Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience

JACQUELINE DE SOUZA ABREU

Abstract: This paper adds to a growing scholarship that argues that the foundational conceptual cause for disputes between law enforcement and Internet Service Providers (ISPs) related to access to digital evidence lies in unique attributes of data and the challenge the internet poses to long-standing notions and frameworks of jurisdiction under international law. Its main purpose consists in showing how the Brazilian experience with cross border access to user data issues fits in and sheds light on this global puzzle, offering a perspective that has been missing in this international discussion. Based on review of scholarship and case law, it analyzes two important supreme court cases from the U.S. (United States v. Microsoft) and from Brazil (Declaratory Action of Constitutionality n. 51) to discuss arguments governments have relied upon to assert direct authority to compel the production of digital evidence (outside the MLAT system), the contentions made by ISPs, and reform proposals.

Keywords: Jurisdiction. Digital evidence. Data protection. MLAT.

1. Introduction

Facebook Brazil has been judicially challenging Brazilian court orders compelling communications content data from users; a national association of Brazilian technology companies recently filed a constitutional claim bringing up the issue to the Brazilian Supreme Court. Microsoft Inc. is in the midst of a judicial dispute with the Department of Justice of the United States because it is refusing to hand over data stored on servers in Ireland; the case has now reached the

Recebido em 3/4/18
Aprovado em 20/4/18

U.S. Supreme Court. On the surface, these cases are "battles" between law enforcement and Internet Service Providers (ISPs) over customers' communications data.[1] They might have policy implications for the protection of user privacy and cloud-computing businesses on a global scale.[2] At their core, however, these disputes constitute legal battles over jurisdiction. On the one hand, national governments claim to have authority to compel production of Internet communications data; and on the other hand, the ISPs challenge it.

There is a variety of causes for such jurisdictional battles. From a pragmatic perspective, there are most notably two. First, law enforcement's interest in as well as reliance and dependence on electronic data as evidence in criminal investigations has grown proportionately to the vast amounts of electronic data collected by ISPs (CLARKE et al., 2013, p. 53-77). Be it for legitimate purposes or for pure and abusive data greed,[3] governments undertake judicial actions to secure their access to the treasure chest. In this context, Mutual Legal Assistance Treaties (MLATs), which have traditionally established international procedures of cooperation among nations for evidence, but are notoriously slow and laborious, are at odds with the new routine needs of the "digitally efficient state"[4] to gather digital evidence stored in different parts of the world and held by multinational companies.

Second, data subjects have independent relationships with ISPs that are usually based on a minimum level of trust.[5] ISPs offer and sell services to customers claiming to do with their data only what they have committed to do in the Terms of Service. Since the Snowden revelations, protecting personal data from government surveillance has become more than a democratic value; it is a business asset and an element of commercial reputation.[6] Many companies are not willing to share their customers' "digital dossiers"[7] with the government in ways that would hurt the trust relationship they have with those customers. Thus, the companies take up the judicial fight against the expansion

[1] That is the general tone of the news coverage. See Apuzzo, Sanger and Schmidt (2015).

[2] See Daskal (2015a) and Schultheis (2015).

[3] See Schneier (2015, p. 78-87) for a general overview on how data collected by private companies ends up in the hands of the government.

[4] See Rushin (2013 apud WARREN, 2015, p. 302).

[5] See Westmoreland (2013) (arguing that third parties holders of information who have their own relationships of trust with data subjects bring another dimension to the international system of evidence sharing); and Donahoe (2016) (arguing that private companies now play an outsized role in setting parameters of privacy and access to information for their users).

[6] See Swire and Hemmings (2015, p. 11).

[7] Term borrowed from Solove (2002, p. 1.084).

of surveillance that might compromise this business model.[8]

This paper takes a theoretical perspective and looks at what enables the battlefield occupied by ISPs and law enforcement. It adds to a growing scholarship that argues that the foundational conceptual cause for disputes like those in the cited cases lies in unique attributes of data and the challenge the *digital* poses to long-standing notions and frameworks of jurisdiction. Its main purpose consists in showing how the Brazilian experience with cross border access to user data issues fits in and sheds light on this global puzzle, offering a perspective that has so far been missing from the international debate, which is dominated by U.S.-E.U. approaches. This paper is dedicated to contributing to the ongoing global discussion on the development of a new or the improvement of the current legal framework applicable to jurisdictional disputes in the context of cross border data requests.

2. A look at paradigmatic cases

Based on unilateral national legislation, governments have claimed authority to directly compel data production from companies offering services in their territory. By contrast, ISPs have refused to comply with such requests, by alleging that they are subject to jurisdiction of a second country and that there is international means to obtaining data – MLAT procedures; their challenges have taken up the issue to high national courts. This section will use two important cases from the U.S. and from Brazil to present the arguments governments have relied upon to assert their authority as well as the contentions made in courts by ISPs.

2.1. United States: the Microsoft Ireland case

Microsoft Inc. has been in a dispute with the U.S. Department of Justice (DoJ) over the disclosure of emails stored on a server in Ireland that are allegedly relevant to a drug trafficking investigation since December 2013. Microsoft contends that a U.S. warrant based on § 2.703(a) of the Stored Communications Act (SCA), compelling the disclosure of the communications, is invalid. The reasoning is that the information to be seized is not stored in U.S. territory, but rather in a Microsoft facility in Ireland; and therefore, Microsoft argues, seizing the information would constitute an extraterritorial search and seizure. A U.S. judge has no authority to authorize such a procedure in these circumstances. Instead, the company contends the DoJ must resort to the MLAT between the U.S. and Ireland. In contrast, the DoJ argues that the warrant, served on a U.S. based company that can access the data from the U.S., is not extraterritorial and therefore is perfectly valid.

The District Court sided with the DoJ. It found that "while [Microsoft's contention is] not inconsistent with the statutory language, [it] is undermined by the structure of the SCA, by its legislative history, and by the practical consequences that would flow from adopting it" (UNITED STATES, 2014a, p. 470). The court conceded that the statute is ambiguous as to whether the limitations on the territorial reach of a warrant issued under Rule 41 of the Federal Rules of Criminal Procedure (UNITED STATES, 2014b), which sets territorial

[8] See Rozenshtein (2018) (calling litigiousness a technique of resistance of "surveillance intermediaries").

limitations,[9] also apply to warrants issued under § 2.703(a) of the SCA.[10] That provision could be read to mean either that only procedural aspects of the warrant application processes are to be drawn from Rule 41, or that procedural as well as substantive rules (including the territorial limitations) must be derived from that rule (UNITED STATES, 2014a, p. 470).

In light of this textual ambiguity, the court turned first to a structural interpretation of the SCA. It discerned that the "warrant" specified in § 2.703(a) is actually a hybrid: part search warrant and part subpoena. The explanation goes as follows: the order is

> obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause. On the other hand, it is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents physically entering the premises of the ISP to search its servers and seize the e-mail account in question (UNITED STATES, 2014a, p. 471).

The subpoena-like character of § 2.703(a) warrants imports subpoena-like power to require the recipient to produce information in its possession, custody, or control, regardless of the location of the information (UNITED STATES, 2014a, p. 472).

Next, the court reasoned that practical implications make it unlikely that Congress intended to treat a § 2.703(a) warrant as a conventional warrant (UNITED STATES, 2014a, p. 475). According to the court, it is difficult to believe that Congress would want to limit the reach of a SCA warrant to data stored in the U.S. because (i) one could evade an SCA Warrant by simply giving false residence information and thereby causing the ISP to assign his account to a server abroad; and (ii) its execution would depend on MLATs, which are slow and laborious, subject to the requested country's discretion and laws; and sometimes even completely unavailable. The burden on the government would be substantial and law enforcement efforts would be seriously impended (UNITED STATES, 2014a, p. 474).

Finally, the court dealt with the presumption against extraterritoriality, which provides that when a statute gives no clear indication of an extraterritorial application, it has none. According to the decision, the concerns that animate the presumption are simply not present in instances at stake: "An SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored" (UNITED STATES, 2014a, p. 475). In conclusion, the court denied Microsoft's motion to quash, holding that "even when applied to information that is stored in

[9] "Rule 41 (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government: (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following: (A) a United States territory, possession, or commonwealth; (B) the premises – no matter who owns them – of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state" (UNITED STATES, 2014b).

[10] "A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure […] by a court of competent jurisdiction". 18 U.S.C. § 2.703(a) (UNITED STATES, 1948, p. 599).

servers abroad, an SCA warrant does not violate the presumption against extraterritorial application of American law" (UNITED STATES, 2014a, p. 477).

