Instituto de Referência em Internet e Sociedade

Obtenção transnacional de conteúdo de comunicações telemáticas na América Latina

Relatório de Pesquisa

iris
INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

Instituto de Referência em Internet e Sociedade

Obtenção transnacional de conteúdo de comunicações telemáticas na América Latina

Relatório de Pesquisa

Orientação científica
Fabrício Bertini Pasquot Polido
Luíza Couto Chaves Brandão

Coordenação
Lahis Pasquali Kurtz

Autoria
Lahis Pasquali Kurtz
Victor Barbieri Rodrigues Vieira

Colaboração e Revisão
Fabrício Bertini Pasquot Polido
Luíza Couto Chaves Brandão

Projeto Gráfico e Capa
André Oliveira e Felipe Duarte

Diagramação e finalização
Felipe Duarte

Produção editorial
Instituto de Referência em Internet e Sociedade

Como citar em ABNT

KURTZ, Lahis; VIEIRA, Victor. **Obtenção transnacional de conteúdo de comunicações telemáticas na América Latina:** relatório de pesquisa. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2020. Disponível em: https://bit.ly/2RkAmaL.Acesso em: DD mmm. AAAA

SUMÁRIO

1. Introdução[1]

Em 2019, o Instituto de Referência em Internet e Sociedade publicou estudo inédito analisando os grupos econômicos integrados por grandes empresas provedoras de aplicações de internet e suas interfaces com a jurisdição brasileira[2]. Mais especificamente, buscou-se investigar a forma como arquiteturas societárias difusas repercutem na efetivação do direito em casos adjudicados pelos tribunais brasileiros nos quais é necessário obter uma prestação jurisdicional por parte de um provedor sediado no estrangeiro, mesmo que este possua escritórios e representação legal em algum nível dentro do território nacional.

Em breve resumo, concluiu-se que a forma como são dispostos esses grupos econômicos resulta em obstáculos significativos para a obtenção da devida prestação jurisdicional. Mais especificamente, a dificuldade encontra-se nos percalços relativos ao compartilhamento de dados envolvendo comunicações telemáticas localizadas no estrangeiro para fins probatórios em processos judiciais no Brasil. O que ocorre por diversas vezes é uma ordem judicial para que o provedor de aplicação em questão forneça informações que permitam localizar o autor de um delito digital, como endereço IP da pessoa que realizou uma postagem tida como infrativa em rede social, sua porta lógica de origem, entre outros identificadores.

Constatou-se, com o estudo, que há grande resistência por parte dos provedores de aplicação localizados no estrangeiro para cumprir as decisões judiciais brasileiras. Esses provedores, por diversas vezes, são sediados nos EUA, mantém seus *data centers* em algum país da Europa ou mesmo nos EUA e detém empresas subsidiárias no Brasil que não necessariamente realizam o processamento dos dados relativos aos usuários brasileiros. Como resultado, o tráfego de dados originados no território brasileiro é direcionado para o Estado no qual estão localizados os servidores principais da empresa.

O principal argumento elencado, portanto, é o da ilegitimidade para figurar no polo passivo dessas demandas judiciais, sob a alegação de que o procedimento correto para obtenção do direito pretendido seria acionar a empresa sede – detentora dos bancos de dados onde as informações requeridas estão armazenadas, e situada em países estrangeiros. O que se observa, nesse sentido, é a tentativa de aproximação da causa do sistema jurídico referente à jurisdição na qual estão sediados os *data centers* ou a empresa – seja essa aproximação relativa à aplicação da lei ou à competência para julgar a demanda, tópicos mais detalhadamente desenvolvidos no estudo original[3].

Apesar de a pesquisa realizada afastar a validade dessas alegações, sendo prevalentes a confusão entre a lei brasileira aplicável e a competência dos tribunais brasileiros para solucionar os conflitos analisados, também é verdade que, em sua vasta maioria, as decisões proferidas pelas autoridades judiciárias brasileiras são no sentido de determinar a execução de sentença em país estrangeiro. Os mecanismos de reconhecimento e execução de sentenças brasileiras no exterior, por sua vez, dependem de cooperação jurídica internacional, segundo instrumentos que necessitam de aprimoramentos. Entre eles se encontram os acordos de assistência jurídica mútua (MLATs – Mutual Legal Assistance Treaties), tratados de cooperação jurídica e outros instrumentos processuais internacionais. Da mesma forma, procedimentos

1 Este relatório apresenta alguns dos resultados de pesquisa realizadas pela equipe do projeto "Cooperação Jurídica Internacional e Litígios da Internet", sob a supervisão científica do Professor Dr. Fabrício Bertini Pasquot Polido.

2 KURTZ, Lahis; CARMO, Paloma; VIEIRA, Victor. **Perfil dos litígios envolvendo a internet no Brasil**: grupos econômicos e jurisdição. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2019. Versão integral disponível em: <http://irisbh.com.br/wp-content/uploads/2019/01/Perfil-dos-lit%C3%ADgios-envolvendo-a-internet-no-Brasil-grupos-econ%C3%B4micos-e-jurisdi%C3%A7%C3%A3o-IRIS.pdf>. Acesso em: 10 de fevereiro de 2020

3 KURTZ, Lahis; CARMO, Paloma; VIEIRA, Victor. **Perfil dos litígios envolvendo a internet no Brasil**, cit.

de cooperação jurídica internacional também são disciplinados pela lei processual interna dos Estados e pelas vias diplomáticas, tendo a reciprocidade um papel ainda relevante no quadro mais amplo das relações internacionais cooperativas[4].

