Institute for Research on Internet and Society

Online secrecy, criminal investigations and international cooperation

Contributions to the Declaratory Action for Constitutionality 51/2017

Institute for Research on Internet and Society

Online secrecy, criminal investigations and international cooperation

Contributions to the Declaratory Action for Constitutionality 51/2017

Scientific Advisor
Fabrício Bertini Pasquot Polido

Project's coordinators
Lucas Costa dos Anjos
Luíza Brandão

Research coordinator
Odélio Porto Jr.

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

Translating and revision
Gustavo Rodrigues
Lahis Kurtz
Luíza Brandão
Victor Vieira

Graphic Project
André Oliveira

Cover
André Oliveira
Felipe Duarte

Layout
Felipe Duarte

Editorial Production
Institute for Research on Internet and Society

Finalization
Felipe Duarte

SUMMARY

1. Introduction 5

2. The internet and the new jurisdiction conflicts - Context 5

3. Clarification on the notion of jurisdiction, in particular "prescriptive jurisdiction" 7

4. Criteria for determining applicable law - An international perspective 9

4.1. The user location: the case Zippo Manufacturing 9

a. Zippo Manufacturing Company vs. Zippo Dot Com and the three-phase test 10

b. Announced obsolescence: why the Zippo case is outdated 11

c. Criteria other than contacts with user locating jurisdiction 11

4.2. The location of the servers: the case United States v. Microsoft Inc. (Microsoft - Ireland) 12

a. The US Department of Justice Claims to the Supreme Court 13

b. Microsoft's defense to the Supreme Court 15

C. The Clarifying Overseas Use of Data Act (CLOUD ACT) 16

4.3. The place where the company that provides the services was constituted (headquarters) 18

a. Favorable decisions to the location of the company's headquarters as a criterion for defining the applicable law 19

b. Contrary decisions to the location of the seat of the company as a criterion for determining the applicable law 20

5.MLATs - Difficulties of its Use and Possible Solutions 21

6.Intentional conceptual confusions: identification of users and anonymity 25

7.The articles 3, sole paragraph and 11 of the Brazil's Internet Bill of Rights 28

8.Protection of users' rights and fundamental safeguards 31

9.Respect for the due process of law 32

10.Argument of the headquarters of the company is not enough to solve the demand 34

11.Additional meadures to solve the issue 36

12.Modernization perspectives and the complementarity of international engagement of the three powers 39

13.Recomprehension of sovereignty and jurisdiction sharing 41

14.Conclusions 44

15.Bibliographic references 45

1. Introduction

This paper results from the request made by the Institute for Research on Internet and Society for admission as 'Amicus Curiae'[1], as well as the memorial filed in this condition, in order to assist the Federal Supreme Court in the assessment of the Declaratory Action for Constitutionality (ADC) n. 51, filed by the Federation of Associations of Information Technology Companies - Assespro Nacional. The purpose of the Action is to analyze the relevance of the Decree 3,810/2001, the Article 237, II of Civil Procedure Code, and Articles 780 and 783 of Criminal Procedure Code, in particular with regard to international legal cooperation for data collection measures of private communication between users of internet applications, aimed at companies with foreign headquarters and establishment.

Regarding the **thematic connection** between the expertise and institutional aims of the Institute for Research on Internet and Society- IRIS and the matters under controversy and constitutional repercussions presented by ADC 51/2017, it is important to emphasize that the intervention of IRIS as amicus curiae and third party is justified on the basis of the relationship of demand with substantive issues and procedures involved in the interface between international law and new technologies. Since 2015, IRIS studies have examined the key profiles and constraints of global governance of the Internet and aspects of jurisdiction, applicable law, recognition of foreign judgment and international legal cooperation, in relevant interdisciplinary analysis involving issues of new technologies, public and private international law.

Issues concerning compliance with legal cooperation mechanisms (e.g. rogatory letters, direct aid, mutual legal assistance) in cross-border internet disputes, and unconditional respect for fundamental rights in transnational civil proceedings are precisely those that inspire the scope and effectiveness of measures to obtain telematic data and the content of private communications between users of Internet applications abroad. These issues raise, as will be argued below, additional caution in the interpretation and application by the Federal Supreme Court of international and domestic standards. In this sense, IRIS gathered the subsidies presented for the decision of Declaratory Action of Constitutionality N. 51, in 11 items, presented here, in addition to the conclusions offered to the Federal Supreme Court.

2. The internet and the new jurisdiction conflicts - context

The initial request of ADC 51/2017 presents, among its argumentative axes, the premise that the headquarters of a company must be the main element of the jurisdiction's definition[2], especially in situations in which judiciary and auxiliary of justice

1 The role of the amicus curiae is essentially to express its opinion on causes of social relevance, general repercussion or whose purpose is quite specific, in a way the magistrate needs technical support. THEODORO, Humberto Jr. *Curso de Direito Processual Civil - Volume 1*. 56ª edição .Rio de Janeiro: Editora Forense, 2015. p. 410.

2 Alex Mills discusses the existence of three distinct types of jurisdiction: (i) "jurisdiction to prescribe or legislate", which refers to the limits of the autonomy of a State to legislate about of certain matter; (ii) "jurisdiction to adjudicate", which refers to the limits of the judiciary of a State, therefore, the limits of its jurisdiction to adjudicate cases involving subjects located abroad ; and (iii) "jurisdiction to enforce", which relates to the limits of the executive branch of the State responsible for enforcing the Law. In this case, the ADC 51/2017 petition refers to the the third type of jurisdiction mentioned by Mills, that is, the limits that exist for Brazil to enforce our domestic legislation in the foreign territory where the company is located involved in a process whose purpose is to obtain the content of private online communications.MILLS, Alex. *Rethinking Jurisdiction in International Law*. In: *The British Yearbook of International Law*, Vol. 84, No. I, 2014. p. 194-195. Available in: <https://goo.gl/dg9hvL> Accessed in 12/03/2018.

intend to obtain the content of private communications through online applications. However, for this premise to be properly evaluated, it is necessary to understand how the internet has affected the way in which states exercise their jurisdiction in the XXI century.

Firstly, it is clear that the internet cannot be merely an additional element to the debate on jurisdiction but a true component of fragmentation, which has challenged the classic international westphalian[3] model and traditional international cooperation designs.