Microsoft appealed and the Second Circuit reversed. The court held that there is no indication that the U.S. Congress wanted the SCA to have extraterritorial application. Further, with regards to the "subpoena-like power of a SCA Warrant" argument, the court affirmed that Congress chose a term of art when it included "warrant" in the SCA, meaning that it did not intend to abandon the territorial limitations characteristically applied to this instrument (UNITED STATES, 2016a, p. 212-231). That said, the question turned on whether a warrant requiring Microsoft to produce data stored in Ireland that it can access from the U.S. was extraterritorial. The court reasoned that the focus of the SCA is the protection of user privacy. For that reason, the relevant act for the extraterritoriality analysis is where the act of invasion of privacy occurs. This conduct takes place when data is seized by Microsoft – *in casu*, from its servers in Ireland (UNITED STATES, 2016a, p. 220). Hence, the relevant act occurs outside the United States, making the warrant extraterritorial and therefore invalid. In the ruling, the court did not lose sight of the government's concerns about a decision that prevents U.S. law enforcement from reaching data stored abroad, but concluded that "these practical considerations cannot overcome the powerful clues in the text of the statute, its other aspects, legislative history, and use of term of art 'warrant,' all of which lead us to conclude that an SCA warrant may reach only data stored within United States boundaries" (UNITED STATES, 2016a, p. 221).

Unsurprisingly, the government appealed; but surprisingly, the U.S. Supreme Court agreed to review the case. As the parties' briefs[11] demonstrate, the focus of the discussion brought to the Court will again be the interpretation of the SCA as to the reach of the warrant: does it suffice that the ISP is U.S.-based to compel data it holds or does the requested data also have to be located in the U.S.? In the background of this discussion lies the potential conflict of laws situation in which Microsoft can be placed, if it has to comply with § 2703(a) warrants for data stored abroad. Disclosure of the emails could make Microsoft breach Irish Data Protection Law, which applies to the sought-after data, as several *amici curiae* highlight. The U.S. government tries to by-pass the MLAT, they further say.

The Supreme Court dismissed the case in April 2018 after the CLOUD Act was enacted. The new legislation will be discussed in section IV.

2.2. Brazil: the ADC 51

The difficulty in obtaining data held by ISPs for law enforcement purposes is not new in Brazil. In fact, the problem, which is faced routinely by Brazilian authorities, is very similar to that currently faced by the U.S. government, except for one complicating twist. ISPs' challenges to Brazilian court orders demanding data disclosure are based not only on the rationale that data is stored abroad, but also on the fact that the Brazilian subsidiary of the ISP does not control access to the requested information. ISPs claim that a U.S. warrant is necessary for the disclosure, because they are bound by U.S. law. Then, they refer to the MLAT. In opposition, law enforcement agents (and many courts) have argued that if the company – subsidiary or not – offers services, that is, makes business in Brazil, then Brazilian

[11] See United States (2018b).

law applies. The implication claimed – but disputed – is that Brazilian courts have authority to compel production of data held by these ISPs, without deference to the MLAT.

The most recent development in this dispute is a constitutional case. In late November 2017, the Federation of Associations of Brazilian Companies in Information Technology (ASSESPRO) filed a Declaratory Action of Constitutionality no. 51 [ADC 51] (BRASIL, 2018) with the Brazilian Supreme Court (STF), seeking a statement that Federal Decree no. 3.810 of 2001 (BRASIL, 2001) (the MLAT between Brazil and the U.S.) and arts. 237, II, and 780 and 783 (provisions related to letters rogatory) of the Codes of Civil and Criminal Procedure (BRASIL, 2015, 1941), respectively, are constitutional pieces of legislation and therefore must be applied by Brazilian courts. ASSESPRO and Facebook Brazil (in an amicus brief) argue that data controlled by foreign companies (Facebook Inc., Google Inc., Microsoft Inc., etc.) can only be obtained from the mother-companies (not with their Brazilian subsidiaries – Facebook Brazil, Google Brazil, Microsoft Brazil, etc.). They also argue that the U.S. companies cannot directly disclose content of communications to Brazilian law enforcement because U.S. law (the SCA) prohibits that conduct.[12] In light of that, the argument goes, the appropriate course is the diplomatic path. The underlying issue is that this has not been the position of many courts in Brazil,[13] which have instead charged huge financial fines, threatened legal representatives with imprisonment, and threatened suspension of the service, in order to force direct compliance.[14] ASSESPRO hopes this scenario will change after a ruling of the STF.

Central to the case will be the *Marco Civil da Internet* (BRASIL, 2014), the Brazilian Legal Framework for the Internet. Aside from regulating the procedure and establishing standards for disclosure of Internet metadata and private communications content in its arts. 7 and 10, the law passed in April 2014 provides that ISPs, which are engaged in any kind of data processing that takes places in the territory of Brazil, must abide by Brazilian law. According to art. 11, that is the case for "data collected in national territory and to the content of communications, when at least one of the terminals [devices] is located in Brazil" (BRASIL, 2014, our translation) and "even if the activities

[12] See Brasil (2018). Paragraphs 31-33 of ASSESPRO's initial brief filed on Nov. 28, 2017; p. 11-20 of Facebook Brasil's amicus brief filed on Dec. 5, 2017.

[13] See Brasil (2018). Paragraphs 24-28 of ASSESPRO's initial brief filed on Nov. 28, 2017, with extensive citation to relevant cases on paragraphs 61-89.

[14] See Brasil (2018). Paragraph 20 of ASSESPRO's initial brief filed on Nov. 28, 2017; p. 7-8 of Facebook Brasil's amicus brief filed on Dec. 5, 2017.

are carried out by a foreign-based legal entity, provided that it offers services to the Brazilian public or at least one member of the same economic group has an establishment in Brazil" (BRASIL, 2014, our translation).[15] Given the legislative choice of wording, there is no denial that the Brazilian law requires foreign companies to comply with Brazilian law when engaging in data processing in the country or treating data collected in the country. The persistent question is whether this means foreign companies are supposed to *directly* respond to data requests pursuant to Brazilian law, outside the MLAT and in spite of other countries' law.[16]

Before the enactment of the Marco Civil, the Brazilian Superior Court of Justice dealt with this question. In a money laundering investigation from 2013, which involved government officials and hence was presented originally at higher judicial level, Google Brazil, the Brazilian subsidiary of Google Inc., alleged "physical and legal impossibility" to comply with court orders from Brazilian judges mandating the disclosure of e-mails: "Google Brazil does not have access to the computers that store the sought-after data, which are located in the U.S. and are operated by Google Inc. – its controller – which is subject to U.S. law" (BARROSO; MENDONÇA, 2013, our translation).[17] To support its position, Google Brazil first and foremost distinguished itself from Google Inc.: Gmail users contractually bind themselves with Google Inc., which operates the email service and holds the data. In addition, it argued that Google Inc. was subject to the restrictions on disclosure set by U.S. law, and therefore could not share data with Google Brazil "even if the U.S. company wanted to". Indeed, the SCA prohibits disclosure of content to foreign governments without a U.S. warrant.[18] Finally, the subsidiary referred to the MLAT between Brazil and the United States, which

[15] An unofficial Portuguese/English comparative version of the text is available at: <https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf>. Acess: Aug. 24, 2018.

[16] In his testimony to the House Judiciary Committee on Cross Border Data Requests, Brad Smith, Microsoft's President and Chief Legal Officer, noted: "The Brazilian courts have long asserted the authority to compel U.S. tech companies to disclose the contents of users' communications to Brazilian law enforcement, even when the data is located in other countries. Recently, the Brazilian Government enacted new legislation that reaffirms this point" (UNITED STATES, 2016d, p. 3).

[17] Google Brasil's memorandum can be found as an attachment to the news piece *STJ determina quebra de sigilo de correspondência virtual de Gmail* [STJ determines disclosure of Gmail accounts] (MIGALHAS, 2013).

[18] As a default rule, the SCA prohibits ISPs from disclosing communications content, but exceptions are listed in 18 U.S.C. § 2.702 (b). Since "governmental entities", under the definition set by 18 U.S.C. § 2711(4) means U.S. governmental agencies, the carve-out for disclosure to government is interpreted not to cover *foreign* governments, which are then subject to the general prohibition. See Westmoreland (2014) (explaining the interpretation of the SCA that affects foreign governments).

provides the diplomatic way to obtain data through a U.S. warrant served on Google Inc.

