porque o tema é muito novo e ainda pende de normatização específica, o que acaba gerando as mais variadas atitudes pelos juízes, fruto de suas interpretações da legislação genérica existente.

Como reflexo disso, muitos juízes, atendendo a pedidos de autoridades policiais e do Ministério Público, ordenam que as filiais brasileiras de grandes empresas de tecnologia e comunicações, como do Facebook, WhatsApp e Yahoo!, entreguem dados provenientes de suas aplicações de Internet.

Apesar da determinação das autoridades brasileiras de entrega dos dados, as empresas muitas vezes se recusam a cooperar, sob alegação de que não têm acesso aos dados armazenados pela empresa-sede nos EUA e eventual entrega seria contrária à legislação americana.

Essas negativas têm rendido multas milionárias às empresas de tecnologia, aplicadas pela Justiça brasileira[27], bem como o mandado de prisão para executivos pela prática do crime de desobediência. A recusa rendeu até a suspensão do funcionamento das atividades por tempo determinado, nos famosos casos de bloqueio do WhatsApp.

O WhatsApp Messenger foi criado em 2009 e em 2016 atingiu a marca de um bilhão de usuários. Em março de 2016, o vice-presidente do Facebook na América Latina foi preso pela negativa do Facebook[28] em conceder informações relativas ao aplicativo WhatsApp,

[27] As sanções por descumprimento de determinação judicial aplicadas aos provedores de serviços de Internet têm como base o art. 12 do Marco Civil da Internet, e variam entre advertência, medidas corretivas e multa, até a suspensão e proibição de atividades que envolvam a retenção de dados.

[28] O Facebook detém o controle do WhatsApp Messenger desde 2014, quando efetuou a compra do aplicativo de bate-papo pelo valor de US$ 22 bilhões.

consideradas essenciais para identificar os membros de uma organização criminosa que estaria atuando no estado do Sergipe. No dia seguinte, contudo, foi concedido *Habeas Corpus* revogando sua prisão preventiva, sob argumentação de que não havia processo judicial e nem investigação policial contra o executivo da empresa[29].

O caso do WhatsApp apresenta uma peculiaridade a mais, que é a alegação de que a própria empresa não teria acesso às mensagens veiculadas em seu aplicativo, em razão da tecnologia de criptografia de ponta-a-ponta, e por isso seria incapaz de fornecer tais dados às autoridades[30].

A criptografia, segundo a Cartilha de Segurança para a Internet[31] do Comitê Gestor da Internet no Brasil, é a ciência de escrever mensagens de forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para autenticar a identidade de usuários; autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias; e proteger a integridade de transferências eletrônicas de fundos.

De acordo com Diego Aranha, pesquisador da Unicamp, a criptografia ponta-a-ponta é aquela em que a capacidade de decriptar mensagens existe apenas nas pontas da comunicação, ou seja, somente quem manda e quem recebe têm acesso à mensagem. Em outras palavras, não há intermediários no canal de comunicação capazes de interceptar as mensagens, nem mesmo o próprio operador do serviço, o que torna o canal mais seguro[32].

---

[29] ZANIOLO, Pedro Augusto. *Crimes Modernos: o impacto da tecnologia no direito*. 3. ed. Curitiba: Juruá Editora, 2016, p. 215.

[30] Há dois processos discutindo o assunto no STF: a ADPF 403, em que o Partido Popular Socialista (PPS) requer que o STF proíba o bloqueio do WhatsApp; e a ADI 5527, em que o Partido da República (PR) argumenta pela inconstitucionalidade dos incisos III e IV do art. 12 do Marco Civil da Internet, que autorizam a suspensão temporária e a proibição do exercício das atividades, respectivamente, de empresa de tecnologia que recusa sua submissão à legislação brasileira. O PR argumenta, na ADI de sua autoria, que os serviços de troca de mensagens pela Internet estão cada vez mais disseminados na sociedade, o que gera uma maior dependência dos cidadãos em relação ao serviço. Assim, a suspensão desses aplicativos, antes de ser uma punição à empresa responsável, torna-se uma medida que penaliza a própria população em geral, usuária dos serviços. Dessa forma, conclui que a prestação de serviços de mensagens pela Internet deveria se submeter ao princípio constitucional da continuidade do serviço, não podendo ser arbitrariamente interrompido pelo Estado. Os relatores das ações, os Ministros Edson Fachin e Rosa Weber, organizaram audiência pública em que diversos especialistas discutiram a lei brasileira e a tecnologia de criptografia do WhatsApp. Embora o escopo das ações não fosse a discussão acerca da criptografia, o tema acabou dominando as audiências públicas.

[31] CARTILHA de segurança para internet. Comitê Gestor da Internet no Brasil, 23 out. 2006. Disponível em: <http://cartilha.cert.br/sobre/old/cartilha_seguranca_3.1.pdf>. Acesso em: 09/05/2018.

[32] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Acesso a comunicações eletrônicas e criptografia: garantias, prerrogativas e devido processo legal. 2017. (2h29m). Disponível em: <https://www.youtube.com/watch?v=W_b2Jr9wFXk>. Acesso em: 09/05/2018.

Os métodos de criptografia atuais são seguros e eficientes e se baseiam e no uso de uma ou mais chaves. A chave é uma sequência de caracteres, que podem conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizado pelos métodos de criptografia para codificar e decodificar mensagens.

O professor Aranha ressalta que tecnologia da criptografia não é novidade. Ela foi desenvolvida a partir da II Guerra Mundial e aprimorada nos anos 1990, mas sempre se restringiu às comunicações confidenciais dos governos e dos militares. A novidade é poder contar com a tecnologia em dispositivos e aplicativos comuns ao público, como técnica de incremento à privacidade.

Segundo Riana Pfefferkorn, pesquisadora da Stanford Law School, as autoridades investigativas estão acostumadas a sempre serem capazes de acessar os dados e o conteúdo das comunicações privadas através do aparato judicial adequado. Tornar a criptografia comercialmente disponível para o público em geral debilita a capacidade inerente da polícia em acessar informações mesmo com a autorização legal apropriada[33].

Para exemplificar isso, a pesquisadora cita o caso americano da Apple v. FBI. Nas investigações do massacre de San Bernardino, na Califórnia, ocorrido em dezembro de 2015, as autoridades policiais encontraram o celular de um dos atiradores: um iPhone.

Uma juíza federal americana ordenou que a Apple colaborasse com o FBI com a assistência técnica necessária para acesso ao dispositivo, o que significaria desativar seu sistema de segurança, que elimina os dados do telefone caso o código correto não seja digitado após 10 tentativas.

A partir do sistema operacional iOS 8, a Apple instituiu a criptografia no sistema de segurança de seus dispositivos, fato que impossibilitava a própria empresa de obter acesso a senha pessoal e ao conteúdo do celular do atirador. O FBI, portanto, requereu que a empresa criasse uma versão do sistema operacional que desativasse o risco da autodestruição de dados dos iPhones em caso de erro do código de acesso, para que os investigadores pudessem tentar várias combinações de senhas até obterem acesso.

A empresa, então, recusou-se a colaborar, sob alegação de que se acatasse aos pedidos do governo, colocaria em risco a privacidade de todos os seus dispositivos, pois se esse novo

[33] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – O debate americano sobre vigilância e criptografia. 2017. (57m42s). Disponível em: <https://www.youtube.com/watch?v=NuszpDZ69qw>. Acesso em: 09/05/2018.

software caísse em mãos erradas, qualquer iPhone em posse física do usuário poderia ser desbloqueado.

O FBI, então, buscou meios alternativos e pagou mais de US$ 1 milhão para que um grupo de hackers profissionais burlasse a senha pessoal do iPhone do atirador sem ativar o mecanismo de segurança do dispositivo que apaga todo o conteúdo do telefone[34].

Com essa solução alternativa encontrada pelas autoridades policiais americanas, o debate jurídico acerca da obrigatoriedade de a empresa de tecnologia colaborar com esse tipo de decisão judicial ficou sem respostas.

Contudo, é possível notar a semelhança da decisão com os bloqueios do WhatsApp: a inabilidade das autoridades em obter as informações desejadas culmina em medidas agressivas ou punições às empresas de tecnologia que causam danos colaterais para milhões de usuários sem qualquer relação com o caso (risco à privacidade de qualquer pessoa que tenha um iPhone, no caso americano, e dano a todos os usuários do WhatsApp no Brasil, que ficaram sem o serviço).

No mais, um detalhe que merece atenção é que o primeiro caso de suspensão do funcionamento do WhatsApp por juiz brasileiro se deu em fevereiro de 2015; o segundo caso, por sua vez, em dezembro do mesmo ano[35]. A criptografia foi incrementada às conversas pela empresa apenas em março de 2016, ou seja, após os primeiros conflitos da empresa com a Justiça brasileira[36].

Fica claro, então, que há uma controvérsia anterior à própria utilização de criptografia pelo WhatsApp: o conflito de jurisdição.

2.2 O conflito de jurisdição

[34] FBI pagou mais de US$ 1 milhão para acessar iPhone de atirador. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/04/fbi-pagou-mais-de-us-1-milhao-para-acessar-iphone-de-atirador.html>. Acesso em: 09/05/2018.

[35] WhatsApp bloqueado: Relembre todos os casos de suspensão do app. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html>. Acesso em: 09/05/2018.

[36] WhatsApp começa a identificar conversas com criptografia. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/whatsapp-comeca-identificar-conversas-com-criptografia.html>. Acesso em: 09/05/2018.

O conflito de jurisdição se dá, na prática, em casos em que o pedido de coleta de dados e/ou de informações de usuários da plataforma digital é direcionado à filial brasileira da empresa de tecnologia sediada no exterior.

No caso de dados do WhatsApp e do Facebook, por exemplo, os pedidos são direcionados à Facebook Brasil, que argumenta ser uma empresa distinta da Facebook Inc., quem realmente controlaria a plataforma e seria a única habilitada a prestar as informações requeridas. Assim, empresas de Internet como o Facebook sustentam que o pedido deve ser destinado à sede, localizada nos Estados Unidos, por meio da cooperação jurídica internacional.

As autoridades de investigação e os juízes brasileiros, por sua vez, geralmente alegam que a cooperação internacional é desnecessária, pois o Brasil já teria jurisdição sobre essas empresas, a despeito de estarem sediadas e processarem dados nos Estados Unidos.

Nesse sentido, há Nota Técnica do Ministério Público[37] na qual se adota o entendimento de que o art. 11 do Marco Civil da Internet determina que as empresas que prestam serviços no Brasil, ainda que não possuam filiais, devem observar a lei brasileira quanto aos procedimentos de coleta, armazenagem, guarda ou tratamento de dados de registro, pessoais ou de comunicações. Assim, são obrigadas a transmitir os referidos dados às autoridades brasileiras quando requisitados, sem a necessidade de pedido de cooperação jurídica internacional.

Com efeito, as autoridades que requerem a coleta dos dados para a investigação criminal e os juízes que ordenam que as empresas de tecnologia os entreguem têm utilizado o Marco Civil da Internet como alicerce jurídico para tais determinações, mais especificamente, o art. 11:

> *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.*

[37] Nota Técnica sobre o Projeto de Lei do Senado nº 169/2017, em que se pretende alterar o Marco Civil da Internet para estabelecer que o juiz poderá determinar a suspensão ou o bloqueio de aplicação de Internet que incentive a prática de crime, mas que veda a suspensão de aplicação de mensagens instantâneas. Disponível em: <http://www.mpf.mp.br/pgr/documentos/notatecnica.pdf>. Acesso em: 09/05/2018.

> *§ 1o O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.*
>
> *§ 2o O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.*

Em outras palavras, o art. 11 do Marco Civil da Internet estipula que os atos de coleta, armazenamento e disponibilidade de dados realizados no Brasil pelos provedores dos serviços de aplicações de Internet estão sujeitos à jurisdição brasileira, especialmente para aquelas empresas que têm sede no Brasil, e mesmo para as empresas sediadas no exterior que ofertem serviço ao público brasileiro.

O Marco Civil da Internet, então, cria uma cláusula de jurisdição, ao determinar que todo tratamento de dado pessoal que ocorre no Brasil, ainda que parcialmente ou quando o dado tenha sido coletado apenas pela localização do terminal em território brasileiro, deve se adequar à legislação brasileira[38].

O § 2º do artigo amplia de forma significativa a abrangência da jurisdição, que fica mantida mesmo se a sede da empresa estiver localizada no exterior, bastando que ela possua uma subsidiária ou escritório do mesmo grupo econômico no Brasil ou que ela oferte serviços a cidadãos brasileiros.

O art. 11, então, é interpretado pelas autoridades administrativas e judiciárias no sentido de que o Marco Civil da Internet não limita a aplicação da jurisdição brasileira apenas para as operações de tratamento de dados pessoais (forma que se denominam as operações de coleta, uso, armazenamento e guarda de dados), mas a estabelece também para a aplicação da lei material e processual penal no que diz respeito ao acesso de dados por autoridades investigativas no bojo de um processo criminal.

Por outro lado, Jacqueline Abreu, pesquisadora na área de Direito e tecnologia, entende que a jurisdição brasileira deve ser aplicada somente nas operações específicas de tratamento de dados pessoais, mas não para o fornecimento de dados armazenados no exterior às

---

[38] ARTESE, Gustavo (coord.). *Marco Civil da Internet: Análise Jurídica sob uma Perspectiva Empresarial.* 1. ed. São Paulo: Quartier Latin, 2015, p. 85.

autoridades. Ainda, sustenta que a jurisdição brasileira não deve ser aplicada indistintamente, para que também sejam respeitadas as legislações de outros países e acordos de cooperação internacional[39].

A redação da parte final do artigo 11, que gera a polêmica, entrou no lugar de outro dispositivo que instituiria uma política de localização de dados, em que as empresas de Internet no Brasil teriam a obrigação de estabelecer seus bancos de dados e armazenar todos os dados gerados pelos usuários brasileiros dentro do território nacional. Se esse fosse o caso, as autoridades teriam acesso facilitado às informações, sem que o ocorresse o referido conflito de jurisdição[40].

Contudo, existia pressão muito forte da sociedade civil contra essa política de localização de dados, pois teria viés muito radical e acabaria inviabilizando e encarecendo a prestação de serviços pelas empresas de Internet de outros países. Dessa forma, o dispositivo foi retirado do Projeto de Lei e as autoridades tiveram que se conformar com a redação que o artigo 11 ganhou, na parte que estabelece que a jurisdição brasileira deve ser respeitada em toda operação de tratamento de dados.

Essa cláusula de jurisdição estabelecida pelo Marco Civil da Internet, contudo, contrapõe-se à legislação americana.

O *Stored Communications Act*, codificado no Título 18[41] do Código dos EUA, §§ 2701-2712, é a lei que dispõe sobre o tratamento legal aplicável a comunicações armazenadas, estabelecendo regime proibitivo de divulgação de tais dados, salvo nas exceções[42] previstas na própria lei.

---

[39] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Desafios da coleta de evidências digitais e a cooperação internacional para acesso a dados. 2017. (1h04m). Disponível em: <https://www.youtube.com/watch?v=mNGspCMf8Ag>. Acesso em: 09/05/2018.

[40] MASSO, F. D.; ABRUSIO, J.; FILHO, M. A. F (coord.). Marco Civil da Internet: Lei 12.965/2014. 2. ed. São Paulo: Editora Revista dos Tribunais, 2014, p. 152.

[41] O Título 18 do Código dos Estados Unidos é o principal código penal do governo federal do país. Trata sobre crimes federais e processo penal.

[42] A proibição de divulgação de conteúdo de comunicações armazenadas possui 8 exceções taxativas previstas no parágrafo 2702(b) do SCA: (1) divulgação ao próprio usuário ou destinatário da comunicação; (2) divulgação autorizada por mandado ou ordem judicial proferidos nos termos específicos das leis americanas; (3) mediante expresso consentimento legal de quem enviou a comunicação ou do destinatário da comunicação; (4) para um pessoa empregada ou autorizada ou sujas instalações são utilizadas para encaminhas essa comunicação para seu destino; (5) conforme seja necessário para a prestação do serviço ou a proteção dos direitos ou propriedade do provedor desse serviço; (6) fornecimento ao National Center for Missing and Exploited Children, em conexão com denúncias apresentadas de acordo com as leis federais de segurança infantil; (7) se o provedor obteve inadvertidamente o conteúdo para a prática de um crime; e (8) fornecimento a entidade governamental, se o

A referida norma foi promulgada em 1986, dado o receio de que a legislação vigente na época não fosse suficiente para assegurar o direito à privacidade das comunicações e dos dados pessoais relacionados ante o desenvolvimento das novas tecnologias decorrentes da Internet.

O *SCA* estipula, dentre outras coisas, que as requisições emanadas por entidades governamentais estrangeiras a empresas americanas devem passar, necessariamente, pelo crivo da Justiça americana para poderem ser cumpridas. Em outras palavras, impõe a reserva de juiz como requisito ao cumprimento dos pedidos de quebra do sigilo do conteúdo das comunicações eletrônicas e fornecimento dos dados, quando formulados por autoridades de outros países.

As empresas de tecnologia que operam em outros países, por conseguinte, recusam-se a cumprir as determinações judiciais locais, sob alegação de contrariedade às normas americanas e para evitar eventual responsabilização judicial em seu país de origem.

Tais empresas, portanto, defendem que a requisição judicial de informações para obtenção de dados armazenados em servidores no exterior deve se dar por meio da cooperação jurídica internacional, mais especificamente, através do MLAT (*Mutual Legal Assistance Treaty*).

O MLAT, ou – em português – Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, é o instrumento elegido pelos países para a execução das tarefas das autoridades responsáveis pela investigação, inquérito, ação penal e prevenção do crime por meio da cooperação e assistência judiciária mútua em matéria penal.

O acordo entre os países foi celebrado em Brasília em outubro de 1997, aprovado pelo Congresso Nacional por meio do Decreto Legislativo nº 262, em dezembro de 2000, e recepcionado no ordenamento jurídico brasileiro na forma do Decreto nº 3.810, em maio de 2001.

A controvérsia que se instaura, portanto, é saber se é necessário o MLAT (pedido de cooperação jurídica internacional) ou se uma autoridade brasileira tem a prerrogativa de ordenar diretamente às empresas de Internet dos EUA que entreguem dados, independentemente de autorização da Justiça americana.