Paralelamente a esse cenário, observou-se nos últimos tempos uma tendência internacional no sentido de se amplificar a importância da disciplina da proteção de dados pessoais. O aumento na relevância dessa matéria em muito se deve ao avanço das novas tecnologias como a inteligência artificial, técnicas e procedimentos relacionados ao *big data*, sendo as preocupações internacionais sobre o tema bem exemplificadas pelo escândalo da Cambridge Analytica em 2018. Nele, usuários da plataforma Facebook tiveram seus dados coletados por uma aplicação interna e compartilhados indevidamente com a empresa controlada pelo SCL Group, sediado na Inglaterra[5]. Essa tendência, por sua vez, repercutiu em movimentos legislativos em diversos países, a fim de promulgar leis para disciplinar a proteção de dados nesses territórios ou então atualizar as legislações já anteriormente vigentes, adaptando-as para a nova realidade do cotidiano digital.

Nesse quadro mais amplo, o Regulamento Geral de Proteção de Dados da União Europeia[6] (GDPR)[7] mostrou-se uma das regulações mais impactantes sobre o tema, influenciando alterações legislativas em diversos países, mesmo além dos limites da UE. O GDPR nasceu como substituto da Diretiva 95/46/CE de 1995, do Parlamento Europeu e do Conselho, regulação esta que representou vanguarda do movimento legislativo global de proteção de dados pessoais. À época em que foi adotada, também influenciou a criação de diversas leis nesse sentido ao redor do mundo, como, por exemplo, a Lei n. 25.326 de 2000, da Argentina, a Lei n. 29733 de 2011, do Peru, a Lei n. 18.331 de 2008, do Uruguai, e a Lei n. 8.968 de 2011, da Costa Rica.

As principais diferenças entre a Diretiva de 1995 e o GDPR são, em suma, relativas à grande precisão técnica e o detalhamento das estipulações da nova legislação, incluindo conceitos pormenorizados de dado pessoal, dados sensíveis e técnicas empregadas para o tratamento destes, bem como enunciando uma série de direitos que garantem ao titular de dados pessoais uma maior autonomia sobre as informações que permitem sua identificação ou elementos identificáveis. Dentre os motivos que justificam a influência do regulamento europeu no contexto internacional, cabe ressaltar a relevância político-econômica do bloco no cenário global e a força dos instrumentos normativos intracomunitários.

O GDPR apresentou, dentre seus diversos dispositivos, uma série de critérios para possibilitar compartilhamento internacional de dados, chamado de "transferência internacional de dados". Entre eles, os países que forem considerados detentores de um grau adequado de proteção de dados pessoais são listados para facilitar o fluxo de dados. Adicionalmente, a existência de uma autoridade nacional para regrar a proteção de dados em um país é tida pela União Europeia como um dos critérios que podem garantir um ambiente regulatório adequado[8].

4 No Brasil, por exemplo, cf. Arts 26 e seguintes do Código de Processo Civil, que submetem a cooperação jurídica internacional à regência pelos tratados e convenções processuais, como regra, e a via diplomática, como procedimento excepcional.

5 ANJOS, Lucas Costa dos. **Privacidade no Facebook:** o que aprender com a Cambridge Analytica. 2018. Disponível em: <http://irisbh.com.br/privacidade-no-facebook-cambridge-analytica/>. Acesso em: 10 de fevereiro de 2020.

6 UNIÃO EUROPEIA. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**. Bruxelas, Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt>.Acesso em: 19 de fevereiro de 2020.

7 Optou-se por utilizar a sigla do regulamento em inglês (General Data Protection Regulation), visto que esta mostrou-se mais amplamente utilizada e facilmente reconhecível do que a sigla em língua portuguesa (RGPD), mesmo dentro do contexto brasileiro.

8 Os artigos 44 a 50 do GDPR disciplinam a transferência de dados pessoais para países terceiros ou organizações internacionais. O artigo 45º, 2, mais especificamente, enuncia os critérios levados em consideração para se medir o nível de proteção a dados pessoais garantido por um

Levando-se em consideração esse contexto, portanto, buscou-se dar continuidade ao estudo realizado anteriormente, sob um novo ângulo. Desta vez, o enfoque foi não apenas o contexto nacional brasileiro frente às empresas em análise, como se fez anteriormente: neste estudo, buscou-se expandir o escopo da pesquisa anterior para a realidade da interação e alcance da jurisdição nos demais países latino-americanos com esses grupos econômicos. O objetivo foi obter respostas relativas às características institucionais e regulatórias que poderiam influenciar na efetividade da obtenção de conteúdo de comunicações armazenado no estrangeiro.

2. Objetivos e procedimentos metodológicos

A pesquisa proposta, mais especificamente, teve por objetivo verificar se a existência de autoridade nacional de proteção de dados influenciaria ou não no diálogo interinstitucional entre judiciários latinoamericanos e empresas que detenham a guarda ou armazenamento do conteúdo de comunicações. Sabemos que há procedimentos, que variam entre judiciais e/ou administrativos dependendo do país, por meio dos quais as autoridades solicitam dados e informações de usuários às empresas.