The Superior Court of Justice rejected Google Brazil's allegations. It acknowledged the alleged "factual impossibility" for lack of direct access to the data. The court held that Google Brazil could not be found in contempt, because it indeed needed the collaboration of agents at Google Inc. to turn over the data. On the other hand, the Court concluded, "the alleged [legal] obstacle does not exist" (BRASIL, 2013, p. 2, our translation).[19] First, Google Brazil legally represents Google Inc. in Brazil. Second, "what is intended is the disclosure of messages sent and received by Brazilians in Brazilian territory related to crimes unquestionably subject to Brazilian jurisdiction" (BRASIL, 2013, p. 2, our translation).[20] Accordingly, "the fact that the data is stored anywhere else in the world does not make it foreign evidence, so as to give rise to the need to resort to diplomatic channels for transfer of the data" (BRASIL, 2013, p. 2, our translation).[21] Moreover, the Court stated, the "mere exchange of data […] between Google Inc. and Google Brazil, because it occurs inside the company, does not violate any protection over the secrecy of the data" (BRASIL, 2013, p. 2, our translation).[22] "[M]ere transmission of data between companies of the same economic group, with the exclusive end of turning it over to the competent judicial authority, in this case, the Brazilian one, does not do the smallest harm to a foreign country's sovereignty" (BRASIL, 2013, p. 3, our translation).[23] The Court also reasoned that "it cannot be the case that a company would establish itself in Brazil, explore its lucrative messaging service through the Internet – which is absolutely legal – but evade its obligation of complying with local laws" (BRASIL, 2013, p. 2, our translation).[24] For those reasons, the Court concluded, the Brazilian subsidiary would be fined daily until the data is turned over.[25]

It remains to be seen whether the Brazilian Supreme Court will follow this understanding.

3. A normative disruption: why jurisdictional battles over data arise

The ISPs' position is not absurd in either case mentioned above. The place where a company is incorporated is used to identify the jurisdiction it is subject to and the laws it has to observe under the international law principle of *nationality* (BURGENTHAL; MURPHY, 2013, p. 253). Moreover, under international law, location of evidence has functioned as a basis for identification of the

[19] Original in Portuguese: "O obstáculo oposto não procede".

[20] Original in Portuguese: "[o] que se pretende é a entrega de mensagens remetidas e recebidas por brasileiros em território brasileiro, envolvendo supostos crimes submetidos induvidosamente à jurisdição brasileira".

[21] Original in Portuguese: "o fato de esses dados estarem armazenados em qualquer outra parte do mundo não os transforma em material de prova estrangeiro, a ensejar a necessidade da utilização de canais diplomáticos para transferência desses dados".

[22] Original in Portuguese: "a mera transferência reservada – poder-se-ia dizer *interna corporis* – desses dados entre empresa contraladora [sic] e controlada não constitui, em si, quebra do sigilo, o que só será feito quando efetivamente for entregue à autoridade judicial brasileira, aqui".

[23] Original in Portuguese: "simples transmissão de dados, resguardado seu conteúdo, entre as entidades pertencentes ao mesmo grupo empresarial, com a exclusiva finalidade de entrega à autoridade judiciária competente, no caso a brasileira, não tem o condão de sequer arranhar a soberania do Estado estrangeiro".

[24] Original in Portuguese: "Não se pode admitir que uma empresa se estabeleça no país, explore o lucrativo serviço de troca de mensagens por meio da *internet* – o que lhe é absolutamente lícito –, mas se esquive de cumprir as leis locais".

[25] In September 2017, the company gave up of an appeal at the Brazilian Supreme Court. See Brasil (2017).

country that has jurisdiction over it and has oriented MLAT procedures.[26] In fact, these legal doctrines have guided the enactment and interpretation of laws regarding data disclosure in other countries,[27] and are at the core of the Budapest Convention on Cybercrime.[28] Against this backdrop, the governments' position both in the U.S. and in Brazil, which disregards the location of the evidence and of the headquarters of a company, respectively, is interpreted by commentators as "unilateral assertions of extraterritorial jurisdiction,"[29] as if these assertions were "anomalies". But are they really?

Traditional jurisdictional frameworks function in the physical world quite well: (i) location where the company is headquartered, as a reference point of the laws that it must observe, and (ii) the location of the evidence, as the decisive parameter of the country which has jurisdiction over that piece of evidence. But when the Internet and electronic data are involved, and specifically in the context of cross border data requests, the normative underpinnings that sustain these hooks are disrupted. Accordingly, it is remarkable how the disputes explored challenge these doctrines and battle for the ultimate decisive point of jurisdiction to lawfully compel the sought-after data. This section tries to explain how these jurisdictional disputes are made possible.

The jurisdictional disputes examined here spring primarily from the intrinsic characteristics of the *digital*. The global nature of the Internet is difficult to reconcile with the local system of laws and local enforcement authorities. Accordingly, disputes around electronic data requests are yet another example of how modern technology challenges traditional jurisdictional frameworks. This section will show how the characteristics of electronic data disrupt the rules that have guided the determination of jurisdiction, and the application of MLATs, enabling the conflicts seen above.

3.1. The multi-territoriality of data: authority to regulate data disclosure

Based on the Westphalian[30] notions of sovereignty and national self-determination, which granted to the nation state absolute control over whatever occurred within its territory, the most traditional basis for the assertion of *prescriptive jurisdiction*. A country's power to exercise authority to regulate persons, things, relations or interests by enacting laws is the *principle of territoriality*.[31] Accordingly, a country may regulate all civil and criminal matters within its borders.[32] All a country needs to regulate something is a *territorial hook*. In this sense,

[26] See Swire and Hemmings (2016, p. 699).

[27] See Maxwell and Wolf (2012, p. 13) (showing how in Japan and Germany the government cannot require a Cloud provider to access and disclose data, if it stores data in another country).

[28] See European Union (2001, p. 17) (providing that "A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29").

[29] See United States (2016b, 2016d).

[30] The term refers to the Peace of Westphalia and refers to the idea of an international order in which no state is permitted to impose rules on others. See Berman (2002, p. 320).

[31] See United States (1987), Shaw (2008, p. 646), Accioly, Silva and Cassella (2010, p. 321-322).

[32] Aside from that, other grounds for the assertion of prescriptive jurisdiction have been developed under international law and exceptionally permit regulation to reach matters *outside its borders*: the harmful-effects doctrine, the principle of nationality, the principle of universal jurisdiction, the protective principle are examples. See Buergenthal and Murphy (2013, p. 259). See also Shaw (2008, p. 652-673).

territorial borders set the area within which legal rules addressing certain matters apply.

Looking at electronic data as *things* that can be regulated, a country has power to exercise prescriptive jurisdiction over data, under the principle enunciated above, when the data is *within* its territory. The complicating factor is that bits can be stored anywhere; they are not ruled by the same physical constraints of atoms.[33] First, electronic data moves from place to place at a speed unparalleled by physical objects. Second, data is divisible: it can be broken into multiple parts and held in multiple locations.[34] Third, data packets can be replicated and transmitted at the same time to multiple places: one merely requires the physical infrastructure that enables access to the Internet to undertake such actions.[35] Consequently, electronic data can be called "multi-territorial" in a way that physical things cannot. The question posed is how this impacts the determination of prescriptive jurisdiction over electronic data.

For that investigation, it is helpful to briefly turn to the literature on Internet governance, since the emergence of *cyberspace* posed a similar challenge to jurisdiction's fundamental reliance on the principle of territoriality. If cyberspace is global and has *virtual* presence in any state in which access to the Internet is available, does that mean that each and every state can regulate matters within that cyberspace? The idea of a "virtual presence" was indeed the basis for assertion of jurisdiction when cases involving "unlawful" speech on internet platforms first emerged. In the now famous case *LICRA v. Yahoo*, for example, a French court found jurisdiction to hear a case against the U.S.-based Yahoo Inc., because auctions on the website were open to French bidders. French law forbidding sale of Nazi memorabilia applied, the court reasoned (FRANCE, 2000).

In a classic article from 1996, Johnson and Post categorically criticized the movement of nation-states to regulate online speech. They argued that "global computer-based communications", which "cut across territorial borders", created a new realm of human activity and undermined the feasibility and legitimacy of laws based on geographic boundaries (JOHNSON; POST, 1996). The key claim in their argument is that cyberspace is different: it has no territorial boundaries. It is independent of physical location: "messages can be transmitted from one physical location to any other location without degradation, decay, or substantial delay, and without physical cues or barriers that might otherwise keep certain geographically remote places and people separate from one another" (JOHNSON; POST, 1996, p. 1.370-1.371). For that reason, they argued, "[T]here is no geographically localized set of constituents with a stronger and more legitimate claim to regulate it than any other local group" (JOHNSON; POST, 1996, p. 1.375).

From this statement followed an argument that "real space jurisdictions" illegitimately assert control over cyberspace life. Nevertheless, coupling Johnson and Post's diagnosis that no local group has any stronger legitimacy to assert jurisdiction on

[33] See Daskal (2015b, p. 365-378) (discussing how data is "different"); Warren (2015, p. 301) (pointing out that transnational investigations involving global communications practices are full of contradictions); Gasser and O'Brien (2014, p. 15) (claiming that the "internationalization" of cloud computing is one of the 'risk vectors' of its regulation).

[34] See Daskal (2015b, p. 369). In the Microsoft case, for example, Microsoft alleges that non-content data related to the requested email accounts were stored in the U.S., whereas content was held in Ireland.