---

provedor acredita haver situação de emergência envolvendo perigo de morte ou ferimento físico grave do indivíduo.

Apesar do caso do WhatsApp ter inflamado o debate, muitas outras empresas já lidaram com o problema no Brasil, sempre se baseando no argumento de jurisdição. Nas ocasiões em que a controvérsia chegou ao STJ, as decisões foram desfavoráveis às empresas de tecnologia.

No caso, a Facebook Brasil impugnava decisão judicial que, em sede de inquérito, determinou que a empresa fornecesse dados telemáticos de contas de investigados, sob pena de multa diária de R$ 50 mil. A empresa, utilizando-se do argumento de jurisdição, alegou que a filial brasileira se dedica apenas à prestação de serviços relacionados à locação de espaços publicitários, veiculação de publicidade e suporte de venda, sendo a Facebook Inc. (empresa-sede) a responsável pelo controle da plataforma e a única capaz de fornecer as informações requisitadas. Dessa forma, considerou necessário o pedido de cooperação jurídica internacional.

A 5º Turma, por unanimidade, entendeu que a empresa jurídica multinacional, por estar instituída e em atuação no país, submete-se necessariamente às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pela Justiça[43].

Ainda, destacaram os Ministros que incumbe ao magistrado autorizar a quebra de sigilo de dados telemáticos, podendo ele se valer dos meios necessários e adequados para fazer cumprir sua decisão, notadamente quando a medida coercitiva imposta (fixação de astreintes) está prevista em lei.

Em outro caso, a Yahoo! Brasil, em suas razões recursais, alegava a impossibilidade de fornecer os dados de e-mail requisitados pela Justiça, pois o domínio solicitado (@yahoo.com) pertenceria à provedora americana Yahoo! Inc., empresa sediada e que armazena seus dados nos Estados Unidos. Os Ministros, reafirmando a jurisprudência fixada no caso anterior, também negaram provimento ao recurso[44].

Diferentemente do entendimento adotado pelo STJ e pelas autoridades investigativas brasileiras, há corrente[45] que reconhece como legítima o argumento de jurisdição utilizado

---

[43] STJ. RMS 55.109/PR, Rel. Ministro REYNALDO SOARES DA FONSECA, QUINTA TURMA, julgado em 07/11/2017, DJe 17/11/2017.
[44] STJ. RMS 55.019/DF, Rel. Ministro JOEL ILAN PACIORNIK, QUINTA TURMA, julgado em 12/12/2017, DJe 01/02/2018.
[45] GIACCHETTA, A. Z; FREITAS, C. T; MENEGUETTI, P. G. *Marco Civil da Internet põe fim a lacunas na legislação.* Disponível em: <https://www.conjur.com.br/2014-abr-30/marco-civil-internet-poe-fim-lacunas-existentes-legislacao#author>. Acesso em: 09/05/2018.

pelas empresas de tecnologia, que reputam necessário o uso do MLAT para a coleta de dados eletrônicos armazenados no exterior.

Para essa corrente, o art. 11 do Marco Civil da Internet é claro ao estabelecer a aplicação da jurisdição brasileira para as operações de coleta, armazenamento, guarda e tratamento de registros, dados e comunicações, mas não para o efetivo fornecimento dessas informações.

Dessa forma, a despeito de considerar obrigatória a observância da legislação brasileira, as disposições no Marco Civil da Internet não teriam o condão de impedir a aplicação da lei estrangeira, notadamente nos casos em que se pretende colher prova localizada fora do Brasil, hipótese em que as normas do respectivo país devem ser observadas.

Assim, a vinculação do provedor estrangeiro a processos judiciais em trâmite no Brasil continuaria sujeita aos tratados internacionais aplicáveis, como o MLAT, conforme denota o próprio texto da Lei, em seu art. 3º, 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".

Além disso, sustentam que o Marco Civil da Internet não institui qualquer espécie de responsabilidade solidária ou subsidiária entre o provedor estrangeiro e outros integrantes do mesmo grupo econômico sediados no Brasil com relação ao cumprimento de ordens judiciais, notificações extrajudiciais e requisições de autoridades policiais, administrativas ou do Ministério Público, visando a remoção ou fornecimento de conteúdos e dados.

A única hipótese de responsabilidade solidária prevista na Lei diz respeito à obrigação de pagamento de multa imposta ao provedor estrangeiro pelo descumprimento das obrigações legais relativas à guarda e divulgação dos registros de conexão e acesso a aplicações, dados pessoais e conteúdo de comunicações privadas de usuários[46]. Nesses casos, também poderão ser submetidas a essas sanções suas sucursais, escritórios ou estabelecimentos situados em território nacional, conforme o art. 12, parágrafo único.

Apesar do debate entre as diferentes correntes, as origens da controvérsia estão ligadas ao mau desempenho do MLAT, que não funciona tão bem atualmente e cuja burocracia e lentidão frustram as autoridades brasileiras.

[46] ARTESE, Gustavo (coord.). *Marco Civil da Internet: Análise Jurídica sob uma Perspectiva Empresarial.* 1. ed. São Paulo: Quartier Latin, 2015, p. 86.

O procedimento do MLAT, que será detalhadamente analisado no próximo capítulo, tem várias etapas e passa por diversas autoridades tanto do Brasil quanto dos EUA. Esse mecanismo excessivamente burocrático faz com que os pedidos de fornecimento de dados demorem, em média, 13 meses, quantidade muito grande de tempo, considerando o dinamismo das comunicações e plataformas de Internet[47].

Os acordos de cooperação internacional foram pensados inicialmente para resolver situações consideradas excepcionais, isto é, casos em que uma autoridade no Brasil precisava ouvir testemunha ou obter documento que estava no exterior, hipóteses que, na prática, eram muito raras.

Nesse sentido, o mecanismo do MLAT foi idealizado para lidar com documentos físicos e pessoas que estavam no exterior. Quando se pensa em Internet e dados digitais, contudo, a realidade é completamente diferente. As empresas de Internet, apesar de estarem situadas em determinado país, estão presentes em todo o mundo e, em que pese seus dados estarem armazenados em servidores em algum lugar do planeta, eles são capazes de transitar rapidamente sem que o acesso à plataforma esteja condicionado a sua localização.

Dessa forma, a ineficiência e defasagem do mecanismo fazem com que as autoridades investigativas e os juízes busquem um alicerce jurídico para considerar o MLAT desnecessário e requerer as informações que consideram cruciais para o inquérito ou processo penal diretamente aos provedores no Brasil.

Do outro lado, as empresas de tecnologia defendem insistentemente o argumento do conflito de jurisdição, em razão da aparente violação às disposições do *Stored Communications Act* e da sua alegada impossibilidade de obter dados controlados somente pela empresa-sede nos Estados Unidos.

Em defesa da segunda corrente, há Ação Declaratória de Constitucionalidade em tramitação no STF, buscando declarar válidos os mecanismos de cooperação jurídica internacional.

2.3 A ADC nº 51 no Supremo Tribunal Federal

[47] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Desafios da coleta de evidências digitais e a cooperação internacional para acesso a dados. 2017. (1h04m). Disponível em: <https://www.youtube.com/watch?v=mNGspCMf8Ag>. Acesso em: 09/05/2018.

A Ação Declaratória de Constitucionalidade nº 51[48], de relatoria do Ministro Gilmar Mendes, foi ajuizada pela Assespro Nacional[49] (Federação das Associações das Empresas de Tecnologia da Informação). Nela, requer que o STF declare a constitucionalidade do Decreto nº 3.810/2001, que recepciona o MLAT no Brasil; do art. 237[50], II, do Código de Processo Civil, que versa sobre a expedição de carta rogatória em casos de cooperação jurídica internacional em processo em curso na Justiça brasileira; e dos artigos 780[51] e 783[52], do Código de Processo Penal, que também tratam da expedição de carta rogatória para diligências necessárias à instrução do processo penal.

Em outras palavras, pedem que os Ministros reconheçam a validade dos mecanismos de cooperação jurídica internacional como forma de realização de diligências processuais e obtenção de provas no exterior em processos em curso no Brasil, especialmente em relação à coleta de dados eletrônicos.

Os dispositivos em epígrafe na ADC nº 51 compõem mecanismos à disposição de autoridades brasileiras para a realização de atos de comunicação processual, como citações, intimações e notificações; atos de investigação ou instrução, como oitivas, obtenção de documentos, quebra de sigilo bancário ou telemático; ou ainda algumas medidas constritivas de ativos, como o bloqueio de bens ou valores no exterior.

Em matéria de cooperação jurídica internacional, cada país é representado por sua autoridade central. No Brasil, o Ministério da Justiça, por intermédio do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional da Secretaria Nacional de Justiça (DRCI/SNJ), atua como autoridade central para tais fins. O DRCI recebe os pedidos da Justiça e os encaminha para outros países, de acordo com as regras estabelecidas por tratados bilaterais ou multilaterais em que o Brasil faz parte.

---

[48] ADC 51. Andamentos disponíveis em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379>. Acesso em: 06/08/2018.

[49] Petição inicial da ADC nº 51. Disponível em: <https://www.jota.info/wp-content/uploads/2017/11/ADC-Assespro-MLAT.pdf> . Acesso em:

[50] CPC: "Art. 237. Será expedida carta:
[...] II - rogatória, para que órgão jurisdicional estrangeiro pratique ato de cooperação jurídica internacional, relativo a processo em curso perante órgão jurisdicional brasileiro".

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

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

A Assespro defende[53], então, que é por meio da cooperação jurídica internacional entre autoridades judiciárias brasileiras e estrangeiras que deve ser requerida a coleta de dados telemáticos armazenados no exterior às sedes americanas, e não diretamente às filiais brasileiras.

A entidade de classe de âmbito nacional argumenta que os dispositivos do CPC e do CPP em debate têm sua constitucionalidade questionada por diversas decisões judiciais, e, por esse motivo, os mecanismos de cooperação internacional não são utilizados pelos magistrados e pelas autoridades investigativas. Ainda, aduz que o MLAT tem experimentado recusa de aplicabilidade ainda maior quando se tratam de empresas do setor tecnologia, através de decisões judiciais fundamentadas no princípio da soberania nacional brasileira.

No mais, a peticionante argumenta que a competência para determinar a entrega de dados é da autoridade competente no território em que o provedor de aplicação, com a legítima autorização para controlar os dados, estiver localizado. Assim, como não há qualquer obrigação prevista na legislação brasileira para que os dados de aplicações de Internet estejam localizados no Brasil, sustenta que a efetiva localização do controlador de dados é essencial para definir a jurisdição competente.

Com base nisso, a jurisdição competente, quando se tratam de empresas americanas, seria a dos Estados Unidos, que veda a disponibilização de conteúdos de comunicações eletrônicas sem prévia autorização de sua Justiça, conforme estipula o *Stored Communications Act*.

Apesar disso, alega que afastar a aplicabilidade dos artigos do CPC e do CPP referentes à carta rogatória e do procedimento previsto no Decreto nº 3.810/2001 é prática comum nos tribunais brasileiros, que enxergam a entrega dos dados diretamente pela filial brasileira da empresa como via processual cabível, em respeito à soberania nacional.

Porém, sustenta a requerente que não há ofensa à soberania brasileira em face do respeito à soberania de Estado estrangeiro e, portanto, o procedimento do MLAT e as cartas rogatórias seriam os meios consonantes com o devido processo legal para a obtenção dos dados em causa, capazes de evitar o conflito de jurisdição gerado por parte do Judiciário brasileiro.

[53] A Assespro também defende a aplicação do MLAT para a requisição de dados bancários armazenados no exterior, porém este não é o escopo do presente trabalho.

Requer, ainda, a concessão de medida cautelar para suspender o julgamento ou a eficácia de decisões nos processos em que são discutidas as mesmas controvérsias judiciais do presente caso.

Na qualidade de *amicus curiae*, a Facebook Brasil obteve o ingresso no feito e se posicionou de forma semelhante à Assespro. Insurge-se contra a maneira que os tribunais descartam a aplicação da cooperação jurídica internacional e requerem diretamente à filial brasileira a coleta de dados eletrônicos, apesar destas não terem acesso às informações. Critica o fato de serem aplicadas às empresas de tecnologia penalidades pecuniárias, a responsabilização criminal de seus dirigentes e até a suspensão de suas atividades como resposta ao inevitável descumprimento das decisões judiciais.

Com posicionamentos similares, também ingressaram no feito como *amici curiae* a Yahoo! Brasil, o Instituto de Referência em Internet e Sociedade (IRIS). Por outro lado, a Sociedade de Usuários de Tecnologia (SUCESU Nacional), que também participa da ação como "amiga da corte", requer o não conhecimento da ação pela ausência de controvérsia constitucional relevante em relação aos dispositivos em epígrafe.

A Advocacia-Geral da União, por sua vez, sustenta que os mecanismos de cooperação internacional indicados pela autora não constituem as únicas maneiras possíveis de solicitar a disponibilização de dados que se encontrem sob domínio de entidade sujeita a jurisdição de outro Estado. Aponta, além do art. 11 do Marco Civil da Internet, a Lei nº 12.965/2014 (que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil) como base legal para justificar a obrigação de atendimento de requisições feitas por autoridades públicas diretamente a empresas brasileiras subsidiárias de empresas estrangeiras provedoras de Internet. No mais, reconhece a compatibilidade das normas indicadas como objeto da ação com a Constituição Federal, mas assevera a impossibilidade de atribuir à declaração de constitucionalidade o efeito pretendido pela autora.

No mesmo sentido se posicionou a Procuradoria-Geral da República. Manifestou-se pela constitucionalidade dos dispositivos constitucionais, sem, contudo, considerá-los os únicos meios possíveis de obtenção de dados telemáticos por autoridades brasileiras, de modo que a declaração de constitucionalidade não resultaria na obrigatoriedade de adoção dos instrumentos neles previstos.

De fato, o propósito de uma Ação Declaratória de Constitucionalidade é sanar um estado de incerteza gerado por dúvidas ou controvérsias sobre a legitimidade de lei ou ato

normativo federal, que pode resultar de pronunciamentos contraditórios dos órgãos jurisdicionais[54]. Contudo, não possui o efeito almejado pela Assespro de tornar obrigatórios os mecanismos de cooperação jurídica internacional previstos pelos dispositivos legais, conforme apontam a PGR e a AGU em suas manifestações nos autos.

Dessa forma, é possível imaginar que o julgamento da ADC nº 51 não seja suficiente para solucionar a controvérsia acerca da coleta de dados eletrônicos armazenados no exterior no bojo de uma investigação ou do processo criminal.

Apesar disso, é evidente que a fundamentação jurídica utilizada pelos Ministros pode inflamar a discussão e até encaminhar uma solução para o conflito, caso deem instruções de como os órgãos jurisdicionais devem se portar quando se depararem com o tema. Tal deliberação, ainda que não vinculante, pode servir de alicerce jurídico para a tomada de decisões dos juízes e tribunais hierarquicamente inferiores na seara de uma investigação criminal ou na instrução de um processo penal.

Deixando de lado a discussão acerca da possível contribuição que o STF pode ou não fornecer ao debate, é necessário avaliar se as empresas de tecnologia estrangeiras filiadas no Brasil podem ou não cumprir os pedidos de fornecimento de dados feitos pelas Justiça brasileira.

2.4 Os obstáculos técnicos e jurídicos enfrentados pelas empresas de tecnologia

Grande parte das empresas provedoras de serviços de Internet se insurgem contra a requisição direta das autoridades brasileiras às suas filiais localizadas no Brasil com base em argumentos de ordem técnica, devido à incapacidade prática de fornecer as informações almejadas; e de ordem jurídica, em razão do conflito entre esses pedidos e a legislação americana.

Inicialmente, as filiais brasileiras de empresas de tecnologia sustentam não possuir condições técnicas para fornecer as informações requisitadas, visto que não controlam ou sequer possuem acesso à plataforma eletrônica e aos dados nela armazenados. Nesse sentido, verifica-se que as filiais no Brasil são meros escritórios, responsáveis estritamente por atividades diversas, como à venda de publicidade. Já empresas-sede, localizadas nos Estados

[54] MENDES, G. F.; BRANCO, P. G. G. Curso de direito constitucional. 7. ed. São Paulo: Saraiva, 2012, p. 1132-1134.

Unidos, efetivamente controlam e operam as plataformas do serviço e são os únicos capazes de acessar e fornecer os dados.

Em sua petição de ingresso na ADC nº 51 como *amicus curiae*, o Facebook Brasil afirma ter como objeto social a prestação de serviços relacionados à comercialização de espaços publicitários, veiculação de publicidade e suporte de vendas, não possuindo qualquer relação com a gestão, operação e administração do Serviço Facebook e nem autorização para acessar as contas ou dados de usuários. Tais tarefas são de controle exclusivo dos operadores do Serviços Facebook, quais sejam, a Facebook Inc., dos EUA, e a Facebook Ireland Limited, da Irlanda.

Em manifestação idêntica aos autos da ADC nº 51, a Yahoo! Brasil sustenta oferecer uma grande variedade de aplicações de Internet, incluindo serviço de e-mail, através do seu portal "http://br. yahoo.com/". Tal como se dá no Brasil, no exterior diversas empresas estrangeiras também oferecem aplicações de Internet sob a marca "Yahoo!".

Assim, em relação aos usuários inscritos nos serviços de Internet oferecidos no Brasil, sob domínio "br.", a Yahoo! Brasil fornece os dados pessoais e conteúdo de comunicações privadas disponíveis em seus servidores, quando requeridos através do meio legal cabível, sem qualquer oposição ou resistência. Contudo, quando há ordens judiciais requerendo a coleta de dados que não dizem respeito aos serviços oferecidos pela filial brasileira, mas pelas empresas estrangeiras, a Yahoo! Brasil não é capaz de cooperar, tendo em vista que se tratam de dados controlados por empresa diversa do mesmo grupo e armazenados em outro país.

Segundo Francisco Rezek, as empresas estrangeiras de tecnologia possuem no Brasil apenas uma empresa subsidiária ou outra empresa do mesmo grupo econômico, mas em que nada se relacionam com o serviço prestado. Destaca que enquanto a empresa central oferece e controla determinado serviço *online*, suas subsidiárias, localizadas em mercados relevantes, oferecem a possíveis anunciantes a oportunidade de veicular peças publicitárias em espaços pré-definidos na plataforma mantida pela empresa central[55].