The policy network *Internet & Jurisdiction*[4] - which has sought to promote debate on this issue with state actors, civil society, business and academia around the world - states that legal tensions between national legal systems, based on the principle of territoriality, emerging due to the cross-border nature of the internet, can be summarized in two main challenges[5]:

1. How to preserve the global nature of the internet while respecting national legal systems?

2. How to combat misuse and abuse on the Internet while guaranteeing the protection of human rights?

In the Proponent's view, these are precisely the fundamental issues behind the controversies raised by ADC 51/2017. At the same time that the mechanisms of criminal prosecution and law enforcement must be respected, the Brazilian State must simultaneously ensure that the solutions adopted do not ignore the transnational nature of the Internet. In addition, the fundamental rights of users must be respected, specifically the civil guarantees that are based on privacy, the protection of personal and telematic data, and the inviolability of confidentiality of private communications.

Thus, it is necessary to recognize that the current instruments of international legal cooperation - administrative and jurisdictional - are still inefficient and incomplete when compared to the demands' volume not only in Brazil, but also in other countries. This view is strengthened by the annual survey conducted by Symantec, a digital security company operating in many countries around the globe, which observed that 62 million people experienced cybercrime practices in Brazil in the year 2017[6]. From this data it can be inferred that there is at least a reasonable demand for access to data stored by

3 The Westphalian international model dates back to the Peace of Westphalia, established by the Treaties of Münster and Osnabrück, signed in October 1648 in Westphalia, Germany. These treaties were the instruments used to end the Thirty Years War, and resulted in the modern concept of "sovereignty", understood at the time as necessary for the survival of a State. Sovereignty, in this sense, is a concept both political and juridical, which confers on a State absolute power over everything and everyone in its territory, and according to this definition, every State would be equally sovereign and independent (principle of the sovereign equality of all States). GIANNATTASIO, Arthur. Roberto Capella. *O Direito Internacional entre Dois Pós-Modernismos: A Ressignificação das Relações entre Direito Internacional e Direito Interno*. In: *Revista Eletrônica do CEDIN*, v. 6, 2010, p. 42-90. Available in: <https://goo.gl/DCrJgT>

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

5 Ibid, p. 6.

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

application providers located abroad, since often the headquarters of these providers and data processing units and data centers are abroad.

To those elements is added the fact that Brazil is a large consumer market for online services, with 99 millions of monthly *Facebook* users[7]; 50 millions of monthly *Instagram* users, the second country in total numbers[8]; and 120 millions of *WhatsApp* users[9]. Part of the young Brazilian population also integrates a significant digital natives market, which characterizes Brazilian users as a huge repository of information and personal data.

In addition, it is reasonable to say that, in the historical context[10] of the negotiations and entry into force of the Brazil-United States Cooperation Agreement (incorporated in Brazilian legal system by Decree 3.810/2001), the instruments provided there were not planned in order to consider that the internet, the speed of its interactions and the large number of users would have impacts on the dynamics of cross-border litigation and processes with international connection in civil, commercial and criminal matters.[11]

3. Clarification on the notion of jurisdiction, in particular "prescriptive jurisdiction"

Jurisdiction, according to the meaning attributed to it by classical international law, "defines the limits of the power of the 'sovereign' coexisting, in particular, the scope of states' regulatory activities in international law"[12]. Its delimitation, however, includes three of its central dimensions, established according to a power to draw up and enforce the right within the territory of a State and addressed to its citizens and persons resident or domiciled there: prescriptive jurisdiction, adjudicatory jurisdiction and enforcement jurisdiction. This division, which is not hermetic or tight, considered the objective of delivering material rights, suits two distinct purposes: firstly, to situate the different levels of discussion related to internet litigation cases with international connection, as well as would be, in a broader relation, the analysis of questions of law applicable to pluriconnected cases[13], jurisdiction and international competence of national courts, and recognition of foreign judgments. Secondly, it makes possible to clarify the degree

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

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

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

10 "From a historical perspective, cross-border interactions were rare, and international legal cooperation tools were designed to handle these exceptions. However, on the open Internet, interactions across borders are becoming the new normal." CHAPELLE, Bertrand de La, FEHLINGER, Paul. *Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation.* In: *Global Commission on Internet Governance, Paper Series*: No. 28 - April 2016. p. 2. Available in: <https://goo.gl/PySHxo>

11 The Access Now is contrary to the current model of MLATs, and they advocate the urgent need for reform in such mechanisms. Criticism, in short, revolves around features such as the slowness of the process involved in the MLATs, as well as in the failure of the model to properly protect the privacy and information of individuals. *The urgent need for MLAT reform*. Access Now. 12/09/2014. Available in: <https://goo.gl/dcqCWi>. *How to fix MLATs* — and a path toward resolving jurisdictional issues. Access Now. 23/05/2017. Available in: <https://goo.gl/JCNv5i>. On this issue, InternetLab also argues in its opinion to the United States Supreme Court that reforms to the MLATs model currently being used are needed to better fit the current international scenario. Available in: <https://goo.gl/V5htVv>. p. 31-37.

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

13 The term "pluriconected cases" or "cases with an international connection" are accepted here, as traditionally adopted in private international law, to designate a set of facts, situations and legal relations containing elements of transnationality, linked to different legal systems in contact. About that, cf. POLIDO, Fabrício B. P. *Direito Internacional Privado nas Fronteiras do Trabalho e Novas Tecnologias*: ensaios e narrativas na era digital. Rio de Janeiro: Lumen Iuris, 2018, p.97 e ss.

of complexity surrounding cases in cyberspace.

In the case *Microsoft Ireland Vs. USA*, on USA Supreme Court, as well as in the one presented in Declaratory Action for Constitutionality N. 51 (unique number 00144965220171000000), the term "jurisdiction" refers specifically to its prescriptive aspect related to the prediction by States of substantive laws applicable in certain circumstances to regulate events in their territory, with their nationals or even whose effects they may feel.[14] In this sense, the expression may also be interpreted, as applied to private international law, as "applicable law" or "substantive jurisdiction"[15].

Prescriptive jurisdiction thus reflects the power of the State to legislate and materially regulate the facts, situations and legal relations that manifest themselves in its territory, and exceptionally outside it, as in criminal, tax, antitrust, environmental and anti-corruption matters. As will be examined, Article 11 of the Brazil's Internet Bill of Rights, for example, contemplates standards with factual supports submitting certain legal relationships involving legal and natural persons to the **substantive regulation** of Brazilian law, nothing referring in turn to "adjudicatory jurisdiction", i.e. to the power-judge of the Brazilian courts; this area, specifically, would be subject to questions of international jurisdiction, as regulated by treaty norms and conventions and internal procedural rules (see Article 13 on the determination of civil jurisdiction and Articles 21 and others of the Civil Procedural Code of 2015 on the rules of international jurisdiction of the Brazilian courts)[16].

At this stage of procedural maturity in Brazilian law and in the handling of litigation brought before higher courts - STF and STJ, it would be inadmissible to confuse issues of applicable law and international jurisdiction for dispute settlement and solution of pluriconected Internet cases[17].