[35] See United States (2016c, p. 2) "the singular characteristic that defines our global cyber network is its universality".

cyberspace with the observations about electronic data actually sheds light on the disruption that enables the current "unilateral assertions of extraterritorial jurisdiction" in the context of cross border data requests. As stated, traditionally, prescriptive jurisdiction over a *thing* is derived from where the *thing* is situated. However, data's mobility, divisibility, location independence, and potential ubiquity make it, as anticipated, "multi-territorial".[36] The multi-territoriality of data engenders multiple assertions of jurisdiction to regulate data.[37] They are not illegitimate *per se*.

This has a direct impact on the companies behind these data flows. The definition of the jurisdictional scope of these data regulations can find ground in different principles of international law, depending on the government's interests at stake. While, traditionally, the "location of a company", as the place where the business is incorporated, well served to identify those who were subject to the laws of the country, this hook can be too narrow in light of the global impact of ISPs. By providing data services made available through the Internet and thereby operating data flows navigating worldwide, ISPs have an impact in many countries other than where they are incorporated. Thus, many countries aim to reach the ISPs through effects-based territorial hooks,[38] like the facts that a service is offered in the country through the Internet or that a user of the service is located there, for example. That explains Brazil's jurisdictional scope set in *Marco Civil* (BRASIL, 2014). In contrast, the principle of nationality can also be useful to set the scope of data regulation and go beyond territorial limits. In fact, that explains the US government's position as to the scope of the SCA: regardless of where Microsoft stores data, the company is U.S.-based and must comply with U.S. law.

The variety of laws which ISPs are suddenly subject to is the root of the tension in the cases studied. At issue in the Microsoft Ireland case, for example, is whether the SCA's applicability to U.S.-based companies is somehow affected by the fact that the data requested is stored abroad. For the U.S. government, the hook of the location of the company should remain unaffected by the location of the data. The District Court

---

[36] See Daskal (2015b, p. 326).

[37] See also Silva and Soares (2017, p. 241) (arguing that, because of internet's architecture, multiple nations may have interest in applying their laws based on various criteria – objective territoriality, passive nationality, national or local security, effects), Basso and Polido (2008, p. 445) (calling internet disputes *hard cases* because of the multiterritorial character).

[38] As Goldsmith (2000, p. 139) responded to critics of the attempts to regulate online speech, the basis for prescriptive jurisdiction, in these cases, is one known to international law: effects-based territorial jurisdiction. See also Lessig (1996, p. 1.404).

agreed without hesitation; the Second Circuit disagreed. Microsoft intends, by contrast, to set a limit to the application of that law based on the location of data. The company stresses the fact that Irish law is implicated when data is located in Ireland, a fact that cannot be ignored. In Brazilian cases, in turn, based on different triggers, both U.S. and Brazilian law are *prima facie* applicable to ISPs: U.S. law because the companies are U.S.-based; and Brazilian law because their services are provided in Brazil. The overlap already exists; the pending tension is how to deal with it.

The takeaway here is that it is crucial to seriously engage with the multiple jurisdictional assertions legitimately available under international law to regulate data and, more specifically, data disclosure.

3.2. The un-territoriality of data: authority to compel data regardless of location

Enforcement jurisdiction, the power to exercise authority to enforce laws and to punish noncompliance, is traditionally even more closely connected to the principle of territoriality than prescriptive jurisdiction. A judgement may be enforced against persons and assets within the country's territory, but never abroad in the absence of consent.[39] Because of this international law principle, there (usually) exists a gap between a nation state's power to regulate and its power to enforce. While a nation's ability to regulate may theoretically extend beyond territorial boundaries, under international law enforcement jurisdiction remains fundamentally constricted to a nation's own borders.[40] A court order from a judge in country A authorizing the collection of evidence physically located in country B can only be enforced if country B consents. Hence, A has to defer to B's jurisdiction and ultimate authority over the evidence.

The relevance of the location of evidence to determine any authority in the digital age has been questioned. Many have argued that the place where bits are located is normatively insignificant to the determination of the authority to compel data.[41] In fact, Daskal (2015b, p. 366-367) states at least three characteristics of data that support this point of view. First, data's mobility is rather arbitrary: an email sent from a US user to a US addressee might as well traffic through France without any knowledge and input of the users and entirely due to technical routing decisions. Second, data is usually stored in more than one server and broken in different parts, all potentially in different locations (DASKAL, 2015b, p. 368-369). Third, the processing of data is independent from location: the location of the actor handling or accessing the data can be disconnected from the location where it is stored (DASKAL, 2015b, p. 369-371). Her conclusion is that the "normative relevance of data's location" (DASKAL, 2015b, p. 329) is undercut. Indeed, if the main feature of the digital world – and of all the data it is

[39] See United States (1987) (providing that "A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state"). See also Rezek (1998, p. 161) (affirming that "only [the local state] may undertake restrictive actions towards people [in a certain territory], given that it holds the monopoly of the legitimate use of public power").

[40] See Nations Unies (1927, p. 18) (stating that "[N]ow the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention").

[41] See Kris (2015), Kerr (2014), and Krishnamurthy (2016, p. 4-5).

made of – is that it is not bound by territorial borders, location of data is an "unstable and often arbitrary determinant of the rules that apply" (DASKAL, 2015b, p. 329). In addition to data's inherent characteristics, the fact that the decision over where to store it is currently ultimately under the data holder's authority – and this may even include building and using data servers at the bottom of the ocean[42] – further alienate the normative relevance of the location of data to account for privacy interests of the data subject (DASKAL, 2015b, p. 373-374). Against this backdrop, and ironically when considering how "multi-territorial" data is, for purposes of establishing the legal rules that apply in a specific case, data is rather "un-territorial".[43]

Both the U.S. and Brazilian governments have capitalized precisely on this normative disconnect in the cases explored. In their assertions of authority to compel data, location of the bits is said to be irrelevant. The U.S. government considers that the location of data, in general, does not constrain the scope of applicability of the SCA and, in the specific case, does not constrain the authority to compel production of data stored abroad via a U.S. warrant. Meanwhile, Brazil rejects that the location of data ought to have any relevance in determining the rules that apply to a specific case setting. These assertions are not unreasonable, given the "un-territoriality" of data.

Relatedly, this tension shakes to its core the functionality of the MLAT process to deal with cross border data requests.[44] MLATs among nations originated in the 1960s to deal with the discontinuity between prescriptive jurisdiction and enforcement jurisdiction.[45] Since a nation's law enforcement officials are not entitled to cross borders and gather evidence located abroad, agents would go through the procedure set by the bilateral or multilateral agreement with the country where the evidence is located in order to collect the material relevant to a particular investigation or prosecution.[46] In this sense, the MLAT was formulated and currently functions under the assumption that the location of the evidence is and should be the reference point to jurisdiction over the evidence.

Yet, as anticipated, the relevance of this factor is precisely part of the issue. "Location of evidence" as the hook for the MLAT process,

[42] See Markoff (2016) (reporting on Microsoft's Project Natick, which tests the placement of server containers underwater).

[43] Term used by Daskal (2015b).

[44] See Bellia (2001, p. 49) and Krishnamurthy (2016, p. 4).

[45] The European Convention on Mutual Assistance in Criminal Matters was enacted in 1962 (EUROPEAN UNION, 1959). The first MLAT the US entered into came 11 years later and was celebrated with Switzerland. See Bellia (2001, p. 50-51).

[46] See Shaw (2008, p. 646) and Souza (2008).

historically, is meant to protect a country's territorial integrity from foreign law enforcement. However, companies that have control over data can have access to it by simply giving instructions to a computer. Indeed, it was highlighted by the magistrate judge in the Microsoft Ireland case that no deployment of U.S. officials abroad would occur. Hence, why should location of the evidence guide the authority to compel data for MLAT purposes? Most significantly, the insistence of the Brazilian courts in stressing how the requests made are inherently connected to Brazil – e.g. fact that the users involved are Brazilians or at least located in Brazil and that the evidence is necessary for the investigation of crimes occurred in Brazil – suggests that a different hook or set of hooks should be considered to replace location of data as determinant of authority to compel production of digital evidence.

MLATs come into play when the question of jurisdiction is solved. As Daskal (2015b, p. 394) points out,

> The MLAT system provides a mechanism for one government to formally request data subject to another sovereign's jurisdiction. It thus kicks in where jurisdiction ends. One still needs to answer the key underlying question: when and in what circumstances a sovereign can claim lawful jurisdiction over data, even if that data is physically located outside its territory and subject to foreign law?

That is precisely the question at issue in the Microsoft Ireland case. Adding into consideration the complication of the Brazilian cases, the question is: when and in what circumstances a sovereign can claim lawful jurisdiction over data, even if the ISP who controls access to the data is located abroad and subject to foreign law? Those are precisely the questions underlying the cases studied. The takeaway is that it is urgent to clarify the limits of jurisdiction and define a new trigger for the MLAT process – or any modern international cooperation system for data sharing – supported by reasons that *make sense* in light of the international conflicts it aims to avoid and principles it aspires to protect.