Dentre os modelos de procedimentos para solicitação dessas informações entre entidades pertencentes a diferentes Estados, cabe apontar os acordos executivos com o governo dos EUA, previstos no CLOUD Act[9]. Esses tratados, segundo a regulação estadunidense, visam a facilitação do procedimento internacional de compartilhamento de dados entre dois ou mais países, tornando-o mais célere e eficiente do que a modelo usual de cooperação jurídica internacional baseado em acordos de cooperação mútua (os MLATs).

No caso deste estudo, portanto, uma das hipóteses que se buscou analisar foi a existência de um desequilíbrio de forças nas relações interinstitucionais perante os EUA, com este último demandando de países terceiros uma prontidão maior do que a sua própria para responder a solicitações de compartilhamento internacional de dados. Buscou-se analisar, ainda mais especificamente, se a receptividade por parte dos EUA, nos pedidos de cooperação, sofreria alterações sensíveis a depender do nível institucional de proteção de dados do país terceiro solicitante em cada caso.

A mesma abordagem foi hipotetizada com relação à receptividade dos países da União Europeia aos distintos ambientes de proteção de dados dos países integrantes da América Latina. Apesar de as empresas acionadas nos casos analisados apresentarem, em grande parte, sedes nos EUA, a UE representa um território em que estas detêm quantidade significativa de bases operacionais e bancos de dados.

Tendo em mente as hipóteses acima, inicialmente pretendeu-se realizar um levantamento dos casos de obtenção dessas comunicações por vias administrativas ou judiciais[10] em países que possuíam autoridades nacionais de proteção de dados e que não possuíam. Por casos a serem analisados, entenderam-se o conteúdo das decisões, judiciais ou

determinado país.

9 ESTADOS UNIDOS. To amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes. **Cloud Act**. Washington, DC. Disponível em: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text. Acesso em: 26 de fevereiro de 2020.

10 Esclarecemos que há dois contextos nos quais autoridades emitem pedidos de cooperação a empresas detentoras de conteúdo de comunicações e dados telemáticos: o judicial (proveniente de litígios processuais no país de origem) e o administrativo (remetido por agências ou autoridades do poder executivo, provenientes de procedimentos como investigações policiais, processos administrativos e afins). Cada um obedece a uma dinâmica e a procedimentos próprios. Esses dois tipos de pedidos são, inclusive, computados de forma separada por algumas dessas empresas em seus relatórios de transparência.

administrativas, em que uma empresa que controla conteúdo de comunicação online tivesse sido chamada perante autoridades locais para fornecer essas informações.

Para enfrentar a tarefa de analisar esses casos, decidiu-se por um recorte, e não por abranger a totalidade dos países latinoamericanos (o que tornaria a tarefa extensa sem necessariamente agregar qualidade aos resultados). A fim de estabelecer critério de relevância, a pesquisa elegeu um critério de consulta aos relatórios de transparência sobre pedidos de dados e informações de usuários de serviços online, divulgado pelas próprias empresas. Foram consideradas, para o levantamento, as plataformas de comunicação online e as empresas responsáveis por elas. Para definir quais as maiores empresas de comunicação online, observou-se o ranking da Apple de aplicativos mais baixados por usuários em 2018[11]:

Facebook Messenger

Facebook

WhatsApp

TikTok

Instagram

UC Browser

SHAREit

Snapchat

Netflix

Vigo Video

Dele, excluíram-se o UCBrowser, por ser um navegador; o ShareIt, pelo enfoque na transferência de arquivos; a Netflix, por ser plataforma de acesso, mas não de publicação, por usuário, de conteúdo. Quanto às plataformas Tik Tok e Vigo Vídeo, não foram localizados relatórios de transparência específicos para o ano de referência. Ainda, as plataformas Instagram e WhatsApp são vinculadas à empresa Facebook. A essa lista foram adicionados os relatórios: da plataforma Twitter, da Apple, da Google e da Microsoft, pela constatação de que há número significativo de pedidos de autoridades registrado em seus relatórios de transparência, de forma que desconsiderá-las poderia não retratar corretamente a realidade.

Esses documentos indicam globalmente o número de pedidos realizados por autoridades de cada país, bem como, em alguns, o tipo de pedido e quantos foram atendidos. Esse é um dado generalizado, que não possibilita a análise caso a caso de cada pedido, uma vez que são divulgados os quantitativos totais de solicitações no ano, algumas vezes categorizando-os pelo tipo de fundamento. Observaram-se quais os países da região com maiores quantidades de solicitações em cada um desses serviços. A análise compreendeu a seguinte lista de relatórios de transparência, considerando 2018 como ano de referência:

11 PROTESTE. Conheça os aplicativos mais baixados no mundo em 2018. ConectaJá. https://conectaja.proteste.org.br/aplicativos-mais-baixados-de-2018/. Acesso em: 31 mar. 2020.

Quadro 1 - Referências dos relatórios de transparência das principais empresas operadoras de plataformas

Plataforma	Link do relatório de transparência - último acesso: 12/2019
Facebook	https://transparency.facebook.com/government-data-requests
Google	https://transparencyreport.google.com/user-data/overview?hl=pt_BR&user_requests_report_period=series:requests,accounts,compliance;authority:;time:&lu=user_requests_report_period&legal_process_breakdown=expanded
Twitter	https://transparency.twitter.com/en/information-requests.html
Snapchat	https://www.snap.com/en-US/privacy/transparency/
Apple	https://www.apple.com/legal/transparency/
Microsoft	https://www.microsoft.com/en-us/corporate-responsibility/lerr

Fonte: Elaborado pelos autores

Em todos os relatórios, percebeu-se constância de países e serviços que recebem a maioria dos pedidos de informação.