Para o professor, são empresas distintas: há a empresa-mãe sediada no exterior, responsável pelo serviço digital e com personalidade jurídica própria; e também há a empresa subsidiária, sediada no Brasil, responsável apenas pela prestação de serviços acessórios ao

[55] Parecer do Professor Francisco Rezek nos autos da ADC nº 51. Disponível em: http://www.franciscorezek.adv.br/wp-content/uploads/2018/02/Parecer-FR-MLAT-STF.pdf>. Acesso em: 19/06/2018;

principal e detentora de personalidade jurídica própria, à luz de outra ordem jurídica nacional. Assim, não há como confundir uma com a outra, nem como exigir desta a conduta exigível daquela.

Além dos empecilhos técnicos expostos, as empresas de tecnologia ainda encontram embaraço jurídico. Isso porque o conteúdo das comunicações não pode ser fornecido às autoridades brasileiras de forma direta, exceto quando há um mandado judicial emitido por um tribunal americano ou o caso concreto se adeque às demais exceções à regra de proibição de divulgação de conteúdo disposta no *SCA*.

Quanto à regra do *SCA*, Eric H. Holder[56], em parecer anexado à manifestação da Facebook Brasil na ADC nº 51, afirma que:

> *(...) a lei de Comunicações Armazenadas (U.S. Stored Communications Act – SCA) proíbe, em termos gerais, que prestadores de serviços de comunicações eletrônicas subordinados à jurisdição dos EUA revelem comunicações de seus usuários a qualquer outra pessoa, exceto se uma das exceções previstas em lei for aplicável. Responder aos pedidos de autoridades policiais estrangeiras não constitui uma dessas exceções, e, portanto, prestadores de serviços não podem em geral responder a esses pedidos unilaterais (por exemplo, um pedido vindo diretamente de um órgão de segurança pública estrangeira ao prestados dos EUA) sem violar a lei dos EUA e estando sujeito a penalidades substanciais.*

Isto é, mesmo que não seja acolhido o argumento das empresas acerca dos referidos impedimentos técnicos, há restrição legal imposta pelo *SCA*. Assim, o fato de uma solicitação de autoridade policial ou judiciária estrangeiras ser dirigida à subsidiária da empresa situada na jurisdição estrangeira não altera a aplicabilidade da proibição do *SCA* acerca do fornecimento do conteúdo de comunicações privadas.

Diante desse cenário, verifica-se que eventual recusa quanto ao fornecimento de conteúdo de comunicações às autoridades brasileiras não decorre de desrespeito, resistência injustificada ou arrogância dos provedores de aplicações de Internet. Decorre, na realidade, do conflito de normas domésticas brasileiras e americanas, que deve ser resolvido através da cooperação internacional.

[56] Eric H. Holder foi Procurador-Geral (Attorney General) dos Estados Unidos entre os anos de 2009 e 2015.

No mais, os referidos empecilhos são utilizados de forma reiterada pelas empresas de tecnologia para justificar o não cumprimento das determinações judiciais que exigem a entrega de dados dos usuários de seus serviços. Assim não há porque duvidar da veracidade dessas alegações, tendo em vista que as empresas de tecnologia não possuem nenhum interesse em obstaculizar investigações e processos criminais e em criar um ambiente "seguro" para a prática de crimes.

Esse foi o entendimento adotado recentemente pelo TJDFT[57], cuja Câmara Criminal anulou multa imposta ao Facebook pela recusa em fornecer os dados requisitados. Com efeito, adotaram tese de que se a filial nacional é responsável exclusivamente pela comercialização de publicidade e não opera em território nacional atos de coleta, armazenamento, guarda e tratamento de registros, dados pessoais e de comunicações, não pode se sujeitar às normas de proteção e tratamento de dados previstas na legislação brasileira.

Ainda, consignaram que a filial nacional, em razão da limitação técnica do serviço que presta no país, não pode ser obrigada pela Justiça brasileira a transgredir sua competência e ter acesso a informações armazenadas em servidores situados no exterior sem seguir os protocolos internacionais que regulam a matéria, sob pena de ofensa à soberania dos Estados.

Assim, eventual assistência judiciária em matéria penal com o governo de outros países deve observar princípios de cooperação e soberania, a exemplo do Decreto nº 3.810/2011, que promulga acordo feito entre o Brasil e os Estados Unidos e prevê a forma que deverá ser feita solicitação de assistência.

Portanto, o capítulo seguinte será dedicado ao exame das estruturas jurídicas da cooperação internacional e ao estudo do efetivo funcionamento do MLAT, a fim de que seja medida a utilidade do aparato de auxílio entre os países para a solução da controvérsia.

[57] TJDFT. MANDADO DE SEGURANÇA: MS 2017.00.2.020591-2, Rel. Desembargador JAIR SOARES, CÂMARA CRIMINAL, julgado em 29/01/2018, DJe: 06/02/2018.

3. O MLAT COMO MECANISMO DE COOPERAÇÃO JURÍDICA INTERNACIONAL PARA ACESSO A DADOS ELETRÔNICOS

3.1 A cooperação jurídica internacional em matéria penal

A disseminação do acesso à Internet, como dito anteriormente, acaba facilitando o planejamento e o cometimento de crimes pelos seus usuários. Os dados capazes de elucidar investigações ou instruir processos contra esses maus usuários da rede muitas vezes estão armazenados no exterior, nos servidores da empresa provedora da aplicação eletrônica utilizada.

Com a discussão aberta acerca da legalidade da requisição de informações diretamente às filiais brasileiras, é necessário buscar outro meio para a coleta de dados eletrônicos. Assim, as empresas de tecnologia defendem a utilização de ferramenta de auxílio internacional para tentar quebrar a barreira entre os países e facilitar a entrega dessas informações sensíveis às autoridades brasileiras.

Nesse quadro, o recurso disponível às autoridades é a cooperação jurídica internacional. Fechar-se à cooperação é transformar seu país em refúgio para criminosos, e arriscar-se a encontrar portas fechadas para os requerimentos formulados ao exterior, já que a política predominante nessa seara é a da reciprocidade[58].

A cooperação penal internacional diz respeito ao conjunto de mecanismos jurídicos postos à disposição de Estados e organizações internacionais especializados para viabilizar ou facilitar a persecução criminal ou a execução penal[59].

A cooperação se faz necessária quando, dentro do processo penal, há elementos de estraneidade. Isto é, quando há fatores estranhos à jurisdição local que tornam necessário o auxílio da jurisdição de outro país para que determinadas diligências processuais possam ser cumpridas[60].

Os mecanismos de cooperação internacional acabam tendo a natureza de procedimentos acessórios da ação penal, já que se destinam, por exemplo, à produção de provas e à realização

---

[58] BALTAZAR JR., J. P; LIMA, L. F (org.). *Cooperação jurídica internacional em matéria penal.* 1 ed. Porto Alegre: Verbo Jurídico, 2010, p. 16.
[59] Ibid., p. 61.
[60] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Acesso a comunicações eletrônicas e criptografia: garantias, prerrogativas e devido processo legal. 2017. (2h29m). Disponível em: <https://www.youtube.com/watch?v=W_b2Jr9wFXk>. Acesso em: 09/05/2018.

de diligências processuais, de modo que suas medidas estarão sujeitas aos mesmos princípios garantistas e normas que regem o devido processo[61] legal penal em cada um dos Estados cooperantes[62].

Os pedidos de cooperação internacional podem ser classificados a partir da perspectiva de um dos Estados envolvidos na relação internacional. Do ponto de vista brasileiro, a cooperação penal será ativa quando o Brasil for o Estado requerente, e passiva quando for o Estado requerido[63].

Em classificação diversa, a cooperação internacional será administrativa, quando realizada por autoridades não-jurisdicionais, a exemplo do Ministério Público e da Polícia, ou judicial, quando empreendida por órgãos judiciais em sentido estrito.

Se a medida que se pretende realizar no outro país se inserir no âmbito de um processo judicial, a autoridade competente para iniciar o pedido de cooperação é o juiz responsável pelo processo, não havendo necessidade de submeter a requisição a autoridade judiciária hierarquicamente superior ou diversa daquela competente para o caso. Não havendo processo judicial instaurado, não há que se discutir competência jurisdicional, senão a competência ou atribuição da autoridade administrativa para formular o pedido de cooperação[64].

A cooperação penal pode ser indireta ou direta. A primeira modalidade se dá quando há intervenção de um ou mais órgãos de ligação, a exemplo das chancelarias e dos ministérios de justiça, ou simplesmente a intermediação da autoridade central previamente estabelecida. Na hipótese da cooperação direta, não há a utilização da via diplomática e nem de autoridades centrais como órgãos de ligação. Nesse modelo, as autoridades envolvidas de cada um dos Estados se transmitem mutuamente os pedidos de cooperação, sem a presença de intermediários[65].

Para a realização das medidas indiretas de cooperação, é necessário que cada um dos Estados envolvidos no procedimento disponha de órgãos encarregados da tramitação e da execução dos pedidos de instrução criminal ou de execução penal. Nessa toada, é chamado de

[61] Destaca-se os art. 28 e seguintes do CPC, que tratam do mecanismo do auxílio direto.
[62] BALTAZAR JR., J. P; LIMA, L. F (org.). *Cooperação jurídica internacional em matéria penal*. 1 ed. Porto Alegre: Verbo Jurídico, 2010, p. 63.
[63] Ibid., p. 72.
[64] Ibid., p. 26/27.
[65] Ibid., p. 73.

autoridade central o órgão técnico especializado, em regra não-jurisdicional, que se encarrega da interlocução internacional na cooperação jurídica em matéria civil ou penal.

Atualmente, para a maior parte dos tratados de assistência jurídica em matéria penal firmados pelo Brasil, é indicado como autoridade central o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), órgão da Secretaria Nacional de Justiça, do Ministério da Justiça[66].

Em síntese, o DRCI/MJ atua na cooperação penal passiva e ativa, no modelo de execução indireta, pois o órgão não pode cumprir diretamente as solicitações de Estados estrangeiros e nem pode requerer medidas de ofício no exterior. Apenas o Poder Judiciário, o Ministério Público e, em alguns casos, a Polícia, podem tomar a iniciativa de pedidos de cooperação internacional[67].

Em ambos os casos de assistência ativa e passiva, o DRCI/MJ verifica a regularidade formal e documental dos pedidos, a fim de que não haja óbices de tramitação perante os órgãos executantes aqui ou no estrangeiro. Na cooperação ativa, o DRCI/MJ recebe os pedidos de auxílio direto das autoridades competentes, se houver tratado internacional vigente (MLAT) e os encaminha aos órgãos centrais estrangeiros. Se não houver tratado entre os Estados cooperantes, o DRCI/MJ envia os pedidos de auxílio direto no exterior por meio da Divisão Jurídica do Ministério da Justiça, que os fará tramitar via diplomática[68].

A autoridade central é escolhida pelo Estado e indicada na assinatura, ratificação ou adesão ao tratado. No caso do MLAT entre Brasil e Estados Unidos, a autoridade central é designada no próprio texto do acordo, no qual o DRCI/MJ é indicado. A função correspondente no ordenamento jurídico americano é exercida pelo Escritório de Assuntos Internacionais da Divisão Criminal do Departamento de Justiça[69] do Estados Unidos[70].

Na cooperação jurídica internacional, sempre será observado o Direito aplicável do país *requerido* para produção do ato requisitado, salvo se existir tratado regulando a cooperação e

---

[66] Nos casos do tratado bilateral entre Brasil e Portugal (Decreto nº 1.320/1994) e o MLAT entre o Brasil e o Canadá (Decreto nº 6.747/2009), a autoridade central é o Ministério Público Federal, por intermédio da Assessoria de Cooperação Jurídica Internacional (ASCJI), órgão da Procuradoria-Geral da República.

[67] BALTAZAR JR., J. P; LIMA, L. F (org.). *Cooperação jurídica internacional em matéria penal.* 1 ed. Porto Alegre: Verbo Jurídico, 2010, p. 79.

[68] Ibid., p. 80.

[69] Nos EUA, o Departamento de Justiça é encabeçado pelo Procurador-Geral. Assim, vale dizer que as funções de Ministro da Justiça e Chefe do Ministério Público estão reunidas em uma só pessoa.

[70] BALTAZAR JR., J. P; LIMA, L. F (org.). *Cooperação jurídica internacional em matéria penal.* 1 ed. Porto Alegre: Verbo Jurídico, 2010, p. 77.

este dispor de maneira diversa[71]. Trata-se do princípio *locus regit actum*, oriundo do Código de Bustamante, segundo o qual os Estados requeridos aplicam suas próprias leis processuais para cumprir requisições de cooperação[72].

Em outras palavras, o país requerente não pode impor efeitos extraterritoriais às suas regras em detrimento das normas do país requerido, que teria sua soberania violada. Caso o país requerente queira colher prova no país requerido, serão as regras deste que regularão o cumprimento da diligência[73].

Com efeito, se no país requerido, diferentemente do país requerente, houver reserva de juiz (isto é, se sua legislação estabelecer que autoridade judiciária local deve aprovar o pedido de cooperação para que ele seja realizado), o pedido de produção de prova ainda assim deve ser submetido a autoridade judiciária do país requerido.

Traçando um paralelo com o caso, fica claro que as autoridades brasileiras, ao realizar o pedido de cooperação internacional para a obtenção de dados eletrônicos armazenados no exterior, devem respeitar a legislação americana, que exige a prévia autorização de sua Justiça para que as empresas de Internet possam fornecer as informações requisitadas.

No mais, a assistência jurídica mútua em matéria penal tem por base tratados comumente chamados de *Mutual Legal Assistance Treaties* (MLAT[74]), um sistema de cooperação penal que transita por intermédio de autoridades centrais. Em regra, é mais célere e menos dispendioso que as cartas rogatórias, que, por sua vez, tramitam pela via diplomática e dependem da cortesia internacional (*comitas gentium*)[75].

A estrutura do MLAT Brasil-EUA, em análise neste trabalho, segue um padrão comum à maioria dos tratados bilaterais dessa espécie. A respeito das regras de procedimento penal transnacional, não há necessidade de interposição legislativa para sua plena execução,

---

[71] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Acesso a comunicações eletrônicas e criptografia: garantias, prerrogativas e devido processo legal. 2017. (2h29m). Disponível em: <https://www.youtube.com/watch?v=W_b2Jr9wFXk>. Acesso em: 09/05/2018.

[72] BALTAZAR JR., J. P; LIMA, L. F (org.). *Cooperação jurídica internacional em matéria penal.* 1 ed. Porto Alegre: Verbo Jurídico, 2010, p. 27.

[73] Ibid., p. 28.

[74] Atualmente, no Brasil, já existem em vigor acordos multilaterais que contemplam a assistência jurídica internacional no âmbito de diversos foros internacionais: Organização das Nações Unidas (ONU), Organizações dos Estados Americanos (OEA), Mercosul, Organização para Cooperação e Desenvolvimento Econômico (OCDE). Além disso, possui tratados bilaterais de assistência jurídica em matéria penal em vigor com mais de 20 países: Bélgica, Canadá, Colômbia, China, Coreia do Sul, Cuba, EUA, Espanha, França, Honduras, Itália, México, Nigéria, Panamá, Peru, Portugal, Reino Unido, Suíça, Suriname, Turquia e Ucrânia.

[75] BALTAZAR JR., J. P; LIMA, L. F (org.). *Cooperação jurídica internacional em matéria penal.* 1 ed. Porto Alegre: Verbo Jurídico, 2010, p. 354.

utilizando-se os dispositivos do próprio tratado, complementados pelos institutos do direito processual interno[76].

Quanto às espécies de medidas previstas no MLAT, o art. 1º, § 2º, do tratado não traz um rol taxativos das diligências cabíveis. Em regra, quaisquer medidas de comunicação processual, de instrução probatória ou de procedimentos cautelares – exceto extradição e transferência de condenados – podem ser executadas com base nesse tratado[77]. Com efeito, a alínea "h" do referido dispositivo estabelece que é permitido "qualquer outra forma de assistência não proibida pelas leis do Estado requerido".

O art. 4º do tratado estabelece, quanto aos requisitos formais do pedido, que as solicitações devem ser apresentadas por escrito, no idioma do Estado requerido, com a assinatura e identificação da autoridade encarregada da persecução criminal no Estado requerente, sob pena de ter a admissibilidade barrada pela respectiva autoridade central.

Ainda, a autoridade interessada deverá descrever a natureza da investigação ou processo, apontando a infração criminal que determinou a persecução. O pedido deverá conter descrição das provas ou informações já colhidas e indicação da finalidade dos elementos probatórios almejados[78].

Elaborado o pedido de cooperação pela autoridade brasileira interessada, ele é enviado ao DRCI/MJ, autoridade central brasileira, que fará um exame inicial de admissibilidade e tramitará a solicitação à autoridade central americana. Este órgão, então, só remeterá o pedido às autoridades americanas competentes se considerar cumpridos os requisitos para auxílio, como a indicação do *probable cause*, explicado detalhadamente no tópico a seguir.

Dessa forma, o Departamento de Justiça americano encaminhará o pedido a um juízo federal, que, após a aferição do cumprimento dos requisitos legais, expedirá mandado de busca e apreensão, determinando ao provedor de aplicação de Internet a disponibilização imediata do conteúdo de comunicações. As informações colhidas, então, terão que percorrer novamente todo o caminho explanado até chegarem ao autor da solicitação de auxílio internacional

[76] BALTAZAR JR., J. P; LIMA, L. F (org.). *Cooperação jurídica internacional em matéria penal.* 1 ed. Porto Alegre: Verbo Jurídico, 2010, p. 356.
[77] Ibid., p. 375.
[78] Ibid., p. 364.

(empresa - juiz americano - autoridade central dos EUA - autoridade central do Brasil - autoridade brasileira que requisitou pedido inicialmente)[79].

Finalizada a explicação da estrutura jurídica do MLAT e de como é sua tramitação, faz-se necessária a análise do funcionamento do tratado na prática, para que possa ser medida a efetiva contribuição e utilidade do mecanismo para a coleta de dados eletrônicos armazenados no exterior.

3.2 A ineficiência do MLAT em dados

Conforme analisado anteriormente, os pedidos de cooperação jurídica internacional em matéria penal podem versar as mais variadas diligências processuais, tais como citações, notificações, interrogatórios de investigados ou réus, oitivas de testemunhas, acesso a informações bancárias, telemáticas, telefônicas, medidas de busca e apreensão e até mesmo o bloqueio de ativos no exterior.