So long as the international community does not fix this problem, aspects of the global digital economy threaten to bridge the gap between prescriptive and enforcement jurisdiction that sustained the creation of MLATs in the first place – in an authoritarian form. When ISPs, as data holders, have persons or assets or simply operate within a country's territory, other tools for enforcement exist.[47] Fines and even arrests can be executed. Additionally, and most significantly, the

[47] On this capability, see Goldsmith and Wu (2006, p. 65-85).

service can be suspended. Governments control the "master switch"[48] as to the availability of Internet-based services in their countries. While enforcement can be frustrated if entities, assets, and persons are all located beyond the territorial reach of a country, an Internet service can be shut down, if it refuses to comply with local law.[49]

Brazilian cases are illustrative of these points. In attempts to compel collaboration from U.S. companies with law enforcement authorities, Microsoft has faced fines and arrests;[50] Facebook's Vice President for Latin America has been arrested;[51] and WhatsApp has been blocked three times.[52] These companies have resisted not for lack of legal basis for jurisdiction under Brazilian law, but by relying on their economic power and user popularity. Even though the country has suffered from practical shortcomings in its ability to obtain the data even after the implementation of these measures, the frustration of Brazilian authorities is so overwhelming, that more aggressiveness cannot be ruled out. At that point, coercion would not be constrained by practical barriers anymore. Alternatively, the situation might incentivize informal means of cooperation with foreign governments, which lack procedural guarantees, accountability, and transparency.[53]

4. Tailoring a normative fix: solving and preventing jurisdictional battles

The previous section showed that the relevance of (i) the location of the company, to ultimately determine the laws it must comply with, and (ii) the location of the evidence, to determine the limits of jurisdiction and the deference to the MLAT process, is under challenge in the digital age. From an international law standpoint, the natural follow-up question is: can these disruptions be neutralized? If so, how? This section briefly addresses these issues from a Brazilian perspective.

Many reform proposals have been presented to avoid jurisdictional battles like those in the Microsoft Ireland and in the Brazilian cases. Kerr (2015) has suggested, for example, a statutory amendment to the SCA, in order to clearly state the circumstances under which a U.S. warrant is valid to compel data stored overseas. If the company is U.S. based, it would have, as a general rule, to abide by a U.S. warrant requesting data, no matter where the data is located. When data is abroad though, data requests could only affect U.S. persons and people located in the U.S.. The CLOUD Act (UNITED STATES, 2018a), recently approved by the U.S. Congress, though slightly different, tries to achieve the same effect: it gives providers the opportunity to quash a data demand when they believe it would affect

[48] Term borrowed from Wu (2011). See also Lemos (2016) (correlating the WhatsApp blockades occurred in Brazil with Wu's idea of a master switch that threatens free speech). I would note, however, that Wu is mostly concerned with private companies who control information flows monopolizing media industries.

[49] See Goldsmith and Wu (2006, p. 65-85) (arguing that control can be exercised through intermediaries, physically located within the country, even when ISPs are headquartered abroad).

[50] See Bass (2015) (reporting about a Microsoft employee in Brazil who was threatened to be arrested by the Brazilian police because the company had refused to turn over Skype data stored in the U.S. that involved a Brazilian customer).

[51] Incident occurred in a recent development involving WhatsApp, see Watts (2016).

[52] About the first incident, see Sganzerla (2015). About the second time, see Greenwald and Fishman (2016). About the third episode, see Conger (2016).

[53] See Westmoreland and Kent (2015, p. 3) (reporting that "ad hoc arrangements with providers" are the most commonly used forms of international legal cooperation).

a non-U.S. person or violate another country's law.[54] Clearly, this new law tries to clarify the scope of jurisdiction at U.S. national level and to tackle the potential conflicts of law by offering guidance to U.S. companies and judges. It tries to solve the issue from a U.S. perspective.

The problem is of global character though. Commentators see the cases studied as a direct consequence of a larger problem: the laborious and slow MLATs.[55] That is specially the attitude towards the Brazil-type of cases, where the country claims to have authority to compel electronic data from a U.S. based company that stores data in the U.S.. MLAT's ineffectiveness and obscurity is said to fuel the frustration of law enforcement agents in foreign countries, and set the stage for the said "unilateral assertions of extraterritorial jurisdiction", the enactment of data localization laws, threats against employees or officers of local subsidiaries, among other things.[56] In view of that, many reform proposals aim to streamline the MLAT process.[57] They intend to modernize the process, such as by making it electronic, rather than paper-based, educating law enforcement in requesting countries, providing adequate staff in responding countries, among other measures.

While commendable, these efforts can only be a partial solution to the jurisdictional battles this paper highlighted. As stressed, the MLAT kicks in only when jurisdiction ends (WOODS, 2015, p. 4; DASKAL, 2015b, p. 394). Neither location of the headquarters and specially not the location of the evidence serve to set these jurisdictional limits convincingly and effectively. Furthermore, as seen in the cases studied, precisely the claim of direct authority to compel data – *in spite of the MLAT* – is made. The MLAT, or any other international system for purposes of sharing digital evidence, even if streamlined, can only work if clarity over the limits of jurisdiction exists and a new set of triggers is agreed upon. Therefore, the fix here is crafting this set of multi-factor rules. Brazilian case law on the matter, as discussed in the Google Brazil case mentioned here, already seems to appeal to a set of multiple factors in that sense (such as the location of the crime, the place of data collection, the citizenship of the accused, and the citizenship of the victim), instead of focusing on only one criterion (where data happens to be stored). While this approach and legal analysis is normatively sensible, it still has to be internationally recognized not to be called "unilateral". Progress has to be made in this direction.

---

[54] The Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 4943, 115th Cong.

[55] See Woods (2015), Clarke et al. (2013, p. 229), and the Portal <mlat.info>, set up by the ONG Access Now and dedicated to MLAT Reform.

[56] See United States (2016b) and Clarke et al. (2013, p. 226-229).

[57] See Woods (2015, p. 4), Swire and Hemmings (2016), Fidler (2015) and Hill (2015).

Alongside the MLAT reform proposals, some others have suggested the creation of "MLAT by-pass mechanisms". Under the Swire and Hemmings (2016, p. 5) proposal, for example, a system inspired in the U.S. Visa Waiver Program would award foreign countries that have a long-history of high-quality procedures for seeking evidence with an expeditious access to the requested data. Under the Daskal and Woods (2015) proposal, in its turn, the admission to an expedited access system through bilateral agreements would be conditioned on compliance with human rights standards: at a high level, looking at the country's surveillance laws, and in the specific case upon which the request is based.[58] The system would allow disclosure under foreign legal process if the case is "wholly domestic", that is, the data request is related to a local crime involving a local victim and a local suspect. Proposals of this kind include amending the SCA (DASKAL; WOODS, 2015; SWIRE; HEMMINGS, 2016, p. 51), in order to allow the disclosure of data held by U.S. companies to foreign governments, if the requirements are met. As flagged before, the SCA has acted as a "blocking statute" to disclosure of data to foreign governments as it prohibited it (UNITED STATES, 2016b; KRIS, 2015). The recently approved CLOUD Act incorporated these proposals and removed that prohibition for countries with whom the United States has entered into executive agreements – "qualifying foreign governments".

From a pragmatic standpoint, an "expedited access system" sounds promising. First, it seems sensitive to the concerns of multi-stakeholders. It seems to please the U.S. government, in the sense that it promotes good relations with foreign countries (SWIRE; HEMMINGS, 2015, p. 7). It seems well aligned with foreign governments' law enforcement goals, as it increases effectiveness (SWIRE; HEMMINGS, 2016, p. 17). It potentially discourages movements for data localization and raises legal certainty, for the relief of ISPs. Speaking to civil society groups, it promises to safeguard democratic values, privacy, and free speech by including substantive protections in the system.[59] Second, it builds on the traditional framework of international jurisdiction and treats the Microsoft Ireland and the Brazilian cases as "anomalies" ("extraterritorial assertions of jurisdiction"): chiefly, it non-explicitly takes advantage of the doctrine that the location of the headquarters of a company ultimately sets the laws it is subject to in terms of data disclosure. The carrot provided is a "by-pass mechanism", but the MLAT would remain the official channel for accessing data controlled by U.S. firms. This alternative may interest Brazilian authorities engaged in this debate and looking for a permanent solution.

From a theoretical perspective, however, the CLOUD Act is not perfect and cases as those experienced in Brazil may not go away. The law and the proposals in which it was based imply, even if inadvertently,[60] that the

[58] The project was partially endorsed by Krishnamurthy (2016) and Swire and Hemmings (2016, p. 51).