Quadro 2 - Número de pedidos de dados de usuários formulados pelas autoridades

Países/ empresas	Facebook (judicial)	Google	Twitter	Snapchat	Apple	Microsoft
Ano	**2018 (jul-dez)**	**2018 (jul-dez)**	**2018 (jul-dez)**	**2018 (jul-dez)**	**2018 (jul-dez)**	**2018 (jul-dez)**
Brasil	3761	2111	55	6	491	1176
Argentina	1564	706	31	5	3	623
México	1371	270	50	1	0	213
Chile	432	139	12	N/D	33	77
Colômbia	432	37	41	1	3	44
República Dominicana	89	3	12	N/D	1	2
Equador	81	2	3	N/D	N/D	16
Guatemala	78	3	7	N/D	N/D	N/D
Peru	58	1	N/D	N/D	N/D	21
Uruguai	15	1	N/D	N/D	N/D	N/D
El Salvador	15	0	N/D	N/D	N/D	1
Paraguai	12	5	1	N/D	1	N/D
Venezuela	3	N/D	N/D	N/D	N/D	N/D
Panamá	1	N/D	N/D	N/D	N/D	1

Trinidad e Tobago	0	N/D	N/D	N/D	N/D	N/D
Costa Rica	0	1	N/D	N/D	N/D	35
Nicarágua	0	N/D	N/D	N/D	1	N/D
Honduras	0	N/D	N/D	N/D	N/D	N/D

Fonte: elaborado pelos autores

O Brasil e o Facebook, respectivamente, são o país e a empresa/plataforma que mais registraram pedidos de dados de usuários. Percebeu-se que os países que mais demandam de uma empresa/plataforma também figuravam no topo da lista nas outras plataformas/ empresas. Por isso, o critério de relevância para inserir determinado país na amostra foi a quantidade de pedidos realizados por suas suas autoridades.

Dessa forma, foram selecionados para a amostra de países com autoridade nacional de proteção de dados a Argentina, o México e a Colômbia, cujos relatórios de grandes empresas/ plataformas online sobre pedidos de dados pessoais de usuários por autoridades em 2018 apresentaram as maiores quantidades. Para a amostra de países sem autoridade nacional de proteção de dados, foram selecionados Brasil, Chile, República Dominicana, Equador e Guatemala, pelo mesmo critério.

Assim, tendo-se definido uma variável – a existência ou não de autoridade nacional de proteção de dados – e amostras com valores distintos dessa variável, escolhidas com critérios relevantes ao objeto pretendido – a maior quantidade de demandas de dados de usuários por autoridades, segundo relatórios de transparência – passou-se à etapa de coleta de decisões.

A partir da coleta de decisões, pretendia-se identificar se havia resultado positivo ou não das ordens judiciais de fornecimento de comunicações de usuários de serviços de comunicação online. Um dos pontos a ser analisado é se as jurisdições locais obtinham êxito sobre essas empresas, em sua maioria de atuação transnacional, ou se algum problema de conflito de competência emergia, bem como se alguma razão de direito a proteção de dados pessoais era invocada como argumento em caso de negativa. De maneira ampla, o objetivo foi identificar o resultado das solicitações feitas por autoridades locais e os fundamentos para tais ordens e para a resposta fornecida pelas empresas.

A partir da obtenção e leitura dos casos, seria realizada comparação entre aqueles onde há e onde não há autoridade nacional de proteção de dados. O objetivo seria identificar se existe um padrão, uma correlação entre a existência ou não da autoridade e a obtenção ou não dessas informações.

Uma das hipóteses seria a seguinte: países contando com autoridade nacional de proteção de dados teriam seus requerimentos de cooperação melhor atendidos pelos EUA ou pela UE. Seria possível presumir que nessas jurisdições haveria maior chance do nível de proteção de dados ser adequado, e isso refletiria em menor risco de uso indevido das informações, bem como em maior confiança das empresas nas autoridades solicitantes. Outra razão que justificaria essa hipótese é que um dos motivos pelos quais a proteção de dados é considerada parte crucial dos serviços de comunicação online é que muitos dos locais onde eles são ofertados não contam com garantias institucionais contra o uso indevido de dados pessoais. Isso levaria de dados pessoais. Isso levaria as próprias empresas a terem de prover essa segurança. Assim, a existência de uma autoridade nacional de proteção de dados conferiria maior confiabilidade no procedimento de entrega de informações, também porque a

existência de um sistema de garantias aos cidadãos daria sustentação legal a essa cooperação.

Por fim, seriam formuladas, na última etapa, hipóteses a respeito dos motivos e contexto no qual ocorre a negativa ou a entrega de comunicações de usuários por empresas a autoridades dos países abrangidos. O estudo previa ainda prospectar possibilidades para o Brasil a partir da implementação da autoridade nacional de proteção de dados no país, indicando mudanças e entraves a serem superados.