Assim, para esclarecer a realidade acerca do funcionamento do MLAT entre Brasil e EUA, foram colacionados a seguir diversos dados juntados aos autos da ADC nº 51 por ofício[80] do DRCI/MJ, autoridade central da cooperação internacional no país, no que tange aos pedidos de quebra de sigilo telemático e de obtenção de dados eletrônicos enviados aos Estados Unidos.

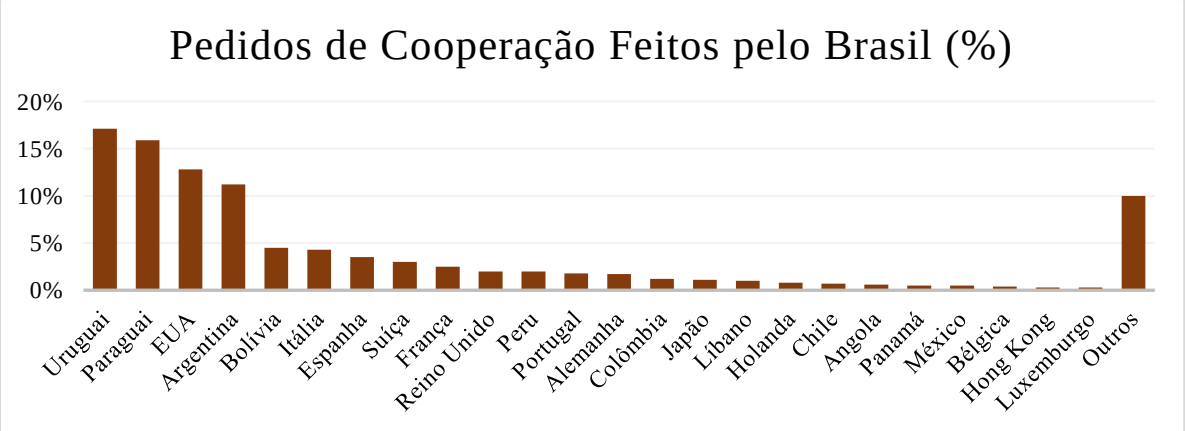
Isto é, os pedidos em análise a seguir representam apenas aqueles enviados do Brasil aos EUA, através do MLAT, em que se pretendiam a obtenção de dados eletrônicos lá armazenados para fins de investigação ou instrução penal.

Inicialmente, considerando todos os pedidos de cooperação jurídica internacional em matéria penal feitos pelo Brasil, verifica-se que os Estados Unidos são um dos principais parceiros do Brasil. Em 2017, foi o 3º país mais demandado pelo Brasil, com cerca de 12% de todos os pedidos totais, ficando atrás apenas do Uruguai e do Paraguai, conforme gráfico abaixo (todos os gráficos foram elaborados especificamente para este trabalho).

---

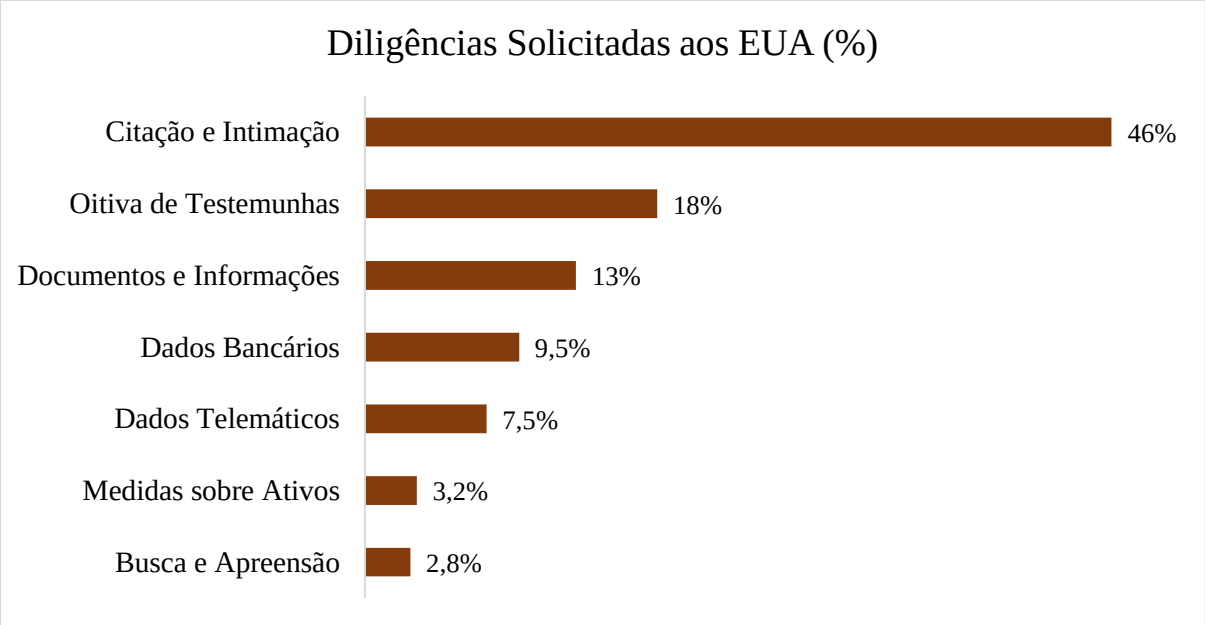
[79] BALTAZAR JR., J. P; LIMA, L. F (org.). *Cooperação jurídica internacional em matéria penal*. 1 ed. Porto Alegre: Verbo Jurídico, 2010, p 369-372.

[80] Petição de apresentação de manifestação nº 10.426/2018, juntado aos autos da ADC nº 51 do STF. Disponível em: <https://www.dropbox.com/s/jhzoho0ddufigv0/Of%C3%ADcio%20DRCI.pdf?dl=0>. Acesso em: 15/05/2018.

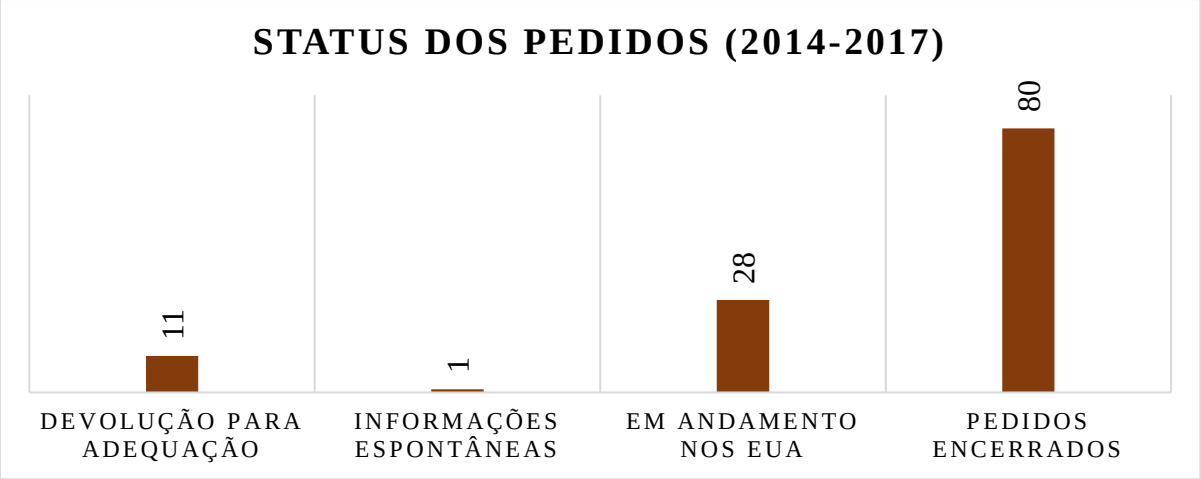


De todos os pedidos encaminhados aos EUA, cerca de 97% são baseados juridicamente no MLAT entre os dois países. Assim, é possível afirmar que este tipo de tratado é o acordo bilateral mais utilizado pelo Brasil em suas demandas em matéria penal no exterior, tendo em vista que dentre outros países mais demandados (Uruguai e Paraguai), os pedidos são fundamentados em acordos multilaterais (Mercosul).

Em relação às diligências solicitadas aos Estados Unidos com base no MLAT, aproximadamente 7,5% dos pedidos de cooperação jurídica dizem respeito a pedidos de obtenção de dados eletrônicos armazenados naquele país, como se observa a seguir.



Considerando a amostragem dos dados restrita aos pedidos encaminhados aos EUA, que buscavam a quebra do sigilo e obtenção de dados eletrônicos, do início de 2014 até o fim de 2017, é possível relatar a existência aproximada de 120 solicitações, que possuem os andamentos retratados no gráfico a seguir.



Conforme se observa acima, dos 120 pedidos, 11 não chegaram sequer a ser enviados aos EUA pelo DRCI/MJ, porque continham falhas graves de elaboração e necessitavam adequação. Por isso, após juízo de admissibilidade administrativo da autoridade central brasileira, foram devolvidas às respectivas autoridades demandantes para correção.

O DRCI/MJ, antes de enviar pedidos sem qualquer chance de atendimento aos Estados Unidos, alerta a autoridade requerente a respeito dos aspectos gerais de admissibilidade do pedido alhures, em especial quanto a melhoria da explicação sobre o nexo causal entre a diligência solicitada, os crimes praticados e os suspeitos (o que é denominado pela legislação americana de *probable cause*, requisito fortemente exigido).

Uma das solicitações não tratava propriamente de pedido de cooperação jurídica, mas de transmissão de informações espontâneas aos EUA, ficando a critério das autoridades do país verificarem se têm ou não interesse em adotar providências cabíveis de investigação.

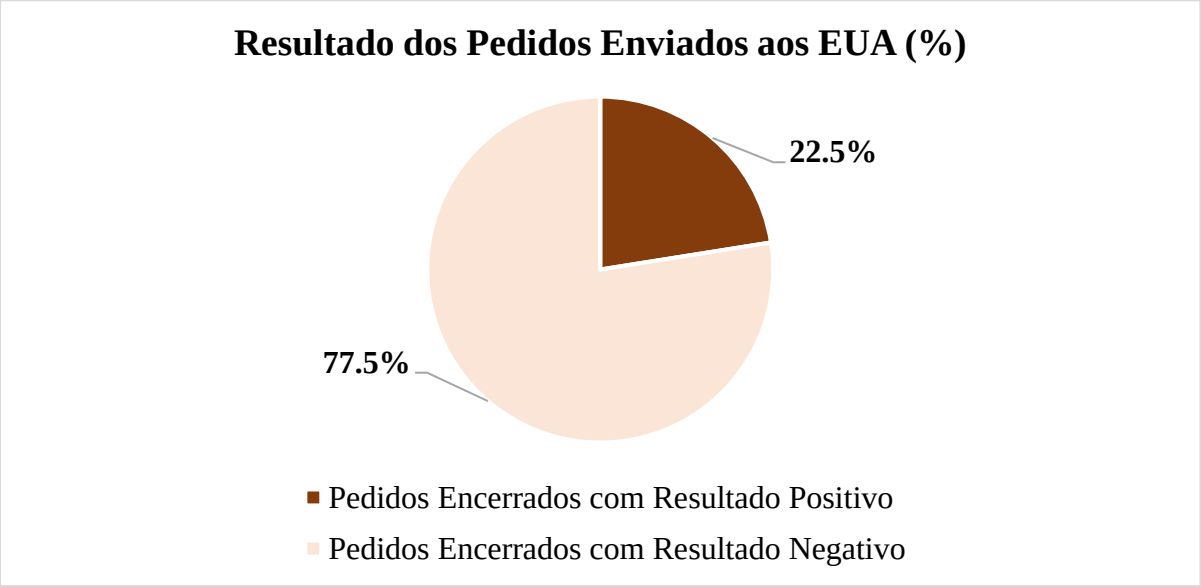
Assim, em relação aos 108 pedidos restantes de cooperação propriamente dita efetivamente remetidos aos EUA, 28 ainda estavam em andamento no país no final de 2017 (quando a pesquisa foi elaborada). Em outras palavras, o Brasil ainda não recebeu resposta conclusiva nesses casos, não se sabendo se as diligências requeridas foram cumpridas ou indeferidas pelas autoridades americanas.

Dentro desses 28 pedidos pendentes, 8 foram enviados no ano de 2014, outros 8 em 2015, 5 em 2016, e 7 em 2017. Assim, percebe-se que há pedidos que se encontram em

andamento há muito tempo[81], o que demonstra certa dificuldade na obtenção de informações céleres sobre dados eletrônicos nos EUA através do mecanismo do MLAT.

Ainda conforme o gráfico acima, em relação aos 108 pedidos de cooperação jurídica propriamente ditos remetidos aos Estados Unidos, 80 deles já foram encerrados pelo DRCI/MJ, seja porque houve resposta positiva ou negativa dos EUA, ou pela desistência da execução dos pedidos pelas próprias autoridades requerentes.

Desses 80 pedidos de cooperação jurídica em matéria penal enviados aos EUA e que foram encerrados, apenas em 18 deles as diligências foram atendidas pelas autoridades americanas, de modo que o índice de aproveitamento é de apenas 22,5% dos pedidos já concluídos, como se observa no gráfico.



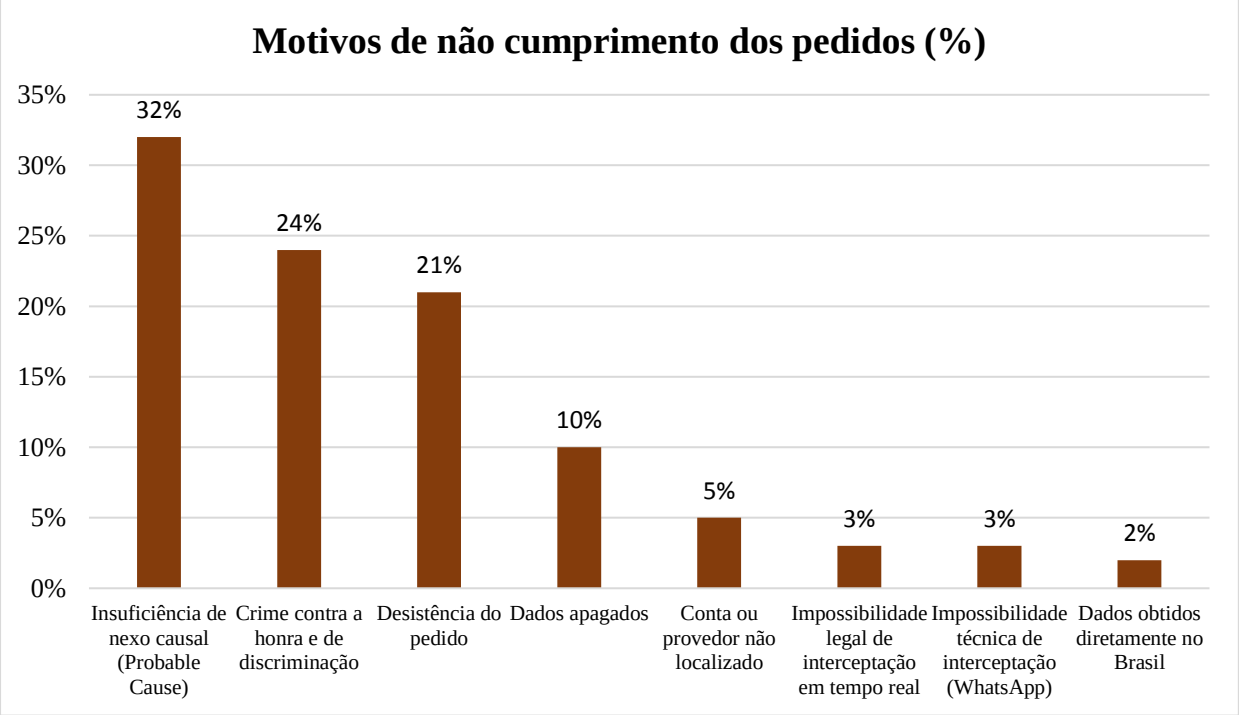
Com efeito, nos outros 62 casos não houve resultados positivos, sendo que em 49 deles houve resposta negativa pelas autoridades dos EUA; e em 13 deles as próprias autoridades nacionais desistiram da execução e perderam o interesse nas diligências, em geral pela demora ou outro fator processual que gerou a perda da oportunidade para uso da evidência solicitada.

Fato curioso é que para as demais diligências solicitadas aos EUA, que não a coleta de dados eletrônicos lá armazenados, o índice de conclusão positiva é inverso, resultando em cerca de 70% dos pedidos cumpridos. Isso evidencia o baixo índice de efetividade dos pedidos de assistência jurídica enviados aos EUA para os fins aqui estudados.

[81] Em alguns desses casos, o grande alongamento desse prazo também se dá pela demora de autoridades brasileiras requerentes que, após receberem pedido de esclarecimentos adicionais dos EUA, não as encaminham de volta com celeridade, contribuindo para o atraso.

Dessa forma, percebe-se que o MLAT em vigor entre o Brasil e os EUA se mostra efetivo para as diligências em geral, com cerca de 70% de cumprimento dos pedidos de cooperação enviados, índice considerado muito bom em comparação com outros países. Por outro lado, para os pedidos destinados à obtenção de dados telemáticos naqueles país, o índice de 22,5% é considerado insatisfatório.

Em relação aos pedidos encerrados de coleta de dados eletrônicos feitos aos EUA entre 2014 e 2017, a grande quantidade de respostas negativas (cerca de 77,5%) tem causas de ordem jurídica e procedimental, como disposto no gráfico a seguir.



Inicialmente, é possível observar que a maior barreira para o cumprimento dos pedidos é jurídica. 32% das requisições foram recusadas por argumentos de insuficiência de nexo causal, ou seja, o não atendimento ao *probable cause* previsto no *Stored Communications Act*, legislação americana que estipula a quantidade suficiente de indícios capazes de autorizar a quebra do sigilo telemático pelas autoridades americanas.

Na maioria dos casos, as solicitações de auxílio jurídico não são cumpridas pelas autoridades requeridas sob argumento de que não há demonstração suficiente do nexo causal entre as medidas solicitadas, as pessoas envolvidas e os crimes praticados, com a alegada necessidade de afastar o sigilo de e-mail, perfil de rede social ou qualquer outro serviço de Internet utilizado.