[59] But see Jaycox and Tien (2015) (criticizing the elimination of U.S. probable cause and the creation of a two tier worlds – those of "good" and "bad" Internet nations), Nojeim (2015a) (also criticizing the elimination of probable cause and judicial review protections for non-US data subjects), Nojeim (2015b) (arguing that the Daskal-Woods proposal should be revised to account for metadata disclosures) and Nojeim (2015c) (pointing out to the difficulties of establishing who decides which countries comply with human rights standards).

[60] See United States (2016b, p. 6) (showing intent to avoid "imperialism": "the U.S. has little justification in imposing [these] specific standards on foreign government access to data of non-citizens who are located outside the U.S."), Swire and Hemmings (2016, p. 57) (recognizing that "it would be somewhat arrogant to take the position that only a U.S.-style probable cause is 'reasonable' when seeking electronic evidence across borders").

ultimate authority to compel data held by U.S. based companies rests in the U.S.; that data held by U.S. companies in the U.S. can only be disclosed under the terms of U.S. law. They are premised on the idea that U.S. law may set the conditions of their operations not only in the U.S., but globally, by regulating the circumstances under which disclosure of data to foreign governments is allowed to take place. This includes having a country like Brazil enter into an executive agreement with the U.S. and being 'certified' by the U.S. authorities. Brazilian authorities may show discomfort with this U.S.-centric approach underlying the new system, even if from a pragmatic perspective it shows to be promising.

In this sense, even if they do not overlook, these frameworks downplay the normative disconnects that this paper highlighted. The assumption that *only* or even *ultimately* the location of the headquarters of a company establishes the laws it must abide by is normatively contradicted by the multi-territoriality of data and practically threatened by alternate enforcement measures. Rather ironically, the "wholly domestic" cases – to which the "expedited access processes" would be applicable – are exactly those where the foreign country's sovereign interests are at its maximum. U.S. law's legitimacy to regulate these cases is at its minimum. The fix here most likely to address the claims of foreign governments is not in the form of a "by-pass mechanism" dictated by U.S. law, but of a new internationally-recognized jurisdictional framework that deals with overlapping and/or conflicting laws from a neutral standpoint.[61] There is progress to be made in that direction.

5. Conclusion

Jurisdictional conflicts such as those materialized in the U.S. v Microsoft and ADC n. 51 (BRASIL, 2018) cases have emerged in courts because of traditional (and outdated) jurisdictional frameworks that are ill-suited for the digital age. The lack of a clear, satisfactory, and fair solution is a symptom of the problem and a proof of its urgency. Data's multi-territoriality originates from the multiple unilateral

[61] An effort in that sense can be found in Svantesson (2017) (calling for a paradigm shift that will move away from strict territoriality) and advancing a three-principle framework for the exercise of jurisdiction based on substantial connection, legitimate interests and reasonableness), La Chapelle and Fehlinger (2016) (arguing that the "institutional gap", created by the inability of the traditional modes of international cooperation to deal with the digital realities, be filled by multi-stakeholder cooperation toward transnational frameworks), for example.

regulations of data disclosure. At the same time, data's un-territoriality makes its location normatively inadequate for triggering international cooperation. All of this shows that a new framework has to tackle these disconnects. International and national law, scholarship and practice must be developed in this area.

This paper tried to insert the Brazilian perspective in this international debate, drawing attention to the state of Brazilian law and case law on the issue, which is important for the assessment of any reform proposals. Hopefully, the insights of this paper will further contribute to developing a successful framework to deal with these challenges.

Sobre a autora

Jacqueline de Souza Abreu é mestre em Direito pela University of California, School of Law, Berkeley, CA, Estados Unidos da América; mestre pela Ludwig-Maximilians-Universität, Munique, BY, Alemanha; coordenadora da área "Privacidade e Vigilância" no InternetLab, centro independente de pesquisa em direito e tecnologia, São Paulo, SP, Brasil; advogada, São Paulo, SP, Brasil.
E-mail: jacqueline.abreu@usp.br

Título, resumo e palavras-chave em português[62]

CONFLITOS DE JURISDIÇÃO POR PROVAS DIGITAIS, REFORMA DA COOPERAÇÃO JUDICIÁRIA INTERNACIONAL, E A EXPERIÊNCIA BRASILEIRA

RESUMO: Este artigo reforça o argumento de que a causa conceitual fundamental para disputas entre autoridades de investigação e provedores de aplicações de Internet relacionadas a pedidos d e quebra de sigilo de comunicações de usuários se deve a atributos únicos de "dados" e ao desafio que a Internet representa para tradicionais noções de jurisdição. Seu principal propósito consiste em mostrar como a experiência brasileira com questões de acesso transfronteiriço a dados se encaixa em e joga luz sobre tal quebra-cabeça global, perspectiva que tem faltado na discussão internacional sobre o tema. Com base em análise da literatura especializada e da jurisprudência, o artigo analisa dois processos judiciais – um dos Estados Unidos (*U.S. v. Microsoft*) e outro do Brasil (ADC n. 51) – a fim de discutir os argumentos de autoridades estatais para compelir a produção direta de provas digitais (fora do sistema de cooperação internacional), as alegações feitas por provedores e as propostas de reforma em nível internacional.

PALAVRAS-CHAVE: JURISDIÇÃO. PROVAS DIGITAIS. QUEBRAS DE SIGILO. PRIVACIDADE. MLAT.

[62] Sem revisão do editor.

Como citar este artigo

(ABNT)
ABREU, Jacqueline de Souza. Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience. *Revista de Informação Legislativa*: RIL, v. 55, n. 220, p. 233-257, out./dez. 2018. Disponível em: <http://www12.senado.leg.br/ril/edicoes/55/220/ril_v55_n220_p233>.

(APA)
Abreu, J. de S. (2018). Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience. *Revista de Informação Legislativa: RIL*, *55*(220), 233-257. Recuperado de http://www12.senado.leg.br/ril/edicoes/55/220/ril_v55_n220_p233

Referências

ACCIOLY, Hildebrando; SILVA, G. E. do Nascimento; CASELLA, Paulo Borba. *Manual de direito internacional público*. 18. ed. São Paulo: Saraiva, 2010.

APUZZO, Matt; SANGER, David E.; SCHMIDT, Michael S. Apple and other tech companies tangle with U.S. over data access. *The New York Times*, New York, Sept. 7, 2015. Available at: <http://www.nytimes.com/2015/09/08/us/politics/apple-and-other-tech-companies-tangle-with-us-over-access-to-data.html>. Access: Aug. 23, 2018.

BARROSO, Luís Roberto; MENDONÇA, Eduardo. Ref.: Inquérito n. 784/DF. *Luís Roberto Barroso & Associados*: escritório de advocacia, Brasília, 1º abr. 2013. Available at: <http://www.migalhas.com.br/arquivo_artigo/art20130418-02.pdf>. Access: Aug. 27, 2018.

BASS, Dina. The case that has Microsoft, Apple and Amazon agreeing for once. *Bloomberg*, New York, Sept. 2, 2015. Available at: <http://www.bloomberg.com/news/articles/2015-09-02/as-microsoft-takes-on-the-feds-apple-and-amazon-watch-nervously>. Access: Aug. 29, 2018.

BASSO, Maristela; POLIDO, Fabricio. Jurisdição e lei aplicável na internet: adjudicando litígios de violação de direitos da personalidade e as redes de relacionamento social. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Ed.). *Direito & internet*: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2008. v. 2, p. 441-487.

BELLIA, Patricia L. Chasing bits across borders. *University of Chicago Legal Forum*, Chicago, v. 35, p. 35-101, 2001. Available at: <https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1430&context=law_faculty_scholarship>. Access: Aug. 28, 2018.

BERMAN, Paul Schiff. The globalization of jurisdiction. *University of Pennsylvania Law Review*, Philadelphia, v. 151, p. 311-545, 2002. Available at: <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3208&context=penn_law_review>. Access: Aug. 29, 2018.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. *Diário Oficial da União*, Rio de Janeiro, 13 out. 1941.

_____. Decreto nº 3.810, de 2 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… *Diário Oficial da União*, Brasília, 3 maio 2001.

_____. Superior Tribunal de Justiça. Inquérito n. 784/DF. Requerente: J. P. Requerido: E. A. Relatora: Min. Laurita Vaz. *Diário da Justiça Eletrônico*, Brasília, 28 ago. 2013. Available at: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1226618&num_registro=201201075060&data=20130828&formato=PDF>. Access: Aug. 24, 2018.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, Brasília, 24 abr. 2014.

_____. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. *Diário Oficial da União*, Brasília, 17 mar. 2015.

_____. Supremo Tribunal Federal. Recurso ordinário em mandado de segurança n. 33.030/DF. Recorrente: Google Brasil Internet Ltda. Recorrido: União. Relator: Min. Ricardo Lewandowski. *Diário da Justiça Eletrônico*, Brasília, 13 set. 2017. Available at: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=312724526&ext=.pdf>. Access: Aug. 27, 2018.