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

15 Ibidem.

16 About this subject, cf. POLIDO, Fabrício B.P. Comentários aos arts. 21-40. In: STRECK, Lenio Luiz; NUNES, Dierle; CUNHA, Leonardo C. (org.). *Comentários ao Código de Processo Civil*. 2. ed. São Pau lo: Saraiva, 2017. p. 73-108 (examining aspects of the international jurisdiction of the Brazilian court and regimes and mechanisms of international legal cooperation in the Brazilian Civil Procedure Code).

17 This, however, does not appear to be the recent approach of the STJ's judgment, particularly as to the confusion between applicable law, jurisdiction and international legal cooperation, including with questionable "exemption" from acts of mutual legal assistance and cooperation, as if they were optional for the Brazilian judicial and administrative authorities. About that, cf. critically, STJ, RMS 44.892/SP, Rel. Ministro Ribeiro Dantas, Quinta Turma, acórdão de 5 de abril de 2016, DJe 15.04.2016 (*"4. Because it is established and operating in the country, the multinational legal entity necessarily submits to Brazilian laws, which is why it seems unnecessary the international cooperation to obtain the data requested by the court"*); STJ, Recurso em Mandado de Segurança n. 55.109/PR, Rel. Min.Joel Paciornik, acórdão de 17.12.2017 (MPF vs. Yahoo!, case *Castanheira-Brasil 247*), maintaining a thesis that the breach of confidentiality of telematic data kept abroad, such as e-mail communication and social networks, is independent of international cooperation procedures. If this were the only argument based on the headquarters of the company (Internet industry), why would it not be possible to admit the same "waiver of cooperation" for a Brazilian subsidiary of a financial institution in Spain (eg Santander) is required to disclose / provide / deliver bank data of a Brazilian national or resident to a current account held in an overseas branch? Just as bank data and confidentiality are sensitive in the course of civil / criminal litigation, telematic data should receive the same protection treatment.

4. Criteria for determining applicable law - An international perspective

Chapelle and Fehlinger state that there are at least four territorial factors determining the applicable law to a particular case involving the internet[18]:

1. The location of the user;
2. The location of the servers that store the data;
3. The place where the company providing the services was set up (head office);
4. And, potentially, the location of the actors who perform the domain name registrations (.com; .org; .net; .br; among others);[19]

Thus, the difficulties in choosing what should be the determining criterion of applicable law, - besides jurisdictional issues - in cases involving information technology companies, have not been exclusive to the Brazilian Judiciary. From these criteria, different court decisions have been handed down by state courts around the world. In this sense, we will explain how certain judges from other countries used criteria 1 to 3, the most recurrent ones, to determine the jurisdiction applicable to a particular case. In this way, we hope to demonstrate how focusing on one of the criteria can lead to diverse legal outcomes, and thus better instruct the judgment of the ADC 51/2017.

4.1. The user location: the case Zippo Manufacturing

Among the most celebrated cases in the debate on establishing jurisdiction in relationships involving the Internet is the Zippo Manufacturing Company vs. Zippo Dot Com[20]. Still in the late 1990s, this demand offered some avenues for the till then uncommon issues, such as determining where the jurisdiction for an internet dispute is. The Pennsylvania district court, which issued the ruling, divided Internet activities into three types: active, passive, and interactive.

According to the established precedent, an **active** defendant would be one who deliberately makes extensive use of the internet, for example, by entering into contracts with residents of another jurisdiction, and such contracts require the repeated transmission of computer files over the internet. In such cases, the defendant was susceptible to the jurisdiction of the places he deliberately affected. A **passive** site, in its turn, would be merely informative and did not solicit or expect activities in and from the places it reached; its operators could not be brought to trial in those places.

The middle ground would be the **interactive** site. In these cases, the precedent set out herein was intended to examine the level of interactivity and commercial nature of the information exchange occurring on the site in order to determine how reasonable and expected it would be for site creators to be processed at that place.

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

19 In Brazil, the responsible for the domains register of the ".br" is the *Registro.br*, executive board of the *Brazilian Network Information Center*- NIC.br. Available in: <http://www.nic.br/quem-somos/>

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

The Zippo case test, although clear and simple, dividing the Internet sites into three categories and allowing the jurisdictional question to be decided on the basis of these places, is today an outdated method, as we intend to demonstrate. Through the complexity of established relationships in the global computer network, as well as the growth of interactions between providers, users and courts of different jurisdictions, this test has been insufficient for the current cross-border Internet issues.

a. Zippo Manufacturing Company vs. Zippo Dot Com and the three-phase test

Zippo Manufacturing was a corporation form Pennsylvania with its main business location in the county of Bradford, where it manufactured "Zippo" cigarette lighters. Its counterpart, Zippo Dot Com was headquartered in Sunnyvale, California. It operated a website and a news service, for which it obtained the exclusive right to use the domain names "zippo.com", "zippo.net" and "zipponews.com". The Zippo Dot Com website contained information about the company, ads and an application for its news service, which offered access to different newsgroups online. The application assigned the subscriber a password, which allowed him to view and/or download the messages stored on his California server from the newsgroup corresponding to his signature.

All Zippo Dot Com offices, employees and servers were located in California, without any activity in Pennsylvania, except contact with potential clients residing in that state (approximately two percent of the total of 3,000 of company subscribers). The basis of the trademark allegations would be the use of the word "Zippo" by Zippo Dot Com in the domain names it held at various locations on its website and in the title of Internet newsgroup posts by Zippo Dot Com subscribers, which could cause confusion in their consumers.

The judgment in this case proposes a three-step test to determine whether the exercise of jurisdiction over a non-resident defendant (in the state of the proceedings) is appropriate: 1) the defendant must have sufficient "minimum contacts"; 2) the claim made against the defendant should arise from such contacts; and 3) the exercise of jurisdiction should be reasonable. That is, there are minimum contacts if the defendant purposely established it with the state of the forum.

In addition, defendants who extend beyond one state and create continuous relationships and obligations to the citizens of another state would be subject to the regulation and sanctions of another state as a result of their commercial actions. Reasonableness, however, stems from the fact that the defendant's conduct and his connection to the state of the forum are such that he should reasonably expect to be brought to court there. This would protect defendants from being forced to respond for their actions in a foreign jurisdiction based on random, fortuitous or virtually non-existent contacts.