3. Resultados obtidos e encaminhamentos para o futuro

Um levantamento importante realizado na primeira etapa do projeto foi de literatura sobre jurisdição e fluxo de dados, bem como sobre investigações envolvendo comunicações online. No campo teórico, foram identificados aportes da literatura discutindo as seguintes problemáticas:

- Restrictions on Cross-Border Data Flows: A Taxonomy[12] - O texto oferece um quadro de leis e regulações sobre dados pessoais de diversos países, inclusive da América Latina, filtrando os principais entraves normativos ao fluxo transfronteiriço de dados, de acordo com a base de dados "Estimativa de comércio digital". Aponta, entre eles: regime de fluxo condicional; requisito de processamento local e banimento da transferência.

- Navigating the Gauntlet: A Survey of Data Privacy Laws in Three Key Latin American Countries[13] - Explora o tratamento de dados pessoais por empresas no Uruguai, Argentina e México, destacando como ocorre a transferência de dados para fora do país, em que casos ela é permitida e como ocorre o fornecimento de dados no contexto de litígios em outros países.

- *Facilitando* the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America[14] - Narra a adoção de regulações de proteção de dados e sua relação com o interesse dos países latinoamericanos em ter competitividade no mercado tecnológico. Mapeia a regulação do assunto nos países da América Latina.

- The un-territoriality of data[15] - Discute os inúmeros problemas que a estrutura de armazenamento e tratamento de dados da internet traz para a jurisdição, considerando sua aterritorialidade: característica de não possuir um único local certo e determinado onde se pode considerar que um dado esteja armazenado.

- Comparative Analysis of Surveillance Laws and Practices in Latin America[16] - Relatório publicado pela E3F expondo as dificuldades enfrentadas em fiscalizar abusos de poder dos países em relação a vigilância sobre dados de cidadãos nos países da América Latina. Destaca que os relatórios de transparência existentes, disponibilizados unilateralmente

12 FERRACANE, Martina. **Restrictions to Cross-Border Data Flows:** A Taxonomy. Ecipe Working Paper n. 1, 2017. Brussels: European Centre for International Political Economy, 2017.

13 EUSTICE, John C.; BOHN, Marc Alain. **Navigating the Gauntlet:** A Survey of Data Privacy Laws in Three Key Latin American Countries. The Sedona Conference Journal, Vol. 14. Phoenix: The Sedona Conference, 2013. Disponível em: https://www.millerchevalier.com/external-publication/navigating-gauntlet-survey-data-privacy-laws-three-key-latin-american-countries Acesso em: 11 fev. 2020.

14 GUTIÉRREZ, Horacio E.; KORN, Daniel. **Facilitando the Cloud**: Data Protection Regulation as a Driver of National Competitiveness in Latin America, 45 U. Inter-American Law Review, 33. Miami: IALR, 2013. Disponível em: https://inter-american-law-review.law.miami.edu/wp-content/uploads/2014/03/Facilitando-the-Cloud.pdf. Acesso em: de fev. 2020.

15 DASKAL, Jennifer. **The un-territoriality of data**. Yale Law Journal, CT, v. 125, n. 2, p. 326-599, New Haven: Yale, 2015. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5729&context=ylj. Acesso em: 10 fev. 2020.

16 RODRIGUEZ, Katitza. **Comparative Analysis of Surveillance Laws and Practices in Latin America**. Necessary and Proportionate. Electronic Frontier Foundation, 2016. Disponível em: https://necessaryandproportionate.org/comparative-analysis-surveillance-laws-and-practices-latin-america. Acesso em: 10 fev. 2020.

por empresas, carecem de verificação, já que é uma informação obtida de maneira parcial, sem a possibilidade de conferência pela sociedade tendo em vista que a outra parte envolvida nos pedidos de informação (o governo) não possui políticas de transparência em relação a pedidos de informação sobre usuários de serviços online.

Adicionalmente, importa mencionar o estudo realizado pelo Instituto Brasileiro de Defesa do Consumidor (Idec) acerca das autoridades nacionais de proteção de dados na América Latina[17]. Ele aborda diversos aspectos dos modelos institucionais dessas autoridades em diversos países da América Latina, e serviu como importante fonte de informações para a realização do presente estudo, bem como contribuiu para a delimitação do próprio escopo de pesquisa do mesmo.

A pesquisa aqui relatada também examinou artigos especializados e legislações sobre proteção de dados pessoais nos países da amostra, destacando-se os trechos relativos à entrega internacional de dados. Ao investigar o quadro regulatório dos países, constatou-se que essas leis são aprovadas e formuladas tendo por referência atender necessidades do cenário global, dos mercados que se abrem para atração e fixação de empresas estrangeiras em países latinoamericanos ou prestação desses serviços nos países. Assim, as leis e requisitos europeus são considerados como referência, de maneira que Uruguai e Argentina, a fim de serem reconhecidos como países com níveis adequados de proteção de dados, são pioneiros em elaborar legislações protetivas e obter esse status. Tanto é assim que ambos figuram entre países terceiros beneficiados pelas decisões de adequação da União Europeia[18].

Também foi possível constatar que existe um conjunto de países latinoamericanos que é mais ativo em requerer, por meio de suas autoridades, dados de comunicações online a empresas que prestam esse serviço na internet. Essa informação foi extraída observando-se os relatórios de transparência das principais plataformas e empresas, selecionadas segundo ranking de *downloads* da Apple de 2018. Argentina, México, Colômbia, Brasil, Chile, República Dominicana, Equador e Guatemala foram selecionados para a amostra de observação por apresentarem os maiores quantitativos de pedidos, e contarem com diferentes valores na variável "possui autoridade nacional de proteção de dados", sendo o valor nos 3 primeiros positivo e, nos outros 4, negativo.