_____. Supremo Tribunal Federal. Ação declaratória de constitucionalidade n. 51/DF. Requerente: Federação das Associações das Empresas Brasileiras de Tecnologia da Informação. Requerido: Presidente da República; Congresso Nacional. Relator: Min. Gilmar Mendes. *Diário da Justiça Eletrônico*, Brasília, 6 abr. 2018. Available at: <http://portal.stf.jus.br/processos/downloadPeca.asp?id=313506744&ext=.pdf>. Access: Aug. 24, 2018.

BUERGENTHAL, Thomas; MURPHY, Sean D. *Public international law in a nutshell*. 5. ed. St. Paul, MN: West, 2013.

CLARKE, Richard A. et al. Liberty and security in a changing world: report and recommendations of the president's review group on intelligence and communications technologies. *The White House*: president Barack Obama, United States, p. 53-77, Dec. 12, 2013. Available at: <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>. Access: Aug. 24, 2018.

CONGER, Kate. WhatsApp blocked in Brazil again. *TechCrunch*, [S.l.], Jul. 19, 2016. Available at: <https://techcrunch.com/2016/07/19/whatsapp-blocked-in-brazil-again/>. Access: Aug. 28, 2018.

DASKAL, Jennifer. The Microsoft warrant case: the policy issues. *Just Security*, New York, Sep. 8, 2015a. Available at: <https://www.justsecurity.org/25901/microsoft-warrant-case-policy-issues/>. Access: Aug. 23, 2018.

_____. The un-territoriality of data. *Yale Law Journal*, New Haven, CT, v. 125, n. 2, p. 326-599, Nov. 2015b. Available at: <https://www.yalelawjournal.org/article/the-un-territoriality-of-data>. Access: Aug. 23, 2018.

DASKAL, Jennifer; WOODS, Andrew K. Cross-border data requests: a proposed framework. *Lawfare*, Washington, DC, Nov. 24, 2015. Available at: <https://lawfareblog.com/cross-border-data-requests-proposed-framework>. Access: Aug. 24, 2018.

DONAHOE, Eileen. So software has eaten the world: what does it mean for human rights, security & governance?. *Just Security*, New York, Mar. 18, 2016. Available at: <https://www.justsecurity.org/30046/software-eaten-world-human-rights-security-governance/>. Access: Aug. 24, 2018.

EUROPEAN UNION. Council of Europe. *European Convention on mutual assistance in criminal matters*. Strasbourg: Council of Europe, 1959. Available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800656ce>. Access: Aug. 28, 2018.

_____. Council of Europe. *Convention on Cybercrime*. Budapeste: Council of Europe, 2001. Available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>. Access: Aug. 27, 2018.

FIDLER, Mailyn. MLAT reform: some thoughts from civil society. *Lawfare*, Washington, DC, Sept. 11, 2015. Available at: <https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society>. Access: Aug. 24, 2018.

FRANCE. Tribunal de Grande Instance de Paris. *La ligue contre le racisme et l'antisémitisme c. la société YAHOO!Inc*. 22 mai 2000.

GASSER, Urs; O'BRIEN, David R. Governments and cloud computing: roles, approaches and policy considerations. *Berkman Center for Internet & Society*, Cambridge, n. 2014-6, p. 1-42, Mar. 2014. Available at: <http://ssrn.com/abstract=2410270>. Access: Aug. 28, 2018.

GOLDSMITH, Jack. Unilateral regulation of the internet: a modest defense. *European Journal of International Law*: EJIL, [S.l.], v. 11, p. 135-148, 2000. Available at: <http://ejil.org/pdfs/11/1/508.pdf>. Access: Aug. 28, 2018.

GOLDSMITH, Jack; WU, Tim. *Who controls the internet?*: illusions of a borderless world. Oxford, UK: Oxford University Press, 2006. Available at: <http://jost.syr.edu/wp-content/uploads/who-controls-the-internet_illusions-of-a-borderless-world.pdf>. Access: Aug. 28, 2018.

GREENWALD, Glenn; FISHMAN, Andrew. WhatsApp, used by 100 million Brazilians, was shut down nationwide by a single judge. *The Intercept*, Washington, DC, May 2, 2016. Available at: <https://theintercept.com/2016/05/02/whatsapp-used-by-100-million-brazilians-was-shut-down-nationwide-today-by-a-single-judge/>. Access: Aug. 28, 2018.

HILL, Jonah Force. Problematic alternatives: MLAT reform for the digital age. *Harvard National Security Journal*: NSJ, Cambridge, Jan. 28, 2015. Available at: <http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/>. Access: Aug. 27, 2018.

HURLEY, Lawrence. U.S. Supreme Court to decide major Microsoft email privacy fight. *Reuters*, London, Oct. 16, 2017. Available at: <https://www.reuters.com/article/us-usa-court-microsoft/u-s-supreme-court-to-decide-major-microsoft-email-privacy-fight-idUSKBN1CL20U>. Access: Aug. 27, 2018.

JAYCOX, Mark; TIEN, Lee. Reforms abound for cross-border data requests. *Electronic Frontier Foundation*: EFF, San Francisco, Dec. 27, 2015. Available at: <https://www.eff.org/deeplinks/2015/12/reforms-abound-cross-border-data-requests>. Access: Aug. 29, 2018.

JOHNSON, David R.; POST, David. Law and borders-the rise of Law in Cyberspace. *Stanford Law Review*, Stanford, v. 48, n. 5, p. 1.367-1.402, May 1996. Available at: <http://firstmonday.org/article/view/468/389>. Access: Aug. 30, 2018.

KERR, Orin S. The next generation communications privacy act. *University of Pennsylvania Law Review*: Penn Law, Philadelphia, v. 162, p. 373-419, 2014. Available at: <https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1546&context=penn_law_review>. Access: Aug. 28, 2018.

_____. A statutory fix for the Microsoft problem: a tentative draft #1. *The Washington Post*, Washington, DC, Sept. 15, 2015. Available at: <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/15/a-statutory-fix-for-the-microsoft-problem-tentative-draft-1/>. Access: Aug. 28, 2018.

KRIS, David. Preliminary thoughts on cross-border data requests. *Lawfare*, Washington, DC, Sept. 28, 2015. Available at: <https://www.lawfareblog.com/preliminary-thoughts-cross-border-data-requests>. Access: Aug. 28, 2018.

KRISHNAMURTHY, Vivek. Cloudy with conflict of laws. *Berkman Center for Internet & Society*: Berkman, Cambridge, n. 2016-3, p. 1-13, Feb. 2016. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2733350>. Access: Aug. 28, 2018.

LA CHAPELLE, Bertrand de; FEHLINGER, Paul. Jurisdiction on the internet: from legal arms race to transnational cooperation. *Center for International Governance and Innovation*, Waterloo, n. 28, Apr. 2016. Available at: <https://www.cigionline.org/sites/default/files/gcig_no28_web.pdf>. Access: Aug. 28, 2018.

LEMOS, Ronaldo. Bloquear a internet está virando normal. *Folha de S.Paulo*, São Paulo, 9 maio 2016. Available at: <http://www1.folha.uol.com.br/colunas/ronaldolemos/2016/05/1769125-bloquear-a-internet-esta-virando-normal.shtml>. Access: Aug. 27, 2018.

LESSIG, Lawrence. The zones of cyberspace. *Stanford Law Review*, Stanford, v. 48, n. 5, p. 1.403-1.411, May 1996.

MARKOFF, John. Microsoft plumbs ocean's depths to test underwater data center. *The New York Times*, New York, Jan. 31, 2016. Available at: <http://www.nytimes.com/2016/02/01/technology/microsoft-plumbs-oceans-depths-to-test-underwater-data-center.html?_r=0>. Access: Aug. 27, 2018.

MAXWELL, Winston; WOLF, Christopher. A global reality: governmental access to data in the cloud: a comparative analysis of ten international jurisdictions. *Hogan Lovells White Paper*, [S.I.], p. 1-13, May 2012. Available at: <http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf>. Access: Aug. 27, 2018.

MIGALHAS. STJ determina quebra do sigilo de correspondência virtual ao Gmail. *Migalhas*, São Paulo, 18 abr. 2013. Available at: <http://www.migalhas.com.br/Quentes/17,MI176608,21048-STJ+determina+quebra+do+sigilo+de+correspondencia+virtual+ao+Gmail>. Access: Aug. 27, 2018.

NATIONS UNIES. Cour Permanente de Justice Internationale. Affaire du "Lotus". *Recueil des Arrêts*, [S.l.], n. 10, p. [1-61], 1927. Available at: <https://www.icj-cij.org/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf>. Access: Aug. 28, 2018.

NOJEIM, Greg. MLAT reform proposal: eliminating U.S. probable cause and judicial review. *Lawfare*, Washington, DC, Dec. 4, 2015a. Available at: <https://www.lawfareblog.com/mlat-reform-proposal-eliminating-us-probable-cause-and-judicial-review>. Access: Aug. 29, 2018.