In addition, defendants who extend beyond one state and create continuous relationships and obligations to the citizens of another state would be subject to the regulation and sanctions of another state as a result of their commercial actions. Reasonableness, however, stems from the fact that the defendant's conduct and his connection to the state of the forum are such that he should reasonably expect to be

brought to court there. This would protect defendants from being forced to respond for their actions in a foreign jurisdiction based on random, fortuitous or virtually non-existent contacts.

b. Announced obsolescence: why the Zippo case is outdated

The Zippo test worked well initially, especially in that context of early network expansion, with sites that were clearly active within one jurisdiction, or totally passive and informative in another, with no element of interactivity. However, regarding the demands that had to deal with the increasing interactivity of the networks, there were few parameters for the objective basis of the judicial decisions.

The Zippo test also adopted a one-size-fits-all approach to all online disputes, which grew in form, nature and complexity: breaches of contractual clauses, privacy, advertising, hacking or misappropriation of data, copyright infringement, debt collection , among other specificities that should be considered beyond the levels of interaction between provider and user.

Another problem with Zippo's scale of interactivity, from active to passive, is that it can falsely describe the nature of the Internet and information and communication technologies, which may be quite different from each other. Each of these technologies is nowadays employed differently and requires its own jurisdictional analysis, given its technical and operational specificities. In addition, many of the disputes involving the internet go beyond the classic and tripartite classification of the Zippo case. Invasions and breaches of privacy, for example, may arise without the involvement of a website. These issues highlight the obsolescence of the Zippo case.

c. Criteria other than contacts with user locating jurisdiction

Currently, when courts are faced with some exceptional disputes, it makes more sense to analyze whether a provider has specifically targeted a particular user or jurisdiction in its action. Particularly in cases of defamation, for example, the test by means of this direction fits adequately to the solution of the fact, as it is possible to notice in Calder v. Jones[21], in which case the US Supreme Court allowed a lawsuit against a newspaper to be taken to the author's state of residence when the newspaper actively visited that state, conducted searches there and published its report knowing its effects would be greater at that location.

The case Sioux Transportation v. XPO Logistics[22], in turn, involved an alleged defamation in two online posts after a commercial dispute between the two companies. It was argued that Sioux had few activities in Arkansas, the home state of XPO, which would make it unfeasible for the jurisdiction of its courts. XPO argued that Sioux's postings, responding to XPO's posts, counted as deliberate contacts with Arkansas, which would support the exercise of its jurisdiction.

21 CALDER, Petitioner, v. JONES, Respondent. Nº. 82-1401. *Appeal from the Court of Appeal of California*. 20/03/1984. Accessed in: 26/03/2018. Available in: <https://goo.gl/wff9c2>

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

Instead of using the Zippo test, the court critically examined this precedent and found it inappropriate for the Internet today:

> 'The internet has undergone tremendous change since Zippo was decided in 1997', stated the court. 'Cloud computing has eliminated the need for downloading files in many situations, location-based technology has made online interactions that formerly existed only in cyberspace more closely tied to specific geographic locations, and the level of user interaction with websites has exploded with social media. All of this calls into question the modern usefulness of the Zippo test's simplistic tri-parte framework: The transmission of computer files over the internet is perhaps no longer an accurate measurement of a website's contact to a forum state.'[23]

4.2. The location of the servers: the case United States v. Microsoft Inc. (Microsoft - Ireland)

The US/Microsoft case (also known as "Microsoft Ireland") was brought to the US Supreme Court in 2017 and is expected to be tried in June 2018[24]. It will seek to answer if a warrant issued with based on the standards of the Stored Communication Act (SCA)[25], would oblige US companies to provide information under their control, but which are stored outside the country, specifically in data centers and data centers located in Ireland.

The dispute began in 2013 when a federal court (Southern District of New York) granted a warrant, based on Paragraph 2703[26] from the *Stored Communications Act* (SCA) of 1986. It aimed to obtain, by investigative authorities, the content of emails and associated data from a Microsoft user suspected of drug trafficking. After this decision, the company provided only the metadata related to the user account, because they are stored in the US. However, Microsoft claimed that it could not provide the content of the emails, because such information was located on a server in Ireland, and that SCA's rules would have no extraterritorial application.

The company's refusal to provide the email content was not upheld by the first instance court, which convicted Microsoft for disobeying a civil contempt order.[27] The claimed appealed to the United States Court of Appeals for the Second Circuit, which upheld the appeal, stating that: (1) SCA was silent as to its extraterritorial scope and

23 Ibid, em tradução livre.

24 Translator's note: at the time this paper was originally written, this case was expected to be judged in 2018. However, the following *Cloud Act,* american law that deals with extraterritorial data collection, approved after this paper was published, made the US Supreme Court end the case, with no solution.The issues discussed, however, remain interesting to be observed.

25 The *Stored Communication Act* is the Title II of the *Electronic Communications Privacy Act* (ECPA) ,approved in 1986. The EPCA sought to update the protection norms to private communications made through computers and other electronic means of communication. US DEPARTMENT OF JUSTICE. *Justice Information Sharing - Electronic Communications Privacy Act of 1986 (ECPA)*. 30/07/2013. Accessed in: 01/03/2018. Available at: <https://goo.gl/hdv2on>

26 This section protects privately stored electronic communications from being accessed indiscriminately by public authorities, establishing criteria such as warrant.18 U.S. Code § 2703 - Required disclosure of customer communications or records. Accessed in: 01/03/2018. Available in: <https://goo.gl/ojNv2A>

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

should, therefore, be interpreted restrictively, as already established in Supreme Court jurisprudence[28]; and that (2) the relevant territorial element to determine what the scope of the warrant would be to verify where the requested data was stored. Thus, a warrant issued in the US and seeking data in Ireland would eventually operate in that country, thus being an extraterritorial application of the law.[29]

a. The US Department of Justice Claims to the Supreme Court

After the second instance trial, the Department of Justice (DoJ) questioned the interpretation given to the Stored Communications Act of 1986 by filing an appeal with the Supreme Court (judicial review), which accepted the case in October 2017. Considering the relevance of the case to the understanding of constitutional repercussions in ADC 51/2017, pending judgment by the Brazilian Supreme Court, the following lines are intended to clarify some relevant points related to the determination of jurisdiction.

The DoJ sustains in its merits brief[30] that Section 2703 of the SCA of 1986 regulates the disclosure/breach of secrecy of the electronic information and that this act must occur in the territory of the USA, and not in Ireland. Thus, access to the server located in another country would constitute "mere accessory conduct", which would not be the main object of regulation of said law. To support this point, the DoJ mentions that the term "disclosure" is often used throughout the normative text, and that the historical analysis of SCA's legislative process would also focus on the act of display/disclosure rather than on the act of storage. Similarly, the DoJ adds that Microsoft could even comply with the warrant through actions that occur exclusively in the US[31], through its data management software.