Assim, o motivo de não cumprimento em análise está afeto a questões jurídicas, na medida em que as autoridades brasileiras necessitam prestar informações suficientes que, sob o ponto de vista da lei americana, demonstrem satisfatoriamente o vínculo da prática criminosa no Brasil com a efetiva utilização de serviços de Internet dos EUA. Esses indícios robustos e imprescindíveis para justificar a quebra do sigilo telemático são fruto da rigorosa lei americana e, somente quando devidamente demonstrados, viabilizam a obtenção do *warrant*[82] autorizativo no país.

Com efeito, não basta às autoridades apenas indicar que determinada pessoa está sendo investigada pela prática de algum crime e que essa mesma pessoa possui conta em um serviço de e-mail ou rede social cujo provedor seja dos Estados Unidos. É preciso fornecer indícios que efetivamente permitam deduzir que o referido e-mail ou rede social é ou foi de fato utilizado para o cometimento ou planejamento do crime.

Consequentemente, é comum que as autoridades brasileiras não possuam as informações necessárias e suficientes para a demonstração do *probable cause*. O elevado nível de nexo causal exigido pela lei americana acaba, muitas vezes, inviabilizando por completo o próprio pedido de cooperação jurídica internacional.

Ocorre também que o próprio conceito de *probable cause* não é muito claro. A Suprema Corte dos Estados Unidos, no caso *Brinegar v. United States*, definiu o requisito legal como "onde os fatos e circunstâncias dentro do conhecimento dos policiais, e dos quais eles têm informações razoavelmente confiáveis, são suficientes, por si só, para garantirem uma crença de uma pessoa de cautela razoável que um crime está sendo ou foi cometido[83]".

Isso demonstra como o conceito de *probable cause* é confuso e indeterminado, de modo que é natural que as autoridades brasileiras tenham dificuldade em atendê-lo. A situação, então, representa a maior causa de não cumprimento dos pedidos de auxílio que objetivam a coleta de dados eletrônicos armazenados nos EUA[84].

---

[82] O *warrant*, no ordenamento jurídico americano, permite acesso a informações e pertences pessoais, após obtenção de um alto standard exigido pela lei, como o probable cause. O *subpoena*, a título de contraste, é feito para requerer ação de quem o recebe, geralmente para compelir pessoa ou entidade a produzirem documentos para fins de evidências. Pode ser feita pelos próprios advogados, desde que forneçam os documentos exigidos e sigam o correto procedimento legal, de modo que é menos rígido e mais fácil de obter que o *warrant*.

[83] U.S. Supreme Court. Brinegar v. United States, 338 U.S. 160 (1949).

[84] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Desafios da coleta de evidências digitais e a cooperação internacional para acesso a dados. 2017. (1h04m). Disponível em: <https://www.youtube.com/watch?v=mNGspCMf8Ag>. Acesso em: 09/05/2018.

No mais, em 24% dos casos, as autoridades americanas não cumprem as solicitações de quebra de sigilo telemático para fins de investigações brasileiras de crimes contra a honra – calúnia, injúria e difamação – e crimes de discriminação previstos na legislação penal brasileira. Isso porque a Primeira Emenda da Constituição dos Estados Unidos dá grande amplitude à liberdade de expressão, de modo que tais condutas não compreendem atos criminosos no país.

São situações em que, por exemplo, o Delegado de Polícia, com objetivo de descobrir a autoria delitiva de crimes contra a honra cometidos através das redes sociais, por usuários que não indicam sua verdadeira identidade, necessita obter informações sobre o cadastro de usuário dos ofensores, ou até mesmo o conteúdo das conversas por onde os ilícitos foram cometidos.

As autoridades americanas, quando recebem solicitação que versam esses tipos de delito, sequer adotam providências para tentar obter as diligências requeridas. Assim, o pedido é restituído às autoridades brasileiras sob argumento da falta de dupla incriminação, pois nos EUA os atos atentatórios contra a honra devem ser resolvidos apenas na esfera cível, com ações destinadas ao pleito de indenizações se o ofendido assim desejar[85].

Dessa forma, há uma verdadeira impossibilidade jurídica de atendimento ao pedido, uma vez que a autoridade central dos EUA para cooperação internacional em matéria penal denega tais solicitações com base jurídica no art. 3º, item 1, "b", do MLAT, que autoriza a recusa em caso de o auxílio provocar possíveis prejuízos aos interesses essenciais de um dos países.

Ainda, 3% dos pedidos foram recusados por solicitarem a interceptação telemática em tempo real, medida que é vedada pela legislação americana, quando requerida exclusivamente por autoridades estrangeiras.

A interceptação telemática em tempo real, também denominada de "grampo", permite a obtenção de informações de algum serviço de Internet no mesmo instante que ocorrem, como a troca de mensagens por e-mail, chats ou outro meio de comunicação. Para esse tipo específico de diligência, a legislação americana é extremamente restritiva, não permitindo a interceptação

[85] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Desafios da coleta de evidências digitais e a cooperação internacional para acesso a dados. 2017. (1h04m). Disponível em: <https://www.youtube.com/watch?v=mNGspCMf8Ag>. Acesso em: 09/05/2018.

em tempo real de comunicações dentro do seu território a pedido de uma autoridade de investigação estrangeira.

Com efeito, a interceptação em tempo real só pode ser utilizada nos EUA na investigação de crimes específicos, deve ser solicitada por funcionários devidamente autorizados dentro do Departamento de Justiça americano, e ainda depende de autorização de juiz competente, após a confirmação de que todos os requisitos legais foram satisfeitos. Dessa forma, o "grampo" só poderia ser implementado em casos de investigações conjuntas entre autoridades competentes de um país estrangeiro e uma agência de investigação dos EUA.

Portanto, caso uma autoridade brasileira responsável pela investigação criminal de tráfico de drogas, por exemplo, perceba que os integrantes da organização criminosa comunicam entre si com frequência por e-mails, cujas mensagens são armazenadas em provedores dos EUA, não obterá uma resposta positiva das autoridades americanas se requisitar o monitoramento em tempo real.

Entretanto, às autoridades investigativas brasileiras resta solicitar a quebra do sigilo telemático e a entrega do conteúdo das mensagens armazenadas, enviadas e recebidas em momento anterior, através do MLAT, com atenção aos requisitos de *probable cause* mencionados anteriormente.

Superados as causas de não cumprimento dos pedidos de cunho jurídico, há também os motivos procedimentais, ou seja, aspectos relacionados ao tempo delongado e outros fatores de ordem prática.

Em 21% dos casos já encerrados, houve a desistência do pedido pelos próprios requerentes no Brasil. Isso porque a demora das autoridades americanas em atender a demanda, além das constantes solicitações de esclarecimentos adicionais para atender a exigência do *probable cause*, acarretam na perda da utilidade da informação ou da evidência probatória solicitada, e na consequente perda de interesse pelas autoridades brasileiras.

No mais, em 10% dos casos, os dados telemáticos almejados já tinham sido apagados, em razão de já ter sido ultrapassado o prazo legal que as empresas provedoras de serviços de Internet têm para mantê-los armazenados.

Em 5% dos casos de recusa, a conta do investigado na plataforma digital ou o próprio provedor de serviços eletrônicos não foram localizados.

3% dos casos de não cumprimento da diligência pelas autoridades americanas se dão por se tratarem de solicitações de quebra de sigilo de informações do aplicativo WhatsApp, no qual a empresa que controla o serviço alega não possuir o mecanismo técnico para acessar tais dados, em razão da tecnologia de criptografia ponta-a-ponta.

Por fim, 2% das recusas foram causadas em virtude de as informações requeridas já terem sido obtidas através da requisição direta das autoridades brasileiras à filial do provedor do serviço no Brasil.

Terminada a análise dos casos em que o pedido foi encerrado sem o cumprimento da diligência requerida, passa-se ao exame dos poucos casos que foram concluídos com resultado positivo.

Dentro dos 18 pedidos nos quais as autoridades americanas atenderam as diligências solicitadas, que representam apenas 22,5% de todos os casos concluídos, em 9 deles foram solicitados apenas dados de conexão e cadastrais, como dados de IP, logins de acesso e registros de uso do serviço de Internet em geral. Conforme analisado ao longo do trabalho, esses tipos de dado recebem menos proteção jurídica do que conteúdo das comunicações e não dependem da reserva de juiz estipulada pelo *SCA* para serem obtidas nos EUA, o que torna o cumprimento da diligência mais fácil.

Apenas nos outros 9 pedidos cumpridos foram solicitadas informações sobre o conteúdo propriamente dito de contas e de comunicações de e-mails ou perfis em rede sociais na Internet, como mensagens enviadas e recebidas, fotos, chats etc. Segundo a estatística do DRCI/MJ, os pedidos dessa natureza foram atendidos, via MLAT, apenas pelas empresas Google Inc. (5 pedidos), Microsoft Inc. (2 pedidos) e Facebook Inc. (2 pedidos), não havendo registros de solicitações de informações de conteúdo que tenham sido atendidos por outras empresas no EUA.

Considerando esses poucos pedidos atendidos via MLAT, cabe menção ao tempo transcorrido para que as autoridades americanas pudessem atendê-los.

Nesse ponto, em relação às solicitações de coleta de dados eletrônicos armazenados nos EUA, informa o DRCI/MJ que o prazo médio para o efetivo cumprimento das diligências pelas autoridades dos EUA é de aproximadamente 13 meses. Tal prazo médio é consideravelmente maior que o estipulado para o cumprimento de pedidos de cooperação internacional destinados a outros tipos de diligência, que é de aproximadamente 8,5 meses.

A autoridade central brasileira aponta que leva apenas 4 dias, em média, para analisar e tramitar as solicitações de cooperação jurídica requeridas pelas autoridades brasileiras, de modo que a demora exagerada nesses casos se dá, preponderantemente, pelo procedimento rigoroso e burocrático que a lei americana estabelece e pela forma que as autoridades do país tratam os pedidos de auxílio.

Conforme explicado, os pedidos, em geral, não são cumpridos de imediato, sendo frequentemente necessário que as autoridades brasileiras formulem esclarecimentos adicionais a pedido dos americanos, a fim de que se atinja o requisito do *probable cause* exigido pelo *SCA*. Apenas com o cumprimento dessa condição, o pedido pode ser remetido a juiz competente para o deferimento do auxílio.

Com base no estudo dos casos através dos anos, o DRCI/MJ aponta que o baixo índice de efetividade não é causado propriamente pelas autoridades americanas ou por dificuldade nas comunicações entre os dois países, tampouco pelo funcionamento do MLAT ou pela forma que o tratado foi redigido.

O problema maior que se verifica, segundo a autoridade central brasileira, é o excessivo rigor e limitação impostos pela legislação dos Estados Unidos, uma vez que todo pedido de cooperação jurídica deve ser cumprido de acordo com as leis do país requerido.

Com efeito, conforme se extrai dos dados apresentados, cerca de 59% das negativas são causadas por exigências jurídicas da lei americana para atendimento, em especial, do *probable cause*. O referido rigor é muito protetivo e, muitas vezes, acaba inviabilizando o cumprimento do pedido de auxílio por completo.

Ademais, mesmo nos casos em que são obtidas respostas positivas, o prazo médio de atendimento de 13 meses é considerado insatisfatório, tendo em vista que os pedidos de cooperação via MLAT para fins de obtenção de dados e quebra de sigilo telemático nos EUA são, por natureza, quase sempre urgentes.

De fato, diversamente de outras diligências de investigação, a quebra de sigilo telemático (assim como o sigilo telefônico e outras formas de monitoramento de comunicações) muitas vezes se destina à obtenção de informações acerca de crimes que ainda não ocorreram, para que seja possível, por exemplo, compreender o funcionamento de determinada organização criminosa.

Desse modo, a coleta dos dados eletrônicos pode ser essencial para o próprio desenvolvimento e direcionamento da investigação, de forma que o largo prazo para a resposta positiva até então observada denotam a insatisfação com o mecanismo de auxílio internacional em estudo.

Concluída a análise dos dados fornecidos pelo DRCI/MJ, fica claro que o uso do MLAT para a obtenção de dados eletrônicos armazenados nos EUA tem se mostrado ser ferramenta extremamente defasada e ineficiente, tendo em vista que apenas 22,5% dos pedidos já concluídos tiveram resposta positiva das autoridades americanas.

Chapelle e Fehlinger resumem os obstáculos estruturais enfrentados na implementação dos MLATs, nos diversos países, dentre problemas de celeridade, escopo, assimetria e escalabilidade[86].

Quanto à celeridade, os MLATs são mal adaptados à velocidade trazida pela Internet e à capacidade viral de disseminação da informação. Os seus intrincados mecanismos de validação, apesar de buscarem promover garantias processuais robustas, acabam tornando o sistema impraticável.

Em relação ao escopo, os MLATs são frequentemente limitados à exigência de que o ato, objeto de cooperação, seja ilícito na legislação dos dois países envolvidos. Assim, a relevância dos MLATs acaba sendo reduzida devido à disparidade de legislações nacionais, principalmente em questões sobre liberdade de expressão nos casos de discurso de ódio e crimes contra a honra.

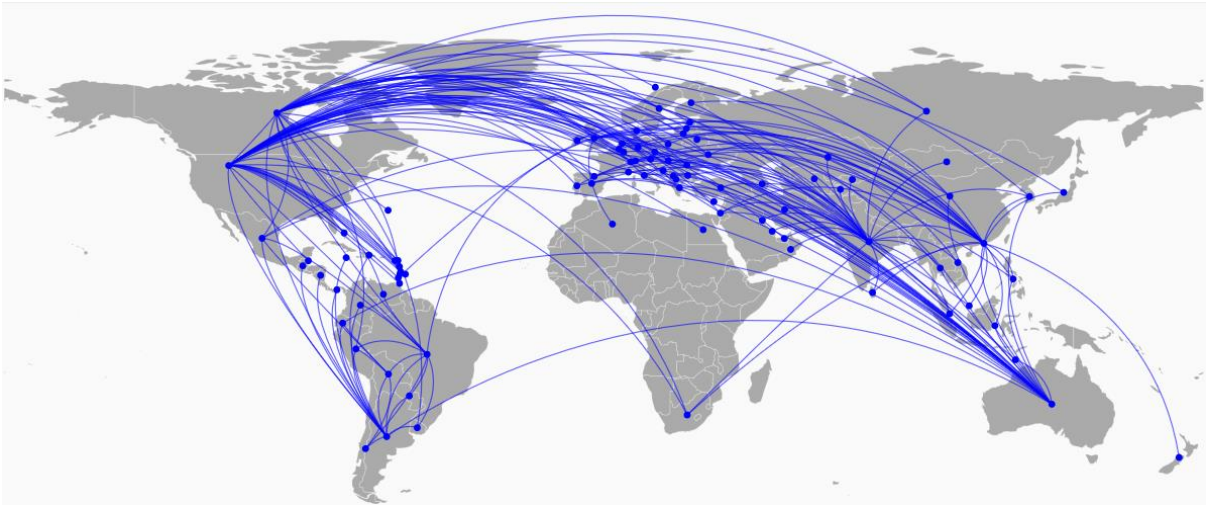
Quanto à assimetria, os MLATs impõem o sistema jurídico do país que recebe o pedido de cooperação, em detrimento daquele que faz o pedido, mesmo que não haja nenhuma conexão territorial do crime com o país requisitado, além da sede do provedor do serviço de Internet. Assim, esses acordos acabam desconsiderando o local de ocorrência do ilícito, ou mesmo a nacionalidade das partes envolvidas.

Por fim, acerca da escalabilidade, o sistema tradicional de MLATs dificilmente consegue abarcar a escala da Internet. Muitos países não firmaram esses acordos de cooperação e estabelecer relações bilaterais entre 190 países iria requerer mais de 15.000 acordos.

---

[86] LA CHAPELLE, Bertrand de; FEHLINGER, Paul. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. 2016. p. 12-13. Disponível em: <https://goo.gl/qAisYB>. Acesso em: 07/06/2018.

Nesse ponto, observa-se a seguir mapa com todos os acordos MLAT entre os países, conforme mapa interativo da ONG internacional Access Now[87].



Assim, como o julgamento da ADC nº 51 pelo STF provavelmente não será suficiente para solucionar o problema, além da expressiva ineficiência do MLAT como mecanismo de cooperação jurídica internacional em matéria penal, é necessário buscar outras alternativas para viabilizar a coleta de dados no exterior.

Portanto, passa-se à análise de outras técnicas de coleta de dados eletrônicos no exterior para viabilizar a investigação ou instrução criminal.

[87] Para os acordos específicos entre cada país, ver: <https://www.mlat.info/>. Acesso em: 05/06/2018.

4. ALTERNATIVAS E SOLUÇÕES PARA A COLETA DE DADOS ELETRÔNICOS NO EXTERIOR

4.1 O *CLOUD Act* e a reforma do *Stored Communications Act*

O caso *United States v. Microsoft Corporation*, da Suprema Corte americana, tinha como questão principal saber se um mandado judicial emitido com base nas normas do *Stored Communications Act* seria capaz de obrigar as empresas dos EUA a fornecerem informações sob seu controle, mas armazenadas fora do país em unidades de guarda e processamento de dados (data centers).

A disputa se iniciou em 2013 quando um juiz federal de Nova York concedeu um mandado, com base no Parágrafo 2703[88] do *SCA*, para que as autoridades de investigação obtivessem os conteúdos de e-mails e dados associados de um usuário da Microsoft suspeito da prática do crime de tráfico de drogas.

Após essa decisão, a empresa forneceu somente os metadados relativos à conta do usuário, pelo fato de estarem armazenados nos EUA. Contudo, alegou que não poderia fornecer o conteúdo dos e-mails, pois essas informações estavam localizadas em um servidor na Irlanda e as normas do *SCA* não teriam aplicação extraterritorial.

A recusa da Microsoft em fornecer o conteúdo dos e-mails não foi aceita pelo tribunal de primeira instância, que condenou a empresa por desobediência a uma ordem judicial (*civil contempt*)[89]. Após recurso ao Tribunal de Apelações para o Segundo Circuito, foi dado provimento ao pleito, sob argumentação de que o *SCA* era silente quanto ao seu alcance extraterritorial, devendo ser interpretado restritivamente. Além disso, o tribunal considerou que

---

[88] 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. Disponível em: <https://goo.gl/ojNv2A>. Acesso em: 02/06/2018.