17 Instituto Brasileiro de Defesa do Consumidor - Idec. **Autoridade de Proteção de Dados na América Latina:** Um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. Idec: São Paulo, 2019. Disponível em <https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina>. Acesso em 10 de fevereiro de 2020.

18 Do ponto de vista procedimental, a Comissão Europeia tem o poder de determinar, com base no artigo 45 do GDPR, se um país externo à União oferece um nível adequado de proteção de dados. A adoção de uma decisão de adequação envolve: uma proposta da Comissão Europeia; um parecer do Conselho Europeu para a Proteção de Dados; uma aprovação de representantes de países da UE e a tomada da decisão pela Comissão Europeia. Sobre as decisões de adequação, ver: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em 23.03.2020.

4. Obstáculos e limitações encontrados

Durante o desenvolvimento do estudo proposto, foram encontrados diversos obstáculos para a devida execução da pesquisa, que resultaram na impossibilidade de se obter resultados conclusivos acerca do objeto que se tinha em análise.

Primeiramente, no que se refere especificamente aos pedidos de informações, dados e comunicações de usuários (essa distinção não é feita em relatórios de transparência), não foi possível levantar hipóteses a partir do material disponível encontrado. Os relatórios de transparência, embora sejam bastante relevantes no sentido de registrar e possibilitar ao usuário conhecer o uso e compartilhamento de seus dados com autoridades, não permitem a formulação de informação crítica sobre as motivações dos pedidos, tipos de casos investigados, motivações para as solicitações e para a resposta fornecida à autoridade, nem mesmo os números de referência dos processos judiciais e administrativos em que foram baseados.

As próprias decisões originalmente selecionadas para análise, da mesma forma, não permitiram que se obtivessem conclusões concretas. Durante a busca pelas referidas decisões (judiciais ou administrativas), constatou-se que os mecanismos de transparência judicial e administrativa mantidos pelos países latinoamericanos estudados não representavam bancos de dados completos o suficiente para possibilitar uma busca exaustiva pelos casos que se pretendia consultar. Isso porque múltiplas vezes os motores de busca pareceram não contar com decisões relativas ao tema de pesquisa que se pretendia (buscas relativas a cooperação jurídica internacional, MLATs, proteção de dados ou mesmo provedores de aplicação específicos, por exemplo, geraram poucos resultados úteis).

Além disso, em mais de uma instância, o que se encontrou não foi um repositório da totalidade das decisões proferidas pelos órgãos judiciários do país em questão, mas sim um compilado de casos icônicos ou um repositório limitado às decisões de cortes superiores de um país. Pode-se citar como exemplos, respectivamente, o portal argentino da SAIJ – no qual são resumidas e disponibilizadas decisões seletas relativas a casos do Judiciário na Argentina – e o repositório de Jurisprudência Nacional Sistematizada do Peru – cujo objetivo não é cultivar um repositório integral da jurisprudência peruana, mas sim apenas sistematizar os principais entendimentos das cortes superiores do país, a fim de fornecer uma fonte de embasamento para as cortes inferiores e uniformizar entendimentos no Judiciário do país. Um dos motores de busca encontrados, ainda, é de natureza privada, sendo portanto cobrada uma taxa para sua utilização – trata-se do Microjuris, da Argentina.

Também obtivemos acesso a decisões administrativas da Costa Rica, de acervo pessoal de um pesquisador colaborador[19], de reclamações levadas à autoridade de proteção de dados daquele país. Mesmo estas não se mostraram suficientes para possibilitar a identificação de tendências jurisprudenciais ou mesmo da prontidão das empresas requeridas para responder satisfatoriamente aos requerimentos de compartilhamento de conteúdo de comunicações. Uma característica comum desse tipo de caso era a solicitação particular de indivíduos para que fosse apagado, retificado ou indenizado o mau uso de dados pessoais por alguma empresa.

A seguir são indicados os bancos de dados consultados durante a execução da pesquisa:

19 Registramos o agradecimento a Roberto Lemaître, pesquisador costa-riquenho, pelo gentil fornecimento de seu compilado de arquivos.

Quadro 3 - Fontes de decisões judiciais

País	Link para fontes encontradas - último acesso: 02/2020
Peru	https://jurisprudencia.pj.gob.pe/jurisprudenciaweb/faces/page/inicio.xhtml
Colômbia	https://www.ramajudicial.gov.co/web/ciudadanos e http://jurisprudencia.ramajudicial.gov.co/WebRelatoria/consulta/index.xhtml
Argentina	http://www.saij.gob.ar/home e http://ar.microjuris.com/home.jsp
Uruguai	http://bjn.poderjudicial.gub.uy/BJNPUBLICA/busquedaSimple.seam