In addition, the Department of Justice seeks to rebut the Court of Appeals' interpretation that Microsoft Inc., in complying with a warrant of secrecy breach of electronic communication, is committing an extraterritorial privacy violation. The appeal was based on the idea that Microsoft would act as a government agent seizing data stored in foreign jurisdiction.

Contrary, DoJ claims that Microsoft does not act as a government agent because it would only have access to information stored in its own files. And it adds that, even if one could be considered as a government agent, the act of accessing the server located abroad could not be considered an extraterritorial seizure[32], because the data are already on the custody and control of the company. And that would not even be configured as an extraterritorial search, in the sense of a violation of privacy considered reasonable[33], because there is no violation of privacy in relation to the act of transferring data of its servers from one country to another, something that the company already does routinely

28 See the cases *United States v. Morrison;*, *Kiobel v. Royal Dutch Petroleum Co.;* and *RJR Nabisco v. European Community*.

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

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

31 Actions that Microsoft representatives would execute in order to access the company's server and transfer the requested data to the authorities.

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

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

to enable its services. Thus, even if a privacy breach occurs, such conduct would be led by the governmental authority in the US territory at the time the data content is displayed.

The DoJ states that if the locus of the data prevails as a determining criterion of jurisdiction, this understanding will be detrimental to the investigative and judgment capabilities of the US authorities. As the location of the data is decided exclusively by the company, an economic bias decision could render the forecasts of the Stored Communications Act unusable, even if the fact investigated involves communication between two citizens residing in the United States. In addition, DoJ points out that other business models could be harmed if data location theory were adopted, such as the case of Google Inc., which can store data from a single user on several servers around the world, even distribute storage for a single email on different servers, with text archived in one location and attachments in another.

It adds that the mechanisms of international legal cooperation established in MLATs would not be an effective alternative. First, because these agreements are not universal, having the US signed MLATs with less than half of all countries in the world. Second, because the process, in most cases, is: (1) slow, and may take months or years; and (2) uncertain, since the receiving State has a certain discretion[34] to refuse it. And (3), because an online service provider may have the practice of constantly changing the location of users' data, making it difficult or even impossible to determine to which country the request for cooperation should be forwarded at a given time[35].

The DoJ also contends that the application of SCA's Paragraph 2703 respects the international treaties to which the US is a signatory. The Budapest Convention on Cybercrime, in its art. 18, settles that states parties should empower their competent authorities to require a service provider to deliver computer data on their possession or control.[36]

The DoJ claims, finally, that several countries do not restrict their ability to demand digitally stored data in another jurisdiction, citing a comparative study of Maxwell & Wolf, 2012. This research states that, among the United States, Australia, Canada, Japan and other six European countries, only two of them establish, in some cases, the physical location of the data as a criterion limiting the access of authorities to electronic information.[37] And, for the other countries of the study, the requirement of breach of confidentiality of data located abroad is allowed as long as there is some element that connects the case to the jurisdiction of the applicant country, such as the presence of the company in its territory.

---

34 It should be added that the aforementioned discretion is not limited to the mere arbitrary decision of the receiving State of the request - refusal is possible in cases where compliance with the request violates the Public Order of the receiving State. In this sense, it enunciates the Article V, 3, of Decree nº 3.810/2001: "Requests shall be executed in accordance with the laws of the Requested State, unless otherwise provided in this Agreement. The method of enforcement specified in the request shall, however, be followed, except in respect of the prohibitions provided for in the laws of the Requested State". Decreto nº 3.810, de 2 de maio de 2001. Available in: <https://goo.gl/oiE1G3>

35 It is important to emphasize that in Private International Law, there are mechanisms to sanction or dissuade the indiscriminate choice of forum, or the displacement of jurisdiction with elision or fraud to the law. In case of fraud to the law, when detected as conduct of the parties, it leads to disregard of applicable foreign law.

36 "Article 18 – Production order.Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a)a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.". CONVENÇÃO SOBRE O CIBERCRIME - Budapeste, 23/11/2001. Accessed in: 05/03/2018. Available in: <https://goo.gl/twrwQu>

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

b. Microsoft's defense to the Supreme Court

Microsoft states, at the brief in opposition,[38] that the Supreme Court should not admit the case, relying on three arguments. The first establishes that it is the competence of the United States Congress to decide on the need to modernize the Stored Communications Act, which is already underway. The second argues that the court of second instance decided correctly, following the test developed by the Supreme Court in its precedents, on criteria defining the extraterritorial application of a given law[39]. And the third refers to the fact that there are still no Courts of Appeals with divergent interpretations of the extraterritorial application of SCA in order to configure one of the requirements normally used by the Supreme Court before accepting a case , which is called circuit split.

In a brief historical review of SCA's legislative framework in the 1980s, Microsoft claims that Congress could not predict the exponential growth of the Internet in recent years, nor would it envision the emergence of current cloud storage services, with the establishment of servers in several countries. It would not be conceivable that the legislature intended to attribute extraterritorial effects to the rules of the ACS.

It adds the company's defense that, when using the Morisson v. National Australia Bank - which states that US federal law should be interpreted restrictively, if its extraterritorial application is not explicit -, it is found that the criterion adopted by SCA is the place of **data storage** and its protection, and not the place where the act of disclosure or breach of confidentiality/revelation of the data by the authorities will occur. This was precisely the interpretation adopted by the Court of Appeals for the Second Circuit Court of Appeals. Thus, if the scope of the law is to reach privately stored private communications, the relevant conduct would be the seizure of communications, which occurs right under the jurisdiction where the server is located.

According to Microsoft, the decision of the Court of Appeal would be correct, which prevented subsequent international tensions that came to light when the decision of the federal court of first instance was rendered, which was based on the extraterritorial application of SCA of 1986. This is because the European Commissioner, the Irish Government, and some Members of the European Parliament made public statements denouncing breaches of sovereignty entailed by the decision.

The company claims to be rash to bring the case to the Supreme Court, as there is no other similar court in the other federal courts that represents a divergence of case law, one of the main requirements for a case to be admitted by the Supreme Court. It would therefore be necessary to await further cases involving other technology companies, so that the Court would have sufficient subsidies to assess the extraterritoriality of the Stored Communications Act.

Finally, Microsoft emphasizes that the US Congress debates bills that will solve the issue, such as the International Communications Privacy Act, the Email Privacy Act and the Cloud Act. It would therefore make more sense for the Legislature to take the lead in adopt innovative solutions when compared to the available remedies. Thus, the legislative process would be better able to strike a balance between the needs of US

38 UNITED STATES OF AMERICA, Petitioner v. MICROSOFT CORPORATION, Respondent. *Brief in Opposition*. 2017. Accessed in: 05/03/2018. Available in: <https://goo.gl/pnz1Wo>

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

police forces and the interests of other sovereign countries..