[89] "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. Disponível em: <https:// goo.gl/7YrorZ>. Acesso em: 02/06/2018.

o elemento territorial para determinar o alcance do mandado seria o local onde os dados requisitados estavam armazenados, de modo que um mandado emitido nos EUA para coleta de dados na Irlanda culminaria na aplicação extraterritorial da lei americana[90].

Após o julgamento de segunda instância, o Departamento de Justiça dos Estados Unidos questionou a interpretação dada ao *SCA* mediante interposição de recurso à Suprema Corte, que aceitou o caso em outubro de 2017.

O órgão governamental defende que a quebra do sigilo e a divulgação de informações eletrônicas em questão ocorre em território americano, e o acesso ao servidor localizado em outro país configuraria mera conduta acessória. Ainda, acrescenta que a Microsoft poderia cumprir com o mandado por meio de ações que acontecem exclusivamente nos EUA, através de seus *softwares* de gerenciamento de dados[91].

Além disso, sustenta que a empresa não agiria como agente governamental, visto que não apreenderia dados armazenados em jurisdição estrangeira, mas apenas teria acesso a uma informação armazenada em seus próprios arquivos. Assim, argumenta que como a localização dos dados é de escolha exclusiva da empresa, uma decisão de viés econômico poderia inutilizar as previsões do *SCA*.

Por fim, defende que os mecanismos de cooperação jurídica internacional estabelecidos em acordos e tratados de assistência jurídica mútua (MLATs) não seriam uma alternativa efetiva. Isso porque esses acordos não são universais, tendo os EUA assinado essa modalidade de instrumento internacional com menos da metade dos países do mundo e porque o procedimento, na maioria dos casos, é lento e de cumprimento incerto.

Por outro lado, a Microsoft argumenta que a jurisprudência da Suprema Corte[92] é no sentido de que as leis federais americanas devem ser interpretadas de forma restritiva, caso não seja explícita sua aplicação extraterritorial. Ainda, aduz que o critério adotado pelo *SCA* é o do local de armazenamento dos dados, e não do local onde ocorrerá o ato de divulgação e quebra do sigilo dos dados pelas autoridades. Nesse ponto, a conduta relevante sob o prisma da lei

---

[90] 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. Disponível em: https://goo. gl/Kz7hWp. Acesso em: 02/06/2018.

[91] United States of America, Petitioner v. MICROSOFT CORPORATION, Respondent. Brief for the United States - Nº 17-2. Disponível em: <https://goo.gl/X5kVUj>. Acesso em: 02/06/2018.

[92] Supreme Court of the United States. MORRISON et al. v. NATIONAL AUSTRALIA BANK LTD. et al. 561 U.S. 247 (2010).

seria o ato de apreensão das comunicações, que ocorre justamente sob a jurisdição onde o servidor está localizado[93].

Cabe salientar que tanto os representantes do governo quanto os da Microsoft concordaram, na audiência reservada para sustentações orais na Suprema Corte, que faria mais sentido que o Poder Legislativo adotasse soluções para o caso, em detrimento dos remédios jurisdicionais disponíveis, tendo em vista o projeto de lei que já estava em andamento na época[94].

O caso da Suprema Corte, contudo, não será julgado. Tornou-se prejudicado após a promulgação do *Clarifying Overseas Use of Data Act*, apresentado em fevereiro de 2018 por senadores democratas e republicanos[95].

O *CLOUD Act*, como também ficou conhecido, foi aprovado celeremente pelo Congresso em 23/03/2018 e assinado pelo presidente Donald Trump no mesmo dia. A lei lida com duas questões principais: o acesso a dados armazenados no exterior pelas autoridades americanas; e as condições através das quais outros países podem requisitar dados de empresas sediadas nos EUA.

Em relação à primeira questão, a lei adiciona uma seção[96] ao *Stored Communications Act* para estabelecer que um provedor americano de comunicações eletrônicas ou serviço de computação remota tem a obrigação de fornecer os dados armazenados sob sua posse, custódia ou controle, independentemente de onde os dados estiverem armazenados.

Essa provisão reflete a posição do Departamento de Justiça dos EUA e codifica o entendimento adotado no caso United States v. The Bank of New Scotia[97], que autoriza *subpoenas* para compelir um banco a apresentar documentos armazenados no exterior, desde que estejam sob posse, custódia ou controle do banco.

A lei também cria mecanismos para que as empresas possam contestar os mandados judiciais das autoridades americanas, caso o alvo da quebra de sigilo não seja um cidadão dos

---

[93] UNITED STATES OF AMERICA, Petitioner v. MICROSOFT CORPORATION, Respondent. Brief in Opposition. 2017. Disponível em: https://goo.gl/pnz1Wo>. Acesso em: 02/06/2018.
[94] UNITED STATES, Petitioner, v. MICROSOFT CORPORATION, Respondent. Nº. 17-2. Oral argument before the Supreme Court of the United States.27/02/2018. Disponível em: <https://goo.gl/aDrz8q>. Acesso em: 02/06/2018.
[95] 115th CONGRESS - THE SENATE OF THE UNITED STATES. S.2383/H.R. 4943. The Clarifying Overseas Use of Data (CLOUD ACT). 2018. Disponível em: <https://goo.gl/4gn81j>. Acesso em: 02/06/2018.
[96] Section 18 U.S.C. §2713.
[97] Supreme Court of the United States. UNITED STATES v. THE BANK OF NEW SCOTIA, 462 US 1119 (1983).

Estados Unidos ou caso haja risco relevante de a determinação judicial violar as leis do país em que os dados estiverem armazenados. Adicionalmente, o *CLOUD Act* busca reforçar mecanismo já existente no ordenamento jurídico, denominado *comity analysis*, segundo o qual os tribunais devem medir se os interesses buscados com a aplicação de ato ou decisão extraterritorial justificam os impactos na soberania e na relação entre os países[98].

Já em relação à segunda questão, quanto aos pedidos de quebra de sigilo e entrega de dados telemáticos feitos por entidades governamentais estrangeiras, a lei busca facilitar a cooperação jurídica internacional.

Conforme explicado, o *SCA* impede que as empresas americanas obedeçam às requisições de entrega de dados de comunicação privada feitas por autoridades judiciárias estrangeiras, quando não há autorização prévia da Justiça americana. A nova lei altera diversas partes do *SCA*, em relação aos dados eletrônicos armazenados e grampos telemáticos, para permitir que os provedores forneçam essas informações diretamente a entidades governamentais estrangeiras – mas apenas àquelas que tiverem firmado acordo executivo com os Estados Unidos.

Esses acordos não estão disponíveis para qualquer país, apenas àqueles que cumprirem uma série de requisitos. Com efeito, o presidente pode apenas firmar esse acordo se o Procurador-Geral, em concorrência com o Secretário de Estado, considerar que: (a) o país estrangeiro tenha garantias processuais e materiais robustas de proteção à privacidade, aos direitos civis de proteção a dados e aos demais direitos humanos de seus cidadãos; (b) o governo estrangeiro tenha adotado procedimentos mínimos de proteção aos dados de cidadãos americanos; e (c) o acordo tenha proteções para prevenir o governo estrangeiro de coletar informações de cidadãos americanos ou de pessoas localizadas nos EUA[99].

Na hipótese de um país se qualificar para o acordo, não seria necessário que todo mandato de quebra de sigilo e entrega de dados de comunicações privadas, emitido por juiz competente, tivesse que passar pelo mecanismo de cooperação previsto no MLAT, podendo ser cumprido diretamente pela empresa.

---

[98] WOODS, A. K.; SWIRE, P. *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems.* 2018: Lawfare. Disponível em: <https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems>. Acesso em: 02/06/2018.

[99] Para mais detalhes, ver: "'(b) EXECUTIVE AGREEMENT REQUIREMENTS". S.2383/H.R. 4943. The Clarifying Overseas Use of Data Act. p. 13. Disponível em: <https://bit.ly/2G3laqY>. Acesso em: 02/06/2018.

Ainda, os pedidos de governos estrangeiros devem ser relacionados apenas a crimes graves (apesar desse conceito não ser esclarecido na lei); devem prover uma justificação razoável, com base no nexo causal entre os a conduta criminosa do usuário sob investigação e o serviço de comunicação eletrônica; devem ser sujeitas a revisão de autoridade judiciária no país estrangeiro; e não podem ser usados para violar a liberdade de expressão.

Apesar de tentar solucionar o problema da coleta de dados eletrônicos no exterior, o CLOUD Act divide opiniões. Grupos da sociedade civil em defesa dos direitos humanos e de privacidade consideram que a lei dá jurisdição ilimitada às autoridades americanas e aumenta unilateralmente os poderes de investigação sobre quaisquer dados controlados por provedores americanos, independentemente de onde estiverem armazenados, enquanto enfraquece as leis de privacidade dos países estrangeiros[100].

Em relação aos acordos executivos, repudiam o fato da lei criar óbices para obtenção de dados apenas dos cidadãos americanos ou residentes no país, permitindo que as informações de usuários de qualquer outro país do mundo possam ser acessadas pelas entidades governamentais em acordo com os EUA, sem que essas pessoas ao menos tenham conhecimento disso.

Em outras palavras, em razão das companhias de tecnologia americanas armazenarem grande parte das informações de Internet do mundo, um país que firmar um desses acordos com os Estados Unidos tem o potencial de obter dados e até realizar grampos telemáticos em pessoas de qualquer lugar do mundo, desde que o alvo não seja natural ou residente dos EUA.

Para os críticos, isso enfraqueceria consideravelmente os padrões de privacidade, porque os pedidos no âmbito desse acordo devem ser feitos diretamente às empresas, e não são submetidos aos mecanismos de proteção que a legislação americana comumente dá à coleta de dados, como a necessidade de um *warrant* autorizativo ou de notificação ao governo. Assim, argumentam que a lei é falha ao não estabelecer a necessidade de notificação em qualquer nível, seja à pessoa cujos dados são coletados, ao país onde essa pessoa reside e ao país onde os dados são armazenados.

Ainda, sustentam que o CLOUD Act permite que autoridades estrangeiras tenham acesso à interceptação telemática em tempo real sem que sejam observadas as regras

[100] FISCHER, C. *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data.* Eletronic Frontier Foundation: 2018. Disponível em: <https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data>. Acesso em: 06/02/2018.

americanas, explicadas no capítulo anterior. Além disso, apesar de o novo acordo aparentar ser mais célere e menos burocrático, acaba enfraquecendo os mecanismos de assistência mútua (MLATs), que dão proteção às medidas de proteção à privacidade exigidas pela legislação americana, notadamente pela fiscalização do governo no processo e necessidade de autorização judicial.

Por outro lado, há juristas que defendem o CLOUD Act. Para esse grupo, os EUA têm legitimidade para legislar sobre áreas em que percebam efeitos domésticos, conforme a noção enraizada de jurisdição, de modo que as novidades da lei não compreendem em aplicação extraterritorial das normas americanas[101].

Ainda, apesar de aparentemente proteger menos os direitos à privacidade, consideram que a lei evita que governos estrangeiros forcem provedores de serviços a armazenar localmente os dados, para que estejam sujeitos a tal jurisdição em detrimento das normas dos Estados Unidos.

Além disso, argumentam que a lei cria um número considerável de garantias, ao permitir que os provedores de aplicações requeiram a anulação ou modificação do processo se fundamentadamente acreditarem que o usuário sob investigação não é cidadão americano ou que a requerida coleta de dados pode criar um risco material de violação às leis do país onde os servidores estão localizados.

As grandes companhias americanas de tecnologia, que se encontravam no meio do conflito entre leis de privacidade de diferentes países, demonstraram apoio ao CLOUD Act, que legitima a entrega de dados às autoridades americanas independentemente de onde estiverem armazenados[102].

A despeito do debate, é certo que os interessados no Brasil não podem depender das novidades trazidas pelo CLOUD Act para resolver o problema da coleta de dados no exterior. Isso porque, inicialmente, a realização de um acordo Executivo pressupõe elevado grau de discricionariedade dos países envolvidos. Com efeito, não são certos os critérios elencados pela

---

[101] WOODS, A. K.; SWIRE, P. *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems.* 2018: Lawfare. Disponível em: <https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems>. Acesso em: 02/06/2018.

[102] Tech Giants Back U.S. Bill Governing Cross-Border Data Searches. Disponível em: <https://www.bloomberg.com/news/articles/2018-02-07/tech-companies-welcome-cross-border-data-search-legislation>. Acesso em: 02/06/2018.

lei para a habilitação de Estados estrangeiros para o acordo, como o de robusta legislação material e processual de proteção à privacidade.

Em outras palavras, mesmo que juristas brasileiros considerem o Marco Civil da Internet como regulação suficiente para tais fins, ainda incumbe a autoridades americanas (Procurador-Geral e Secretário de Estado) avaliar o nível de proteção à privacidade das normas brasileiras.

Além disso, ainda que o Brasil possua vasta regulamentação de proteção de dados, capaz de cumprir os requisitos do CLOUD Act, a realização do acordo é de cunho inteiramente discricionário dos líderes do Poder Executivo de ambos os países, de modo que não é possível criar qualquer tipo de expectativa ou previsibilidade quanto a isso.

No mais, caso o acordo executivo seja realizado, o pedido a ser enviado pelas autoridades brasileiras às empresas de tecnologia ainda deve observar uma série de requisitos bastante rigorosos, semelhantes aos do MLAT, que provavelmente também vão acabar inviabilizando parte das requisições.

Conclui-se que o CLOUD ACT, apesar das críticas que recebe, pode facilitar o fornecimento de dados armazenados no exterior às autoridades brasileiras, caso o tratado executivo com os Estados Unidos seja feito. Isso porque o modelo desburocratiza os pedidos de coleta de informações ao permitir que sejam feitos diretamente aos provedores de serviços de Internet.

Contudo, não há qualquer elemento que indique que esse acordo será firmado entre os países, devido à sua completa arbitrariedade. Um grande problema pode surgir caso o presidente dos EUA use o CLOUD Act para negociar um acordo apenas com o Reino Unido, deixando alguns dos maiores mercados de tecnologia do mundo de fora, como a Índia e o Brasil[103].

Isso porque, antes mesmo da lei ser aprovada pelo Congresso americano, os Estados Unidos e o Reino Unido já negociavam acordo para permitir que os seus governos tivessem acesso facilitado aos dados armazenados nos respectivos países, pendendo apenas de promulgação do CLOUD Act.

---

[103] WOODS, A. K.; SWIRE, P. *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems.* 2018: Lawfare. Disponível em: <https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems>. Acesso em: 02/06/2018.

Destaca-se que o Reino Unido aprovou em 2016 umas das leis de vigilância mais intrusivas do mundo, o Investigatory Powers Act. A lei, cujo objetivo é combater o terrorismo, amplia consideravelmente os poderes de acesso e coleta de dados das autoridades policiais e das agências de segurança, incluindo a possibilidade do próprio governo *hackear* computadores, redes, servidores e celulares até mesmo fora do país, além de apenas exigir autorização judicial para coleta de espécies limitadas de dados eletrônicos[104].

Em outras palavras, a legislação do Reino Unido parece não atingir os elevados parâmetros de proteção de dados exigidos pelo CLOUD Act para habilitação do país ao acordo executivo[105]. Isso evidencia a arbitrariedade e falta de critérios objetivos do Poder Executivo americano, que deve provavelmente usar seus próprios interesses para recompensar ou punir as nações estrangeiras[106].

Dessa forma, fica claro que o Brasil não pode esperar que o CLOUD Act vá solucionar a controvérsia de imediato e, por enquanto, deve se socorrer a outros meios para efetuar a coleta de dados eletrônicos armazenados no exterior.

4.2 Técnicas controversas de investigação

A inabilidade do sistema internacional de fornecer as soluções necessárias para o problema através de métodos cooperativos incentiva a adoção de técnicas agressivas e de atos unilaterais pelos governos, como busca de um meio mais eficiente para a coleta de dados no exterior. Essas alternativas, que parecem funcionar de imediato, apresentam graves impactos em diversos setores, como na economia, nos direitos humanos, na infraestrutura dos meios eletrônicos e na segurança[107].

Essas maneiras controversas de acesso a dados eletrônicos, tais quais os mecanismos do *backdoor* de aplicações, da proibição de criptografia forte, da política de localização de

---

[104] What is the IP Act and how will it affect you? Disponível em: <http://www.wired.co.uk/article/ip-bill-law-details-passed>. Acesso em: 02/06/2018.
[105] KIM, S.; FIDLER, Mailyn. The Weak Link in a Double Act: U.K. Law is Inadequate for Proposed Cross-Border Data Request Deal. 2017: Lawfare. Disponível em: <https://www.lawfareblog.com/weak-link-double-act-uk-law-inadequate-proposed-cross-border-data-request-deal>. Acesso em: 02/06/2018.
[106] JAYCOX, Mark; e TIEN, Lee. *Reforms Abound for Cross-Border Data Requests*. Electronic Frontier Foundation. 2015. Disponível em: <https://goo.gl/2WJAfV>. Acesso em: 05/06/2018.
[107] LA CHAPELLE, Bertrand de; FEHLINGER, Paul. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. 2016. p. 7. Disponível em: <https://goo.gl/qAisYB>. Acesso em: 07/06/2018.

dados e do Estado agindo como *hacker*, foram extraídos da experiência de diferentes países ao lidar com o problema.

O *backdoor*, ou porta dos fundos, é um mecanismo especial construído artificialmente para satisfazer as necessidades da Justiça, geralmente discutido em conjunto com a criptografia. Trata-se da inserção proposital de uma falha de projeto no protocolo criptográfico para tornar possível a interceptação de mensagens em trânsito ou acesso aos dados armazenados pelo próprio provedor da aplicação[108].

Em outras palavras, corresponde a uma falha no sistema de segurança da aplicação de Internet que permite com que os desenvolvedores acessem o conteúdo que desejarem, em tese após requisição das autoridades investigativas. Um exemplo já analisado neste trabalho é o do caso Apple v. FBI, no qual as autoridades policiais e judiciais queriam que a empresa de tecnologia atualizasse o *software* para criar uma falha no sistema de segurança dos iPhones, protegido com criptografia. Desse modo, objetivavam acessar o celular do investigado sem que os seus dados fossem autodestruídos após a inserção da senha pessoal incorretamente por 10 vezes[109].