_____. MLAT reform proposal: protecting metadata. *Lawfare*, Washington, DC, Dec. 10, 2015b. Available at: <https://www.lawfareblog.com/mlat-reform-proposal-protecting-metadata>. Access: Aug. 29, 2018.

_____. MLAT reform: who decides?. *Lawfare*, Washington, DC, Dec. 24, 2015c. Available at: <https://www.lawfareblog.com/mlat-reform-who-decides>. Access: Aug. 29, 2018.

OSULA, Anna-Maria. Accessing extraterritorially located data: options for States. *Nato Cooperative Cyber Defense Centre of Excellence*, Tallinn, 2015. Available at: <https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options%20for%20States_Anna-Maria_Osula.pdf>. Access: Aug. 27, 2018.

REZEK, José Francisco. *Direito internacional público*. 7. ed. São Paulo: Saraiva, 1998.

ROZENSHTEIN, Alan Z. Surveillance intermediaries. *Stanford Law Review*, Stanford, v. 70, p. 102-189, Jan. 2018. Available at: <https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/01/70-Stan.-L.-Rev.-99.pdf>. Access: Aug. 24, 2018.

SCHNEIER, Bruce. *Data and Goliath*: the hidden battles to collect your data and control your world. New York: W.W. Norton & Company, 2015. p. 78-87.

SCHULTHEIS, Ned. Warrants in the clouds: how extraterritorial application of the stored communications act threatens the United States cloud storage industry. *Brooklyn Journal of Corporate, Finance & Commercial Law*, New York, v. 9, p. 661-693, 2015. Available at: <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1033&context=bjcfcl>. Access: Aug. 24, 2018.

SGANZERLA, Taisa. WhatsApp in back on in Brazil. But why was it blocked in the first place?. *Global Voices*, [S.l.], Dec. 17, 2015, Available at: <https://globalvoices.org/2015/12/17/whatsapp-blocked-brazil-facebook-zuckerberg-rousseff/>. Access: Aug. 29, 2018.

SHAW, Malcolm Nathan. *International law*. 6. ed. Cambridge: Cambridge University Press, 2008.

SILVA, Alice Rocha da; SOARES, Filipe Rocha Martins. Conflitos entre regulações internas relativas à internet e o direito do comércio internacional: o papel da OMC perante o sistema de computação da nuvem. *Revista de Direito Internacional*, Brasília, v. 14, n. 1, p. 237-247, 2017. Available at: <https://www.publicacoesacademicas.uniceub.br/rdi/article/view/4599/pdf>. Access: Aug. 28, 2018.

SOLOVE, Daniel J. Digital dossiers and the dissipation of fourth amendment privacy. *Southern California Law Review*, Los Angeles, v. 75, p. 1.083-1.167, 2002. Available at: <http://www-bcf.usc.edu/~usclrev/pdf/075502.pdf>. Access: Aug. 24, 2018.

SOUZA, Carlos Affonso Pereira de; VIOLA, Mario; LEMOS, Ronaldo. *Understanding Brazil's Internet Bill of Rights*. Rio de Janeiro: Instituto de Tecnologia & Sociedade, 2015. Available at: <http://itsrio.org/wp-content/uploads/2015/11/Understanding-Brazils-Internet-Bill-of-Rights.pdf>. Access: Aug. 24, 2018.

SOUZA, Carolina Yumi de. Cooperação jurídica internacional em matéria penal: considerações práticas. *Revista Brasileira de Ciências Criminais*, São Paulo, v. 16, n. 71, p. 297-325, mar./abr. 2008.

SVANTESSON, Dan Jerker B. *Solving the internet jurisdiction puzzle*. Oxford, UK: Oxford University Press, 2017.

SWIRE, Peter; HEMMINGS, Justin D. Stakeholders in reform of the global system for mutual legal assistance. *Georgia Tech Scheller College of Business*, Atlanta, n. 32, p. 1-17, Nov. 2015. Available at: <http://ssrn.com/abstract=2696163>. Access: Aug. 24, 2018.

_____. Mutual legal assistance in an era of globalized communications: the analogy to the Visa Waiver Program. *Annual Survey of American Law*, New York, n. 71, p. 687-800, Jan. 2016. Available at: <https://annualsurveyofamericanlaw.org/wp-content/uploads/2017/04/71-4_swirehemmings.pdf>. Access: Aug. 24, 2018.

UNITED STATES. United States Code: title 18: crimes and criminal procedure (1948). *Government Printing Office*, June 25, 1948. Available at: <https://www.gpo.gov/fdsys/pkg/USCODE-2013-title18/pdf/USCODE-2013-title18.pdf>. Access: Aug. 27, 2018.

_____. Restatement, third, Foreign Relations Law of the United States (1987). *American Law Institute*, 1987.

_____. District Court for the Southern District of New York. Warrant to Search n. 13-MAG-2814; M9-150. Appellant: Microsoft Corporation. Appellee: United States. *Government Printing Office*, New York, Sept. 4, 2014a.

_____. Federal Rules of Criminal Procedure (2014). *Government Printing Office*, Washington, DC, Dec. 1st, 2014b. Available at: <http://www.uscourts.gov/sites/default/files/federal_rules/FRCrP12.1.2014.pdf>. Access: Aug. 27, 2018.

_____. Court of Appeals for the Second Circuit. Appellant: Microsoft Corporation. Appellee: United States. *Government Printing Office*, 2016a.

_____. House of Representatives Judiciary Committee. Statement of Jennifer Daskal. *House of Representatives Judiciary Committee*, Washington, DC, Feb. 25, 2016b. Available at: <https://judiciary.house.gov/wp-content/uploads/2016/02/jennifer-daskal-testimony-updated.pdf>. Access: Aug. 28, 2018.

_____. House of Representatives Judiciary Committee. Statement for the record by the honorable Michael Chertoff, co-founder & executive chairman of the Chertoff Group and former secretary of the U.S. Department of Homeland Security. *House of Representatives Judiciary Committee*, Washington, DC, Feb. 25, 2016c. Available at: <https://judiciary.house.gov/wp-content/uploads/2016/02/michael-chertoff-testimony.pdf>. Access: Aug. 28, 2018.

_____. House of Representatives Judiciary Committee. Written testimony of Brad Smith president and chief legal officer, Microsoft Corporation. *House of Representatives Judiciary Committee*, Washington, DC, Feb. 25, 2016d. Available at: <https://judiciary.house.gov/wp-content/uploads/2016/02/brad-smith-testimony.pdf>. Access: Aug. 28, 2018.

_____. The House of Representatives nº 4943 (2018). To amend title 18, United States Code, to improve law enforcement access to data stored across borders, and for other purpose. *Government Printing Office*, Washington, DC, Feb. 6, 2018a. Available at: <https://www.congress.gov/115/bills/hr4943/BILLS-115hr4943ih.pdf>. Access: Aug. 28, 2018.

_____. Supreme Court. Brief for petitioner United States v. Microsoft Corporation n. 17-2. *Reporter of decisions, Supreme Court of the United States*, Washington, DC, Apr. 17, 2018b. Available at: <https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf>. Access: Aug. 27, 2018.

WARREN, Ian. Surveillance, criminal law and sovereignty. *Surveillance & Society*, Australia, v. 13, n. 2, p. 300-305, 2015.

WATTS, Jonathan. Brazilian police arrest Facebook's Latin America vice-president. *The Guardian*, London, Mar. 1st, 2016. Available at: <https://www.theguardian.com/technology/2016/mar/01/brazil-police-arrest-facebook-latin-america-vice-president-diego-dzodan>. Access: Aug. 27, 2018.

WESTMORELAND, Kate. Trust us, we're the government: sharing evidence internationally. *The Center for Internet & Society*: CIS, Stanford, Apr. 29, 2013. Available at: <http://cyberlaw.stanford.edu/blog/2013/04/trust-us-were-government-sharing-evidence-internationally>. Access: Aug. 24, 2018.

_____. ECPA reform is not just a U.S. issue. *The Center for Internet & Society*: CIS, Stanford, Apr. 10, 2014. Available at: <http://cyberlaw.stanford.edu/blog/2014/04/ecpa-reform-not-just-us-issue>. Access: Aug. 27, 2018.

WESTMORELAND, Kate; KENT, Gail. Foreign law enforcement access to user data: a survival guide and a call for action. *The Center for Internet & Society*: CIS, Stanford, p. 1-27, Jan. 2015. Available at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2547289>. Access: Aug. 29, 2018.

WOODS, Andrew K. Data beyond borders: mutual legal assistance in the internet age. *Global Network Initiative*, Washington, DC, 2015.

WU, Tim. *The master switch*: the rise and fall of information empires. New York: Vintage Books, 2011.