Fonte: Elaborado pelos autores

A dificuldade de se obter fontes de consulta para a análise proposta também mostrou-se um obstáculo significativo. Para além da escassez de decisões, uma busca por MLATs que fossem relativos ao compartilhamento de conteúdos de comunicações e envolvessem países da América Latina e da União Europeia ou Estados Unidos viu-se interrompida pela indisponibilidade de uma importante fonte de pesquisa que se estava utilizando para esse fim. O domínio <mlat.info>, gerenciado pela ONG Access Now[20], que compilava esses acordos internacionais em escala global e possibilitava a realização da pesquisa em tempo hábil (levando-se em consideração o reduzido número de pesquisadores neste trabalho) deixou de ser acessível. A ausência de repertório dos acordos em base unificada tornou inviável a busca pelos instrumentos, particularmente porque podem ser distribuídos entre acordos bilaterais e multilaterais (de alcance global ou regional). Como consequência, não foi possível analisar a existência de cláusulas de facilitação do acesso dos países estudados a conteúdos de comunicações para fins comprobatórios e de persecução penal, por exemplo, prejudicando consideravelmente os resultados do estudo.

A título exemplificativo, pode-se acrescentar que o Brasil tem um MLAT firmado com os EUA, incorporado ao ordenamento jurídico interno por meio do Decreto nº 3.810, de 02 de maio de 2001[21]. Esse tratado enuncia os mecanismos e o alcance da cooperação jurídica internacional e assistência jurídica mútua entre os dois países em matéria penal, as questões procedimentais e as autoridades estatais envolvidas nesse processo, entre outros. Serve, portanto, como fonte importante de informações sobre os procedimentos de cooperação internacional entre Brasil e EUA – motivo que ilustra a importância de se analisar os MLATs existentes entre os países selecionados e os EUA e países da Europa para o desenvolvimento da presente pesquisa.

Outro obstáculo encontrado para a obtenção de resultados conclusivos foi uma impossibilidade de se correlacionar os dados obtidos entre si para que fossem realizadas induções plausíveis. Não foi possível, por exemplo, testar a correlação entre os índices de êxito na obtenção de conteúdos de comunicações em cada país analisado com a dimensão de cada um, suas relevâncias político-econômicas no cenário internacional, a maturidade do cenário de proteção de dados de cada um ou com o reconhecimento pela União Europeia de que um país seja detentor de grau satisfatório de proteção de dados. Essa insuficiência de

20 ACCESS NOW. Disponível em: https://www.accessnow.org/. Acesso em: 11 fev. 2020.

21 BRASIL. DECRETO Nº 3.810, DE 02 DE MAIO DE 2001. **Promulga o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América, celebrado em Brasília, em 14 de outubro de 1997, corrigido em sua versão em português, por troca de Notas, em 15 de fevereiro de 2001**, Brasília, DF, maio 2017. Disponivel em: <http://www.imprensanacional.gov.br/mp_leis/leis_texto.asp?ld=LEI%209887>. Acesso em: 01 de abril de 2020.

análise ocorre pela relatada falta de dados sobre o índice de pedidos realizados, as razões para sucesso ou fracasso na obtenção governamental dos conteúdos de comunicações, e o conteúdo das decisões judiciais sobre os casos relacionados.

Importa também mencionar que, durante a execução da pesquisa, a União Europeia ainda não havia emanado decisões acerca do nível de proteção de dados em todos os países analisados. Embora esse detalhe não estivesse diretamente relacionado com a pergunta de pesquisa ("A existência de autoridade nacional de proteção de dados pessoais facilita na obtenção de conteúdos de comunicações?"), essas decisões poderiam apontar para alguma conclusão mais substancial. Por exemplo, se um país sem autoridade de proteção de dados fosse considerado, ainda assim, detentor de um nível adequado de proteção de dados, a hipótese inicial estaria falseada e teria de ser revista. A escassez dessas decisões por parte da UE foi, portanto, outro obstáculo para a realização do presente estudo.

Finalmente, importa ressaltar que a extrema atualidade do tema implica considerável indisponibilidade de vasto material para consulta. Trata-se de obstáculo que potencialmente será amenizado conforme a evolução dos procedimentos e mecanismos decisórios da União Europeia relativamente aos graus de adequação e conformidade dos padrões de proteção de dados dos países da América Latina. Com o tempo, também se espera aumento nos casos divulgados de compartilhamento ou não de conteúdo de registros de dados de comunicações entre usuários de internet com países terceiros, bem como de mais informações sobre os procedimentos implicados na transferência de informações para países da América Latina e outras regiões do mundo e vice-versa.

5. Considerações finais

Espera-se, não obstante as limitações apontadas, que os resultados parciais aqui apresentados sejam úteis para continuidade e aprofundamento dos estudos aqui propostos em momento futuro. A revisão bibliográfica já realizada tende a mostrar-se como referencial para institutos e centros de pesquisa, em especial na América Latina, e que estejam envolvidos em temas correlatos ao que se estudou no presente trabalho.

Também é forçoso afirmar que a própria falta de resultados conclusivos na pesquisa representa conclusão importante relativamente à opacidade sobre como se operacionaliza a transferência internacional de dados, inclusive de conteúdo de comunicações telemáticas, para países que não detêm o mesmo poderio político-econômico que países da União Europeia ou os Estados Unidos. Esse "vazio" indica, entre outras coisas, que o intenso esforço regulatório de proteção de dados que se tem observado entre os países da América Latina não aparenta – ao menos com base nas estatísticas disponíveis – atender às perspectivas destes por uma melhora evidente nas relações interinstitucionais com o Norte Global.