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

It is relevant to note that both the government and Microsoft representatives indicated they agreed, at the oral hearing for oral submissions to the Supreme Court[40], that the US Congress would be better able to resolve the issue. In addition, the parties have indicated that they both support the CLOUD Act, Clarifying Overseas Use of Data, which was presented in February by Democratic and Republican senators.[41] This project was hastily approved by Congress on 3/23/2018, and signed by President Trump on the same day, due to the fact that it was inserted in conjunction with the annual budget bill of 2018 (omnibus spending bill)[42], which, if not approved, threatened to generate a crisis in the federal government due to lack of resources.

There was no discussion about the Cloud Act as an individual project in any of the Houses of Congress. Thus, it is still unclear whether the recent approval will have a setback, or whether it will cause the Supreme Court to stop trying the United States v. Microsoft. Nevertheless, it is still very important that we explain how this law seeks to solve the jurisdictional problem discussed in the Supreme Court.

The Cloud Act addresses two basic questions: (1) whether US authorities can access data stored overseas; (2) and under what conditions other countries may request data from companies based in the USA.

As regards the first question, the Bill proposes to amend the Stored Communications Act in order to an electronic communications provider or remote computing service be required to provide the data stored under its possession, custody or control, in case regardless of where the data is stored. Some jurists contend that, prior to approval, the bill was in line with Supreme Court jurisprudence, especially in relation to the United States v. Bank of Nova Scotia, which has allowed banks in the US to be summoned to file documents (subpoena) that are abroad, provided they are in their possession, custody or control.[43]

The law also creates mechanisms for companies to challenge or alter US authorities' warrants if the target of breach of confidentiality is not a US citizen and there is a material risk that the act would violate the laws of another country. In addition, the law seeks to strengthen existing mechanism in the legal system, called comity analysis[44], which establishes that courts should seek to measure the possible impacts of an extraterritorial act or decision on sovereignty and relations between countries if the measure is applied.

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

41 115th CONGRESS - THE SENATE OF THE UNITED STATES. S.2383/H.R. 4943. *The Clarifying Overseas Use of Data* (CLOUD ACT). 2018. Accessed in: 22/03/2018. Available in: <https://goo.gl/4gn81j>

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

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

44 "Comity, in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other […] it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens or of other persons who are under the protection of its laws." Hilton v. Guyot, 159 U.S. 113, 163–64 (1895). In: BREWER, David. *Obtaining Discovery Abroad: The Utility of the Comity Analysis in Determining Whether to Order Production of Documents Protected by Foreign Blocking Statutes*. Houston Journal of International Law. Vol. 22, nº 3. 2000. Accessed in: 22/03/2018. Available in: <https://goo.gl/dxRbwp>

With respect to the second question, regarding the requests for breach of confidentiality made by foreign governments, the law seeks to facilitate international cooperation. Current US law prevents US companies from obeying certain requests made by judicial authorities from foreign countries. The law alters various parts of the Electronic Communications Privacy Act, allowing US companies to obey foreign court orders for data breach of secrecy, telematics intercepts, among others. However, this forecast will only be valid for countries that sign an international agreement with the US, fulfilling certain requirements established by the Executive.

In short, Cloud Act establishes as conditions[45] that the foreign State must have sound procedural guarantees and materials to protect privacy, civil rights, and other human rights of its citizens; that the procedures are supervised by the Judiciary, or other independent authority; freedom of expression is not violated; and that the State adopt procedures to prevent citizens, natural persons with permanent residency, or legal entities located in the United States from receiving data from governmental authorities.

In the event of a country qualifying for the agreement, it would not be necessary for any warrant of secrecy, or another similar court order issued by a competent court, to go through the MLAT cooperation mechanism and be followed directly by the company. This would meet the demand of many research authorities who claim to have difficulties with the current cooperation mechanisms. However, it is not known, if the law is approved, which and how many countries will be accepted as eligible to the agreement with the US, mainly because some of the requirements are open concepts, and that may vary as to their significance for different legal systems. It adds that if this mechanism were restricted to a few US allies, such as the United Kingdom, for example, jurisdictional problems would continue in the various countries that also have a strong presence of US technology companies, such as Brazil.

Finally, it should be noted that there are a number of US civil society groups[46] (*American Civil Liberties Union*; *Human Rights Watch*; *Electronic Frontier Foundation*, entre outros) who criticized the bill for it unilaterally increasing the investigative powers of the police forces to cases involving transnational elements. They have shown concerns about protecting privacy and weakening the MLATs' cooperative system. In a joint letter to the Congress[47], one of the criticisms made is that the MLAT system, despite facing several application problems, still guarantees greater protection of human rights, since requests from foreign governments must be reviewed by the DoJ and judged by a US judge that would comply with strict standards established in the US legal system.

Electronic Frontier Foundation (EFF) states[48] that the Bill, in practice, allows US authorities to have access to data from any person in another country, regardless of its or the data's location. Similarly, authorities from a foreign country who have entered into an agreement with the US Executive could request information about a third person, regardless of location or nationality, provided he or she is not a US citizen or permanent resident of the United States. These prerogatives would end up hurting the sovereignty of various countries and the privacy rights of countless users around the globe.

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

46 *Coalition Letter Opposing the CLOUD Act*. 12/03/2018. Accessed in: 23/02/2018. Available in: <https://goo.gl/qYB2EG>

47 Ibid.

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

4.3. The place where the company that provides the services was constituted (headquarters);

The criterion of location of the headquarters of the company that provides the services is one of the criteria of definition of jurisdiction and applicable law reminiscent of the principle of territoriality. Under the principle of territoriality, the jurisdiction and / or applicable law are defined according to the location of those involved and their acts. The application of the principle in cases involving the Internet, however, is always quite complicated by the difficulty in locating satisfactorily an act as being of one or another State.[49]

Especially on the internet, the territorial principle as a criterion of jurisdiction is flawed, since the geographical location of a legal act carried out by the Internet is difficult to predict. The act may be committed by a person in a country X, through a platform whose servers are located in country Y, and affect another individual in country Z, resulting in competition between several States with equally legitimate claims with respect to territorial connection criteria.[50] Identifying the ideal location of an online activity that results in a relevant legal fact is therefore a difficult and complex issue.