Contudo, esse método é falho por diversos motivos. Com efeito, tornaria o trabalho dos desenvolvedores muito mais complexo, visto que além de projetarem do protocolo inicial de segurança das aplicações, teriam que se preocupar também em criar uma exceção para violar os próprios princípios iniciais de segurança.

Além disso, essa falha proposital também precisaria ser protegida. Dentro da empresa, haveria potencial risco de abuso interno, pois os funcionários da empresa de tecnologia teriam acesso a essa porta dos fundos nos seus servidores. Externamente, haveria o sério risco de *hackers* invadirem o sistema da empresa para obterem acesso ao *software* de *backdoor*, o que colocaria os dados de todos os usuários do serviço em risco.

De fato, escolher inserir uma falha de projeto do sistema de segurança das aplicações para permitir que as investigações sejam mais convenientes é tornar os sistemas menos seguros. Não se trata de mecanismo específico para acesso a dados de investigados, como um grampo

---

[108] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Acesso a comunicações eletrônicas e criptografia: garantias, prerrogativas e devido processo legal. 2017. (2h29m). Disponível em: <https://www.youtube.com/watch?v=W_b2Jr9wFXk>. Acesso em: 09/05/2018.

[109] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – O debate americano sobre vigilância e criptografia. 2017. (57m42s). Disponível em: <https://www.youtube.com/watch?v=NuszpDZ69qw>. Acesso em: 09/05/2018.

telemático, mas de uma falha que traria impactos negativos e exposição de dados a todos os usuários da plataforma eletrônica.

Por fim, o mecanismo de *backdoor* criaria uma vulnerabilidade também em relação à harmonização das requisições por diferentes governos. Isso porque os dados de um serviço, como o WhatsApp, ficariam disponíveis a todos os governos com acesso ao mecanismo, de modo que a privacidade de todos os usuários seria posta em risco. Percebe-se, então, que se trata de meio bastante intrusivo e arriscado[110].

A *criminalização da encriptação forte* também surge como esforço de alguns países para limitar o acesso do público à tecnologia forte o suficiente para resistir à decriptação por agências de inteligência do governo.

Destacam-se as guerras criptográficas movidas pelos Estados Unidos, com início na década de 1990, após os primeiros serviços munidos da tecnologia serem oferecidos aos consumidores, e retomados na atual década com o desenvolvimento cada vez maior de serviços e produtos criptografados, em especial o sistema operacional iOS 8 do iPhone[111]. Mais recentemente, há o caso da China, que possui lei aprovada no Congresso determinando que qualquer fabricante de produto ou serviço que contenha criptografia seja capaz de decriptar as comunicações se necessário[112]. Na prática, proíbe-se a encriptação forte.

Com efeito, as técnicas matemáticas conhecidas para desenvolver a criptografia são conhecidas há décadas, de modo que proibir a encriptação é restringir o acesso humano a parte da matemática, à pesquisa acadêmica, à liberdade de programar e ao empreendimento utilizado em proteção da privacidade. Além disso, não é um método muito efetivo, pois todos os usuários do serviço teriam sua segurança significativamente reduzida, ao passo que qualquer célula criminosa minimamente sofisticada encontrará acesso a outras formas criptografadas de comunicação.

---

[110] Nesse ponto, destaca-se a existência de projeto de lei no Congresso americano (*Secure Data Act*), cujo objetivo é proibir qualquer agência governamental ou órgão jurisdicional de forçar companhias a construir *backdoors* em dispositivos e comunicações criptografadas, tendo em vista o recorrente argumento da comunidade de pesquisadores, cientistas e desenvolvedores da área de que não existe *backdoor* seguro. Para mais detalhes, acessar: <https://www.eff.org/deeplinks/2018/05/secure-data-act-would-stop-backdoors>. Acesso em: 30/05/2018.

[111] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – O debate americano sobre vigilância e criptografia. 2017. (57m42s). Disponível em: <https://www.youtube.com/watch?v=NuszpDZ69qw>. Acesso em: 09/05/2018.

[112] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Acesso a comunicações eletrônicas e criptografia: garantias, prerrogativas e devido processo legal. 2017. (2h29m). Disponível em: <https://www.youtube.com/watch?v=W_b2Jr9wFXk>. Acesso em: 09/05/2018.

Em seguida, *a política de localização de dados* é uma imposição legal que obriga os provedores de Internet a armazenarem seus dados no país em que o serviço é prestado. Essa medida tem como objetivo aumentar o controle governamental sobre os dados dos usuários do país e facilitar o acesso pelas autoridades, devido à indiscutível aplicação da jurisdição local.

Conforme já dito, o governo brasileiro tentou implementar provisão que obrigaria os provedores de serviço de Internet a manterem em território nacional servidores com os dados e registros dos usuários do país, mas a medida acabou sendo retirada do texto legal[113]. Isso porque se trata de recurso bastante agressivo do ponto de vista da livre iniciativa, capaz de desestimular o investimento de empresas estrangeiras no Brasil e até inviabilizar a prestação de serviços por empresas menores e *start-ups*, que não teriam como alocar recursos humanos e financeiros suficientes para possuir servidores aqui.

A medida, cujo objetivo é facilitar o acesso das autoridades aos dados em detrimento da livre iniciativa das empresas, não é eficaz, e acabaria prejudicando também os usuários, que teriam menos serviços de tecnologia disponíveis. Essa política também seria muito prejudicial aos países menores e com menor desenvolvimento, que teriam investimento reduzido pelas empresas de tecnologia.

Por fim, outra técnica controversa e invasiva de acesso a dados é por meio de *ataques hackers providenciados pelo próprio governo*. A atividade *hacker* consiste em fazer com que as tecnologias e os sistemas eletrônicos ajam de uma maneira que o desenvolvedor, o dono ou o usuário não gostariam, a fim de que respondam da maneira que o invasor quer. O Estado, ao agir na qualidade de *hacker*, pode infiltrar remotamente dispositivos eletrônicos para copiar, deletar, danificar ou criar dados durante as investigações, de acordo com suas necessidades. O governo pode até criar e disseminar *malwares* capazes de danificar computadores, técnicas perigosas já utilizadas em países como os Reino Unido e nos Estados Unidos[114].

Há países que se esforçam para criar uma base jurídica para tal atividade, capaz de legitimar o modo de coleta de informações e facilitar o procedimento, uma vez que não há intermediários como a empresa provedora do serviço de Internet e governos de outros países onde os dados estão armazenados[115]. A prática hacker também permite ao governo a condução

---

[113] MASSO, F. D.; ABRUSIO, J.; FILHO, M. A. F (coord.). Marco Civil da Internet: Lei 12.965/2014. 2. ed. São Paulo: Editora Revista dos Tribunais, 2014, p. 152.

[114] Government Hacking and Subversion of Digital Security. Disponível: <https://www.eff.org/issues/government-hacking-digital-security>. Acesso em: 02/06/2018.

[115] E quando o Estado vira hacker? Amie Stepanovich no Internet Lab. 2017. (6m28s). Disponível em: <https://www.youtube.com/watch?v=cxbgNKZmdIA>. Acesso em: 02/06/2018.

de novas formas de vigilância em tempo real, ao intencionalmente ligar o microfone, câmera ou GPS do dispositivo da pessoa investigada, por exemplo.

A título ilustrativo, Ahmed Ghappour alerta que invasões de dispositivos informáticos feitas pelas autoridades investigativas americanas em investigações na *dark web* envolvem, em grande parte dos casos, pessoas localizadas em outros países como alvos dos inquéritos. Assim, afirma que essa prática pode também acarretar na maior aplicação extraterritorial da jurisdição dos EUA na história[116].

Essas ferramentas podem ter várias consequências negativas para a segurança e privacidade de usuários que não fizeram nada de errado e nem estão ligados à investigação. Além disso, essas medidas são desproporcionais em relação à ameaça, tendo em vista que causam danos aos dispositivos eletrônicos infectados quando há técnicas de acesso menos invasivas e mais apropriadas.

Com efeito, os governos não podem abrir mão das técnicas de segurança na Internet para permitir o acesso a dados de alguns investigados, pois os custos negativos à sociedade são inúmeros. Acima de tudo, os governos devem promover um ambiente mais seguro de acesso aos usuários inocentes, sem que corram os riscos colaterais da vigilância intrusiva, ao invés de reduzir ainda mais a confiança das pessoas na Internet através das mencionadas técnicas de redução de segurança[117].

Conforme mostrado, tais medidas afetam negativamente: (a) a economia, ao criar barreiras de entrada no mercado, desestimular investimento de empresas estrangeiras no país, frear a inovação e criar obstáculos para o investimento em países em desenvolvimento; (b) os direitos humanos, ao limitar a liberdade de expressão, o acesso à informação e a privacidade dos usuários de Internet; (c) a infraestrutura dos meios eletrônicos, ao criar restrições para o desenvolvimento da tecnologia e da proteção a dados em prol da vigilância; e (d) a segurança, ao criar falhas que põem todos os usuários de Internet em risco e estimular tensões diplomáticas a longo prazo[118].

---

[116] GHAPPOUR, Ahmed. *Searching places unknown: law enforcement jurisdiction on the dark web*. Stanford Law Review. 69.4. 2017. Disponível em: <https://stanford.io/2pIBCGa>. Acesso em: 05/06/2018.

[117] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Reforma do MLAT entre privacidade e eficiência. 2017. (52m02s). Disponível em: <https://www.youtube.com/watch?v=0AwSGbGXgr0&t=2725s>. Acesso em: 06/02/2018.

[118] LA CHAPELLE, Bertrand de; FEHLINGER, Paul. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. 2016. p. 7. Disponível em: <https://goo.gl/qAisYB>. Acesso em: 07/06/2018.

4.3 Possíveis soluções para o problema

Ao longo deste trabalho, foram trazidas várias técnicas de acesso a dados eletrônicos armazenados no exterior, que podem ser divididos em alternativas de força bruta ou de cooperação legal.

As soluções de força bruta consistem em mecanismos que valorizam a eficiência às custas dos direitos humanos básicos, como a implantação de *backdoor*, o *hackeamento* pelo governo, a política de localização de dados, a proibição da criptografia forte, conforme visto nesse capítulo, e até a prisão de executivos e a suspensão ou encerramento de serviços de uma empresa, após o não cumprimento de determinação judicial feita diretamente à filial brasileira. São soluções originadas da frustração das autoridades governamentais investigativas, que buscam meios cada vez mais agressivos em razão da recorrente inabilidade em alcançar as informações pretendidas pelos meios colaborativos.

As soluções colaborativas, por sua vez, buscam facilitar o acesso a dados às autoridades investigativas sem abrir mão da proteção de direitos fundamentais, da privacidade e da atenção ao devido processo legal. Conforme analisado ao longo deste trabalho, dizem respeito aos mecanismos de cooperação jurídica internacional em matéria penal – o MLAT, em especial – e oferecem meios jurídicos para obtenção dos dados eletrônicos, tendo em vista a incapacidade técnica e jurídica das filiais das empresas de tecnologia localizadas no Brasil em colaborar. Contudo, esse mecanismo se mostra excessivamente ineficaz e defasado em relação às crescentes demandas atuais.

Apesar das críticas a todas as alternativas apresentadas ao longo do estudo, não foi identificada solução única, capaz de resolver, ao mesmo tempo, os problemas de ineficiência apresentada pelos mecanismos de auxílio internacional e da falta de proteção a direitos fundamentais de privacidade, nos demais modelos apresentados.

A solução para o debate pode se dar, então, por meio de diferentes esforços e mudanças, que podem resultar em um panorama mais positivo sem que seja necessário recorrer aos meios de força bruta, menos protetivos dos direitos de privacidade.

Inicialmente, destaca-se a reforma do MLAT. O referido sistema de assistência legal mútua, cujo procedimento foi debatido com detalhes nesse estudo, apresenta-se como meio de realização de diligências no exterior. Assim, mesmo que o crime tenha ocorrido no Brasil, com

agente e vítimas brasileiras, caso haja necessidade de se obter uma informação vital armazenada em servidor no exterior, as autoridades investigativas têm que se submeter a esse processo para acesso a dados.

Processo que geralmente é demorado e ineficiente por diversos motivos, notadamente pelo excessivo rigor estabelecido pela legislação americana, a ser observada no cumprimento das diligências requeridas. Em especial, o requisito do *probable cause*, um dos standards legais mais altos do mundo, é o que gera a maior quantidade de pedidos finalizados com resultado negativo dado pelas autoridades americanas[119].

O não atingimento do referido requisito se dá pela falta de conhecimento e costume das autoridades brasileiras em relação a esse tipo de cooperação jurídica internacional. Com efeito, a construção do caso criminal no Brasil se dá de forma distinta dos Estados Unidos e as autoridades investigativas e judiciárias daqui muitas vezes não estão preparadas para planejar seus pedidos de auxílio internacional tendo como base a legislação americana e o requisito do *probable cause*[120].

Apesar de todos os problemas observados, o MLAT deve ser aperfeiçoado por meio de reformas, pois é um mecanismo que estabelece garantias processuais mais robustas e uma maior proteção à privacidade, já que a autoridade requerente precisa respeitar as proteções legais de ambos os países envolvidos para acessar os dados.

Nessa toada, a reforma do MLAT deve ser pensada não só para prover mais recursos financeiros para a execução dos pedidos de cooperação internacional, mas também para simplificar os procedimentos e treinar melhor as pessoas envolvidas no processo no país, como as autoridades policiais, do Ministério Público e da Justiça, e funcionários da autoridade central, responsáveis pela tramitação dos pedidos de auxílio[121].

Dessa forma, ao modelo básico de cooperação via MLAT pode ser dado maior eficiência e celeridade sem que os direitos humanos sejam sacrificados, tendo em vista que a demora no procedimento muitas vezes se dá em razão da devolução do pedido pelas

---

[119] Petição de apresentação de manifestação nº 10.426/2018, juntado aos autos da ADC nº 51 do STF. Disponível em: <https://www.dropbox.com/s/jhzoho0ddufigv0/Of%C3%ADcio%20DRCI.pdf?dl=0>. Acesso em: 15/05/2018.

[120] InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Desafios da coleta de evidências digitais e a cooperação internacional para acesso a dados. 2017. (1h04m). Disponível em: <https://www.youtube.com/watch?v=mNGspCMf8Ag>. Acesso em: 09/05/2018.

[121] JAYCOX, Mark; e TIEN, Lee. Reforms Abound for Cross-Border Data Requests. Electronic Frontier Foundation. 2015. Disponível em: <https://goo.gl/2WJAfV>. Acesso em: 05/06/2018.

autoridades americanas, para que sejam feitos esclarecimentos após a não observância do *probable cause*.

No mais, em relação ao papel que o próprio poder Judiciário do país pode exercer, cabe destaque à ADC nº 51 do Supremo Tribunal Federal. No caso, discute-se a constitucionalidade de mecanismos de cooperação internacional para a coleta de dados eletrônicos.

Conforme argumentado pela AGU e pela PGR em manifestações aos autos, a declaração de constitucionalidade dos artigos em questão não tem o efeito pleiteado pela autora de tornar obrigatória a adoção dos mecanismos neles previstos, de modo que o julgamento do processo não será capaz, por si só, de solucionar a controvérsia.

Apesar disso, eventual deliberação dos Ministros a respeito de como deve ser feita a coleta de dados eletrônicos armazenados no exterior fortalecerá uma das correntes, seja a favor da requisição direta às filiais no Brasil ou da necessidade de cooperação internacional para pedido à empresa sede. Por tais motivos, o caso do STF adquire grande importância para o futuro do debate no país e deve ser observado com atenção.

Ainda, apesar das críticas apresentadas ao novo modelo de cooperação criado pelo CLOUD Act, é inegável que eventual acordo executivo com os Estados Unidos poderia facilitar e tornar mais célere a busca por dados eletrônicos armazenados naquele país.

Conforme explicado, a realização do acordo executivo está sujeita à discricionariedade das autoridades americanas, tanto em relação aos requisitos permissivos que os países devem conter para se habilitarem, quanto à efetiva negociação do acordo. Desse modo, assim como a ADC nº 51, não pode ser considerada alternativa capaz de solucionar, por si só, o problema de imediato, em razão da falta de previsibilidade quanto a realização do acordo executivo.

Contudo, caso venha a ser negociado, pode servir como instrumento mais célere que o MLAT para que as autoridades brasileiras peçam diretamente às empresas de tecnologia os dados em questão, sem intermédio de autoridades centrais e órgãos do governo americano.

Uma ressalva que se faz ao modelo é que, apesar de simplificar e desburocratizar as requisições de coleta de dados, retira a supervisão das autoridades governamentais dos EUA às empresas de tecnologia. Dessa forma, serão incumbidas de avaliar se o cumprimento do pedido gera conflito com a lei americana, assim adquirindo grande responsabilidade para lidar com

assuntos sensíveis, que provavelmente não receberão tratamento heterogêneo por todas os provedores de serviços de Internet[122].

Por fim, o Brasil deve dar maior atenção ao cenário internacional e progredir sua participação em foros internacionais de debate sobre privacidade e vigilância, proteção a dados e crimes cibernéticos. Em outras palavras, o Brasil deveria investir em acordos multilaterais especificamente voltados ao tratamento de dados, tendo em vista a anunciada ineficiência dos acordos bilaterais.

O preenchimento da lacuna institucional não depende da criação de novas organizações internacionais, e nem de dar novas atribuições a organizações já existentes, visto que os problemas relacionados à Internet são relevantes para uma pluralidade de entidades governamentais. É necessária uma abordagem mais criativa, como a formação de uma rede de governos interessados na resolução do problema[123].

La Chapelle e Fehlinger sugerem a criação de uma rede que envolva todos os grupos afetados pelo problema em comum, como os Estados, as plataformas de Internet, organizações internacionais, a sociedade civil, operadores técnicos e os especialistas acadêmicos. A diversidade dos atores envolvidos seria capaz de representar os mais variados pontos de vista e apresentar potenciais soluções para o problema. Assim, a partir da análise dos conflitos de jurisdição na Internet e dos diferentes cenários legais existentes, a rede pode desenvolver uma resolução cooperativa em relação a pedidos transfronteiriços de acesso a dados[124].

Em relação a acordos multilaterais já existentes, destaca-se a Convenção de Budapeste, de 2001. É um tratado internacional de direito penal e processual penal firmado no âmbito do Conselho da Europa para definir de forma harmônica os crimes praticados por meio da Internet e as formas de persecução. Dos países não-membros do Conselho Europeu, são signatários o Canadá, Japão, África do Sul e os Estados Unidos.