Por outro lado, a inconclusão de resultados poderia suscitar preocupações analíticas críticas, particularmente as que dizem respeito às assimetrias de poder regulatório e de aplicação das leis envolvendo dados e internet. A separação do globo em macrorregiões informacionais, a exemplo das Américas, União Europeia, Eurásia e China e fortalecimento da indústria de internet e TI demonstra a oportunidade de expansão de estudos que se dediquem a compreender as dinâmicas da governança de dados. Não à toa, o fluxo transnacional de dados torna-se componente inafastável para identificação dos sujeitos, interações e processos na geopolítica da informação e do conhecimento e novas formas de desigualdade na economia global.

6. Referências bibliográficas

ACCESS NOW. Disponível em: https://www.accessnow.org/. Acesso em: 11 fev. 2020.

ANJOS, Lucas Costa dos. **Privacidade no Facebook**: o que aprender com a Cambridge Analytica. Belo Horizonte: IRIS, 2018. Disponível em: http://irisbh.com.br/privacidade-no-facebook-cambridge-analytica/. Acesso em: 10 fev. 2020.

APPLE. **Transparency**. Disponível em: https://www.apple.com/legal/transparency/. Acesso em: 11 fev. 2020.

DASKAL, Jennifer. The un-territoriality of data. **Yale Law Journal**, CT, v. 125, n. 2, p. 326-599, New Haven: Yale, 2015. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5729&context=ylj. Acesso em: 10 fev. 2020.

DROPBOX. **Transparency reports**. Disponível em: https://www.dropbox.com/en_GB/transparency/reports. Acesso em: 11 fev. 2020.

ESTADOS UNIDOS. To amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purposes. **Cloud Act**. Washington, DC. Disponível em: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text. Acesso em: 12 nov. 2019.

EUSTICE, John C.; BOHN, Marc Alain. Navigating the Gauntlet: A Survey of Data Privacy Laws in Three Key Latin American Countries. **The Sedona Conference Journal**, Vol. 14. Phoenix: The Sedona Conference, 2013. Disponível em: https://www.millerchevalier.com/external-publication/navigating-gauntlet-survey-data-privacy-laws-three-key-latin-american-countries Acesso em: 11 fev. 2020.

FACEBOOK. **Transparency.** Disponível em: https://transparency.facebook.com/government-data-requests. Acesso em: 11 fev. 2020.

FERRACANE, Martina. Restrictions to Cross-Border Data Flows: A Taxonomy. **Ecipe Working Paper**. n. 1, 2017. Brussels: European Centre for International Political Economy, 2017. Disponível em: http://popsdev.org/wp-content/uploads/2018/03/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf. Acesso em: 11 fev. 2020.

GOOGLE. **Transparency report**. Disponível em: https://transparencyreport.google.com/user-data/overview?hl=pt_BR&user_requests_report_period=series:requests,accounts,compliance;authority:;time:&lu=user_requests_report_period&legal_process_breakdown=expanded. Acesso em: 11 fev. 2020.

GUTIÉRREZ, Horacio E.; KORN, Daniel. Facilitando the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America, 45 U. **Inter-American Law Review**, 33. Miami: IALR, 2013. Disponível em: https://inter-american-law-review.law.miami.edu/wp-content/uploads/2014/03/Facilitando-the-Cloud.pdf. Acesso em: 11 fev. 2020.

Instituto Brasileiro de Defesa do Consumidor - Idec. **Autoridade de Proteção de Dados na América Latina**: Um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. São Paulo: Instituto Brasileiro de Defesa do Consumidor, 2019. Disponível em: https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina. Acesso em 10 fev. 2020.

KURTZ, Lahis; CARMO, Paloma; VIEIRA, Victor. **Perfil dos litígios envolvendo a internet no Brasil**: grupos econômicos e jurisdição. Belo Horizonte: IRIS, 2019. Disponível em: http://irisbh.com.br/publicacoes/perfil-dos-litigios-envolvendo-a-internet-no-brasil-grupos-economicos-e-jurisdicao/. Acesso em: 10 fev. 2020.

LINKEDIN. **Transparency reports**. Disponível em: https://transparency.twitter.com/en/information-requests.html. Acesso em: 11 fev. 2020.

MICROSOFT. **Transparency**. Disponível em: https://www.microsoft.com/en-us/corporate-responsibility/lerr. Acesso em: 11 fev. 2020.

PROTESTE. Conheça os aplicativos mais baixados no mundo em 2018. **ConectaJá**. https://conectaja.proteste.org.br/aplicativos-mais-baixados-de-2018/. Acesso em: 31 mar. 2020.

RODRIGUEZ, Katitza. **Comparative Analysis of Surveillance Laws and Practices in Latin America**. Necessary and Proportionate. Electronic Frontier Foundation, 2016. Disponível em: https://necessaryandproportionate.org/comparative-analysis-surveillance-laws-and-practices-latin-america. Acesso em: 10 fev. 2020.

SNAPCHAT. **Transparency**. Disponível em: https://www.snap.com/en-US/privacy/transparency/. Acesso em: 11 fev. 2020.

TWITTER. **Transparency report**. Disponível em: https://transparency.twitter.com/en/information-requests.html. Acesso em: 11 fev. 2020.

UNIÃO EUROPEIA. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**. Bruxelas, Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt>.Acesso em: 19 de fevereiro de 2020.