A number of cases have discussed the possibility of defining the jurisdiction and/or applicable law according to the place where the company involved in the litigation in question is situated. In a few paradigmatic cases, however, a national court has chosen to dismiss jurisdiction or national legislation in favor of foreign institutes. The choice of the location of the company's headquarters generally occurs through forum selection clauses included unilaterally in the contracts of adhesion (Terms of Service - ToS), based on an Anglo-Saxon contractual model that can hardly be supported in continental law institutions that protect consumers' rights. The court-elect clauses that call for jurisdiction and the law applicable to the place of incorporation of the company are generally considered void in most jurisdictions when invoked by the company to argue the incompetence of a local court.[51]

One of the paradigmatic cases not only for Internet Law, but also for the issue of jurisdiction and law applicable in this context, is the case LICRA (The Ligue Contre Le Racisme et L'Antisemitisme) v. Yahoo!, started in 2000 and concluded around 2006. In the case, the French Anti-Racism and Anti-Semitism League sued Yahoo! for making available on its e-commerce site the auction of Nazi memorabilia, conduct typified in the French Penal Code. The facts were not disputed during the case, but the American company defended itself on the grounds that the auctions were conducted under United States jurisdiction, and therefore the French court would not have jurisdiction to adjudicate the case. The case had parallel proceedings also in the United States.

In the French trial, the court reaffirmed the competence of the French court, alleging that: i) the auctions were open to users from any country, including France; ii) the exhibition and display of these objects caused public disturbance and were against the French Penal Code; and (iii) the US company was aware of the access of French users to the service, as it provided a French language site with advertising directed at French

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

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

51 IRIS. Competência Internacional dos Tribunais Domésticos e Litígios de Internet, 2018. p. 20. Available in: <https://goo.gl/7RveQq>

citizens and had a French branch office. Condemned to Yahoo! to take measures to prevent French citizens from having access to the auction. When the American company refused, the Court then fined it 100,000 francs a day.

In 2001, Yahoo! chose not to appeal the decision. Instead, he brought the case to the Northern California District Court requesting it to dismiss the French order as ineffective in American territory. In the first instance,[52] the court upheld the French conviction as conflicting with the First Amendment of the American Constitution. The superior instance of the Ninth Circuit, however, reversed the decision on the grounds that the District Court had no jurisdiction over LICRA. The criterion used was that of "minimum contacts" that according to the Ninth Circuit were not present between LICRA and the State of California.

The most relevant development for the case came in 2006,[53] when the Ninth Circuit again adjudicated an application for a declaratory judgment that would deem ineffective on American soil the conviction of the French Court. Once again, the US Court of Appeal dismissed Yahoo! 'S request, making relevant comments on the issue of conflict of laws and sovereignty generated by the case. Judge Fletcher would have said: *"At Yahoo! is necessarily arguing that it has, under the First Amendment, a constitutional right to violate the French Criminal Law and to facilitate its violation by third parties. [...] the existence of such extraterritorial right under the First Amendment is uncertain."*

The judge's consideration is relevant when considering the paradoxes of sovereignty and the conflicts of law generated by the Internet: to what extent does the application of national legislation guarantee a "right" to the violation of the legislation of another country?

A. Favorable decisions to the location of the company's headquarters as a criterion for defining the applicable law

The Administrative Court of Hamburg, Germany, recently overturned an order from Hamburg's Data Protection Authority (DPA) against Facebook. The Court ruled that the applicable data protection law would be Irish, rather than German, depending on the location of the European branch office of the company being in that country. [54]

The litigation began when the Data Protection Authority received a complaint from a user after Facebook blocked her account by using a pseudonym, required a copy of her identity, and unilaterally changed her username to her real name. Hamburg's DPA ruled that Facebook could not unilaterally change the names chosen by its users to their real names, nor did it require them to be officially identified, since the German data protection law would guarantee a 'pseudonym's right' in profiles online.

Rejecting the decision of the DPA, the Hamburg Court ruled that the operations of the companies Facebook Ireland and Facebook Germany constitute "establishments"

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

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

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

within the meaning of Article 4 (1) (a) of the Data Protection Directive 95/46 / EC.[55] However, it argued that if several national data protection laws could be applied only because the data controller is established in several Member States of the European Union, then the European State law with which the data operation is associated. In the case, the Court of Hamburg held that, since Facebook Ireland is the controller of that data and also the group's center of operations in Europe, the Irish Law should be applied.

The Court refused to make a broad interpretation of the term "establishment" in Article 4 (1) (a) of the Directive. For the Court of Hamburg, the case differs from the case judged by the Court of Justice of the European Union (CJEU) in the case involving the Spanish DPA and the company Google Spain, because the data in question are under the authority of a controller established in one of the States of the European Union. Thus, there would be no risk that European citizens would be deprived of the protection of the Directive, while in the Spanish case, the search controller was located outside the European Union.

The interpretation of Article 4 (1) (a) of the Directive by the German Court indicates that multinational companies such as Facebook may refrain from observing a myriad of conflicting national laws, at least within the European Union. Although the conflicts of law found by Brazilian courts are in a significantly different context in which there are no supranational guidelines such as Directive 96/45 / EC, the case may still bring light to the conflict of laws involving data controllers located in foreign soil.

B. Contrary decisions to the location of the seat of the company as a criterion for determining the applicable law

The decision itself, however, contrasts with other European decisions involving similar jurisdictional issues. A more comprehensive interpretation of Article 4 (1) (a) was used by the CJEU in cases Google Spain v. Mario Costeja[56] and Weltimmo.[57]

In Google Spain case, the CJEU ruled that European law would normally apply to a foreign data controller established outside the Union's borders. The court held that Article 4 (1) (a) does not necessarily require that processing of personal data be conducted by the relevant establishment itself, being sufficient that it get conducted in the "context of the activities" of this establishment. Thus, the court understood that sales made by Google's establishment in Spain would be "inherently linked" to data processing conducted by the company's arm in the United States.

In the Weltimmo case, the CJEU reiterated the broad notion of "establishment" in the Directive. The Court has ruled that if a data controller exercises "... real and effective activity, even if minimal ..." through "stable installations" within the territory of the State, shall be deemed to have an "establishment" in the territory of that State. Weltimmo was a registered company in Slovakia but to whom the Data Protection Authority of Hungary wanted to fine for violating various provisions of the Hungarian Data Protection Act. The

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

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

57 CJUE, *Case C-230/14*. Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság. Available in: <https://goo.gl/aSfaEJ>

CJEU considered that Weltimmo was established in Hungary for operating a website in the Hungarian language, with advertisements in Hungarian, representation, address and bank account in the country.

5. MLATs - Difficulties of its Use and Possible Solutions

The use of legal cooperation agreements, "MLATs", currently presents a series of difficulties of efficiency and effectiveness. In general, these mechanisms were designed for exceptional cases, in a historical context in which transnational crimes were an exception. However, with the increasing use of the Internet in the world, transnational relations became increasingly common, being present in different aspects of citizens' daily life.