Além da criação de novos tipos penais puníveis, há previsão também da utilização, pelos signatários, de serviços informáticos de busca remota e em tempo real; interceptação e

---

[122] LA CHAPELLE, Bertrand de; FEHLINGER, Paul. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. 2016. p. 7. Disponível em: <https://goo.gl/qAisYB>. Acesso em: 07/06/2018.
[123] Ibid., p. 10.
[124] Ibid., p. 11.

confisco de dados em trânsito ou armazenados, inclusive para fins de prova judicial; e bloqueio do acesso de terceiros, bem como a possibilidade de se determinar a remoção dos dados[125].

O Brasil não aderiu à Convenção por questões de política internacional, isto é, por não ter participado da negociação dos seus termos. Contudo, há especialistas que criticam esse posicionamento e defendem que o país poderia enriquecer seus conhecimentos técnicos específicos por meio do intercâmbio de experiências que a adesão ao tratado forneceria. Além disso, a adesão estimularia a harmonização da legislação brasileira à internacional no tema, o que facilitaria o combate de crimes cibernéticos transfronteiriços pelo mundo[126]. Ainda, a Convenção já foi ratificada em países que abrigam grandes provedores de aplicações e servidores de armazenagem de dados, como os EUA, de modo que a adesão do Brasil poderia facilitar a troca de dados vitais entre os países.

Além da participação ativa, cabe ao Brasil ficar atento às inovações legais de grande impacto no mundo. Na União Europeia, cabe menção à recente regulação de proteção a dados, o *Regulamento Geral sobre a Proteção a Dados*. O *RGPD*, como também é conhecido, serve para harmonizar as leis de dados privados por toda Europa, com objetivo de proteger e empoderar a privacidade de todos os cidadãos, além de reorganizar a maneira como companhias lidam com dados privados.

Nesse ponto, verifica-se que a entrada em vigor do *RGPD*, em 25 de maio de 2018, fez com que a Câmara dos Deputados acelerasse votação e aprovasse dias depois o Projeto de Lei nº 4.060/2012[127], do deputado Milton Monti (PR-SP). O Projeto, que segue agora para o Senado Federal, regulamenta o uso de dados pessoais, tanto pelo poder público, quanto pela iniciativa privada; exige que companhias, órgãos e qualquer um que reúna informações sobre pessoas justifiquem a necessidade da coleta dos dados; além de proibir que seja acumulado conteúdo maior que o suficiente para os objetivos de uma aplicação ou serviço[128].

---

[125] Kaminsky, O. Conheça o Tratado Internacional contra crimes na Internet. 2001: Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2001-nov-24/convencao_lanca_tratado_internacional_cibercrimes>. Acesso em: 02/06/2018.

[126] Erdelyi, M. F. Itamaraty ainda estuda adesão à Convenção de Budapeste. 2008: Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste>. Acesso em: 02/06/2018.

[127] PL 4060/2012. Andamentos disponíveis em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>. Acesso em: 06/02/2018.

[128] Câmara aprova projeto da "GDPR brasileira", sobre uso de dados pessoais. Disponível em: <https://www.tecmundo.com.br/seguranca/130778-camara-aprova-projeto-gdpr-brasileira-uso-dados-pessoais.htm>. Acesso em: 02/06/2018.

Assim, apesar de não tratar especificamente da coleta de dados no exterior, o esforço parlamentar demonstra que o país está dando mais importância à proteção de dados privados e à necessária atualização da legislação interna como resposta às grandes inovações observadas externamente.

Em suma, o que se pretende dizer é que o Brasil deve incrementar sua participação em foros internacionais de discussão do assunto, para que participe ativamente da elaboração de tratados multilaterais de cooperação jurídica internacional para acesso a dados no exterior. O interesse na resolução do problema não se restringe ao Brasil, de modo que vários outros países também estariam interessados nesse tipo de resolução.

O Brasil possui um dos maiores mercados de Internet do mundo e produz uma quantidade enorme de conteúdo através de seus usuários. Isso dá ao país relevância e influência no cenário internacional para negociar meios mais favoráveis, eficientes e legítimos de acesso a dados eletrônicos, ao invés de apenas se portar como expectador da política de outros países e se sujeitar às leis e tratados por eles emanados.

É verdade que a falta de coordenação das estruturas de cooperação jurídica internacional e de critérios uniformes de jurisdição para solução de litígios de Internet pode criar dificuldades no cotidiano dos tribunais e das autoridades administrativas que lidam com o contencioso transnacional, mas não pode servir como fundamento para a supressão de etapas básicas do processo, cujo intuito é garantir a observância dos direitos fundamentais das partes e de todos os usuários da Internet.

Assim, através da implementação das medidas sugeridas, como a reforma do MLAT e maior participação no debate internacional sobre o tema, o país pode fortalecer suas autoridades judiciárias e administrativas com meios mais eficientes e menos burocráticos para acesso aos dados eletrônicos sensíveis para a investigação ou instrução criminal, sem que seja necessário recorrer às soluções de força bruta e sacrificar direitos humanos básicos de segurança e privacidade.

Dessa forma, é possível esperar um panorama mais positivo e menos controverso em um futuro próximo, a fim de facilitar o acesso das autoridades investigativas e judiciárias aos dados telemáticos armazenados no exterior.

CONCLUSÃO

Os recursos tecnológicos estão cada vez mais presentes na realidade de grande parte da população brasileira, cujo acesso a essas inovações também tem crescido significativamente. Em consonância com o crescimento do acesso à Internet, também cresce a quantidade de crimes cometidos ou planejados através da rede.

Com efeito, uma pesquisa realizada pela *McAfee* em parceria com a *Center for Strategic and International Studies* revela que o crime cibernético gera um prejuízo global de US$ 600 bilhões para as empresas, representando 0,8% do PIB mundial[129]. No mesmo sentido, de acordo com um relatório da Norton Cyber Security, em 2017 o Brasil passou a ser o segundo país com o maior número de casos de crimes cibernéticos, apenas atrás da China, afetando cerca de 62 milhões de pessoas e causando um prejuízo de US$ 22 bilhões[130].

Seria ingênuo acreditar que o Direito é capaz de ser mais rápido do que as inovações tecnológicas, de modo que a Internet deve ser projetada para criar mais segurança aos seus usuários. Com o desenvolvimento acelerado e constante dos serviços e tecnologias ligadas à Internet, é possível que em um futuro não muito distante grande parte dos processos criminais seja instruídos majoritariamente com provas digitais.

Dessa forma, amplia-se o debate acerca da melhor forma de coleta de dados eletrônicos, especialmente quando armazenados no exterior, tendo em vista que grande parte das empresas de tecnologia que provém os serviços de Internet comumente utilizados estão localizadas nos Estados Unidos. Essa discussão se dá tanto do ponto de vista legal, em relação aos meios juridicamente legítimos para tanto, quanto do ponto de vista finalístico, em relação à eficiência das técnicas de coleta de dados.

A requisição direta às filiais brasileiras das empresas de tecnologia, amparadas pelo art. 11 do Marco Civil da Internet, conforme explicado, incorre em obstáculos de cunho técnico e jurídico. Isso porque as filiais brasileiras são meros escritórios das empresas e não detém o controle das plataformas digitais, de modo que as empresas-sede no exterior são as únicas

---

[129] Relatório revela que crime cibernético gera prejuízo global de US$ 600 bilhões. Disponível em: <https://canaltech.com.br/seguranca/relatorio-revela-que-crime-cibernetico-gera-prejuizo-global-de-us-600-bilhoes-108634/>. Acesso em: 06/02/2018.

[130] Brasil é o segundo país no mundo com maior número de crimes cibernéticos. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm>. Acesso em: 02/06/2018.

habilitadas a fornecer essas informações. Além disso, a legislação dos EUA exige prévia autorização da Justiça americana para que suas empresas possam fornecer os dados de comunicação requeridos por entidades governamentais estrangeiras.

Dessa forma, a recusa das empresas de tecnologia em cumprir as determinações judiciais brasileiras tem rendido multas, a suspensão do funcionamento de serviços e até a prisão de executivos. Em face disso, discute-se no STF, por meio da ADC nº 51, a constitucionalidade de mecanismos de cooperação internacional, que se apresentam como alternativa para a coleta de dados eletrônicos.

Conforme exposto, a cooperação jurídica internacional tem como base jurídica o MLAT, que é acordo bilateral de auxílio em matéria penal realizado com os Estados Unidos e diversos outros países. Porém, a análise de dados fornecidos pelo DRCI/MJ, autoridade central brasileira, permite concluir que essa técnica é ineficiente e defasada, por motivos variados.

A principal razão do não funcionamento da cooperação internacional com os EUA, entretanto, é a falha das autoridades brasileiras em atingir o requisito do *probable cause* imposto pela legislação americana, que exige que tais pedidos sejam instruídos com indícios fortes de ligação entre o crime cometido e a comunicação eletrônica que se pretende obter.

Como método alternativo de coleta de dados, o recente CLOUD Act traz a possibilidade de os Estados Unidos realizarem acordos executivos com outros países para tornar possível a requisição de dados diretamente às empresas de tecnologia, sem que seja necessária a tramitação do pedido pelas autoridades centrais e órgãos governamentais americanos. Contudo, para estar habilitado a negociar o acordo com os EUA, o país deve possuir legislação robusta de proteção a dados e demais requisitos a serem observados pelas autoridades americanas.

Apesar de aparentar ser mais célere e menos burocrático que o procedimento via MLAT, o CLOUD Act não passa isento de críticas e não pode ser tomado pelo Brasil como solução única para o problema, uma vez que não há qualquer previsão de realização do acordo, em razão da completa arbitrariedade dada às autoridades americanas para tanto.

Em seguida, foram brevemente apresentadas alternativas de "força bruta", isto é, aquelas que põem em risco os direitos à privacidade e segurança de todos os usuários de Internet em busca de uma solução mais eficiente e invasiva do Estado para acesso a dados eletrônicos. Destacam-se o mecanismo de *backdoor* na criptografia, a proibição de criptografia forte, a política de localização de dados e o governo agindo como *hacker*. Contudo, tais meios

afrontam direitos fundamentais básicos e sacrificam a segurança, a privacidade e a confiança dos usuários na rede, quando o papel dos governos deveria ser justamente zelar por essas proteções, de modo que não podem ser tomados como solução para a controvérsia aqui analisada.

As alternativas que observam os direitos fundamentais e o devido processo legal, como a cooperação jurídica internacional, são chamadas de soluções colaborativas e sobre esse escopo devem ser concentradas as tentativas de resolução do debate. Para tanto, é necessário que sejam feitos diferentes tipos de esforços para melhora do cenário atual de controvérsia e dúvida.

Assim, destaca-se a reforma do MLAT, através do maior investimento de recursos financeiros e, principalmente, na necessária melhora na instrução das autoridades brasileiras que atuam na área. Isso porque grande parte da demora e do não funcionamento da cooperação jurídica internacional têm como causa o desconhecimento no modo que o processo penal é conduzido nos EUA e na consequente falha na observância do requisito básico do *probable cause*, em razão da falta de clareza do conceito.

Internamente, também merece atenção a referida ação de julgamento pelo STF. Ainda que a decisão proferida não tenha o condão de fixar qual meio deve ser utilizado pelas autoridades brasileiras para obtenção de dados eletrônicos armazenados no exterior, a deliberação dos Ministros pode trazer importantes argumentos em defesa de alguma das correntes, seja aquela em favor da requisição direta às filiais das empresas no Brasil, ou seja a que defende a cooperação jurídica internacional.

No mais, apesar das críticas feitas ao CLOUD Act, caso seja negociado um acordo executivo entre os Estados Unidos e o Brasil, esta pode ser uma forma mais célere e menos burocrática de contato entre as autoridades brasileiras e as empresas americanas detentoras dos dados telemáticos almejados. Assim, as novidades da nova lei não podem ser completamente descartadas.

Por fim, é necessário que o Brasil tenha maior participação no cenário internacional, notadamente em foros de debate sobre o tema e em tratados multilaterais de proteção a dados e meios de cooperação na coleta transfronteiriça de dados eletrônicos, tendo em vista que a Internet facilita consideravelmente a prática de crimes que envolvam mais de um país.

O maior obstáculo quando se pensa em auxílio internacional é o da necessária adaptação do país requerente à legislação do país requerido. Dessa forma, a participação do Brasil em tratados multilaterais pode estimular a uniformização da legislação dos países signatários quanto ao assunto, de modo que a cooperação e o contato entre os países-membros ficariam significativamente facilitadas e observariam menos custos de transação.

Com isso, apesar de não haver alternativa capaz de resolver, por si só, o debate acerca da coleta de dados armazenados em outro país, as referidas soluções de política interna e externa podem ser adotadas pelo Brasil para diminuir o cenário de incerteza das autoridades policiais, do Ministério Público e judiciárias em relação ao tema.

Defender a eficiência a aplicação das leis brasileiras não pode significar abrir mão do interesse dos brasileiros, que são beneficiados com a grande quantidade de serviços de Internet e não podem ter seus direitos fundamentais sacrificados. Assim, os meios colaborativos e harmônicos com os direitos à segurança e privacidade devem ser sempre priorizados.

Em um ambiente político transnacional com altíssimo grau de competitividade entre os atores políticos, agentes econômicos e instituições, construir modelos de incentivos de coordenação do fluxo de informações entre os países, especialmente para o aumento da segurança da Internet, mas sem que se olvidem os direitos fundamentais, consiste em prioridade da governança eletrônica e garantia de um futuro sustentável para as atividades humanas.

REFERÊNCIAS BIBLIOGRÁFICAS

ARTESE, Gustavo (coord.). *Marco Civil da Internet: Análise Jurídica sob uma Perspectiva Empresarial*. São Paulo: Quartier Latin, 2015.

BALTAZAR JR., J. P; LIMA, L. F (org.). *Cooperação jurídica internacional em matéria penal.* 1 ed. Porto Alegre: Verbo Jurídico, 2010.

CARTILHA de segurança para internet. Comitê Gestor da Internet no Brasil, 23 out. 2006. Disponível em: <http://cartilha.cert.br/sobre/old/cartilha_seguranca_3.1.pdf>. Acesso em: 09/05/2018.

Erdelyi, M. F. Itamaraty ainda estuda adesão à Convenção de Budapeste. 2008: Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste>. Acesso em: 02/06/2018.

FEROLLA, G.; NAVES, J. P. M.; ZUGAIBE, N. C. *Documento eletrônico como meio de prova no processo penal brasileiro*. Revista dos Estudantes de Direito da UnB. Brasília, 2016.

FISCHER, C. *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data.* Eletronic Frontier Foundation: 2018. Disponível em: <https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data>. Acesso em: 06/02/2018.

GHAPPOUR, Ahmed. *Searching places unknown: law enforcement jurisdiction on the dark web*. Stanford Law Review. 69.4. 2017. Disponível em: <https://stanford.io/2pIBCGa>. Acesso em: 05/06/2018.

GIACCHETTA, A. Z; FREITAS, C. T; MENEGUETTI, P. G. *Marco Civil da Internet põe fim a lacunas na legislação.* Disponível em: <https://www.conjur.com.br/2014-abr-30/marco-civil-internet-poe-fim-lacunas-existentes-legislacao#author>. Acesso em: 09/05/2018.

Government Hacking and Subversion of Digital Security. Disponível: <https://www.eff.org/issues/government-hacking-digital-security>. Acesso em: 02/06/2018.

InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Acesso a comunicações eletrônicas e criptografia: garantias, prerrogativas e devido processo legal. 2017. (2h29m). Disponível em: <https://www.youtube.com/watch?v=W_b2Jr9wFXk>. Acesso em: 09/05/2018.

InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – O debate americano sobre vigilância e criptografia. 2017. (57m42s). Disponível em: <https://www.youtube.com/watch?v=NuszpDZ69qw>. Acesso em: 09/05/2018.

InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Desafios da coleta de evidências digitais e a cooperação internacional para acesso a dados. 2017. (1h04m). Disponível em: <https://www.youtube.com/watch?v=mNGspCMf8Ag>. Acesso em: 09/05/2018.

InternetLab e FDUSP. I Congresso Internacional de Direitos Fundamentais e Processo Penal na Era Digital – Reforma do MLAT entre privacidade e eficiência. 2017. (52m02s). Disponível em: <https://www.youtube.com/watch?v=0AwSGbGXgr0&t=2725s>. Acesso em: 06/02/2018

JAYCOX, Mark; e TIEN, Lee. *Reforms Abound for Cross-Border Data Requests*. Electronic Frontier Foundation. 2015. Disponível em: <https://goo.gl/2WJAfV>. Acesso em: 05/06/2018.

Kaminsky, O. Conheça o Tratado Internacional contra crimes na Internet. 2001: Consultor Jurídico. Disponível em: <https://www.conjur.com.br/2001-nov-24/convencao_lanca_tratado_internacional_cibercrimes>. Acesso em: 02/06/2018.

KIM, S.; FIDLER, Mailyn. The Weak Link in a Double Act: U.K. Law is Inadequate for Proposed Cross-Border Data Request Deal. 2017: Lawfare. Disponível em:

<https://www.lawfareblog.com/weak-link-double-act-uk-law-inadequate-proposed-cross-border-data-request-deal>. Acesso em: 02/06/2018.

LA CHAPELLE, Bertrand de; FEHLINGER, Paul. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. 2016. Disponível em: <https://goo.gl/qAisYB>. Acesso em: 07/06/2018.

MASSO, F. D.; ABRUSIO, J.; FILHO, M. A. F (coord.). Marco Civil da Internet: Lei 12.965/2014. 2. ed. São Paulo: Editora Revista dos Tribunais, 2014.

MENDES, G. F.; BRANCO, P. G. G. Curso de direito constitucional. 7. ed. São Paulo: Saraiva, 2012.

NETO, M. F.; SANTOS, J. E. L.; GIMENES, E. V. *Crimes na Internet e Inquérito Policial Eletrônico*. 1. ed. São Paulo: EDIPRO, 2012.

WOODS, A. K.; SWIRE, P. *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems.* 2018: Lawfare. Disponível em: <https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems>. Acesso em: 02/06/2018.

ZANIOLO, Pedro Augusto. *Crimes Modernos: o impacto da tecnologia no direito*. 3. ed. Curitiba: Juruá Editora, 2016.