Chapelle and Fehlinger summarize the structural problems faced in the implementation of the MLATs, in the different countries, in 4 issues[58]:

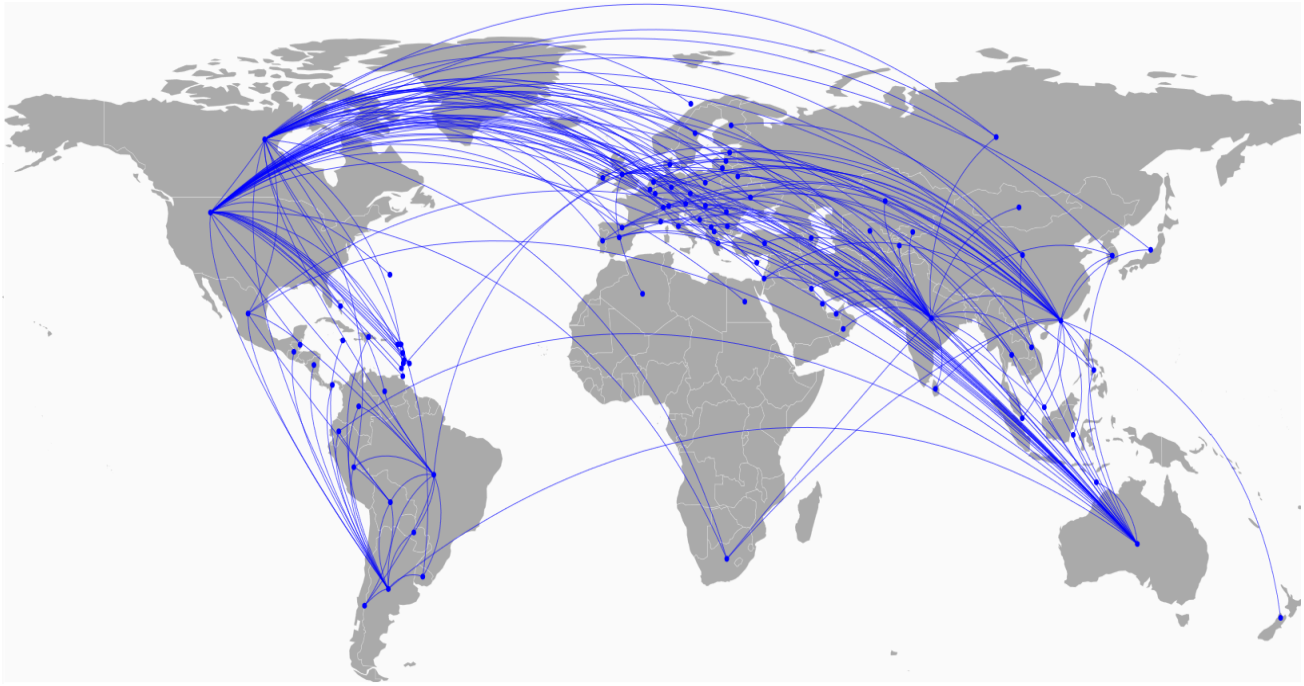
1. Speed: MLATs are poorly adapted to the speed brought by the internet and to the viral capacity of information dissemination. In the best scenario a request for cooperation by MLAT takes several months to be processed, taking up to 2 years between certain countries. Their intricate validation mechanisms, despite seeking to promote robust procedural guarantees, ultimately end up making the system as a whole impractical.

2. Scope: MLATs are often limited to the requirement that the act, object of cooperation, be an unlawful one in the legislation of the two countries involved (dual incrimination). Thus, the relevance of the MLATs ends up being reduced due to the disparity of national legislations, mainly in questions about freedom of expression, as in cases of hate speech and defamation. They have also been ineffective in cases where the location of the requested data is unknown by state agents.

3. Asymmetry: In practice, MLATs impose the legal system of the country that receives the request for cooperation, to the detriment of the one making the request, even if there is no territorial connection with the requested country beyond the seat of the operator of an online service. These agreements also end up by disregarding the place where the unlawful act took place, or even who the parties are. Thus, a growing number of countries have criticized the MLAT system, especially when considering the dominant role in the market of companies based in the United States.

4. Scalability: The traditional MLATs system can hardly scale the internet. A large number of countries do not have such cooperation agreements and establishing bilateral relations between 190 countries would require more than 15,000 agreements.

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



MLAT agreements between countries, according to interactive map of the international NGO *Access Now*.[59]

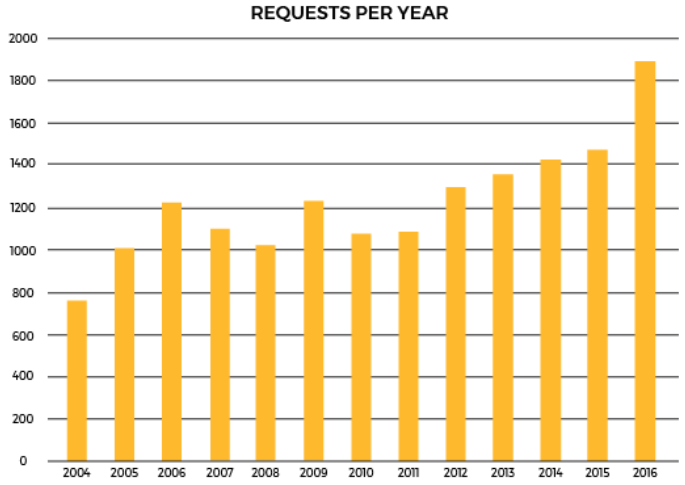
Thus, the authors believe that innovative solutions that overcome the structural limitations of the MLATs are needed in order to guarantee due process of law and the efficiency of agreements. However, they recognize that reform processes will not be easy and that, in their view, there is still no simple solution in the near future.

This diagnosis about the efficiency of international cooperation seems to be confirmed in Brazil. This hypothesis becomes clearer when comparing the numbers of requests for cooperation in criminal matters made by the Department of Asset Recovery and International Legal Cooperation with data from the transparency reports of certain IT companies and with the data on requests for telematic tapping carried out by the Brazilian authorities.

Regarding the Department of Asset Recovery and International Legal Cooperation (*Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional*[60] - DRCI), board of the Justice Ministry, the General Coordinator of Assets Recovery, Isalino Giacomet, estimates that a process of criminal cooperation between Brazil and other countries takes an average of 7 months to materialize, and this time can be reduced in some emergency situations. He also informs that in 2016 there were about 1,900 new applications in the criminal area, with about two assets for each liability (2: 1). The US was among the top 3 respondents, behind only Uruguay and Paraguay, respectively.

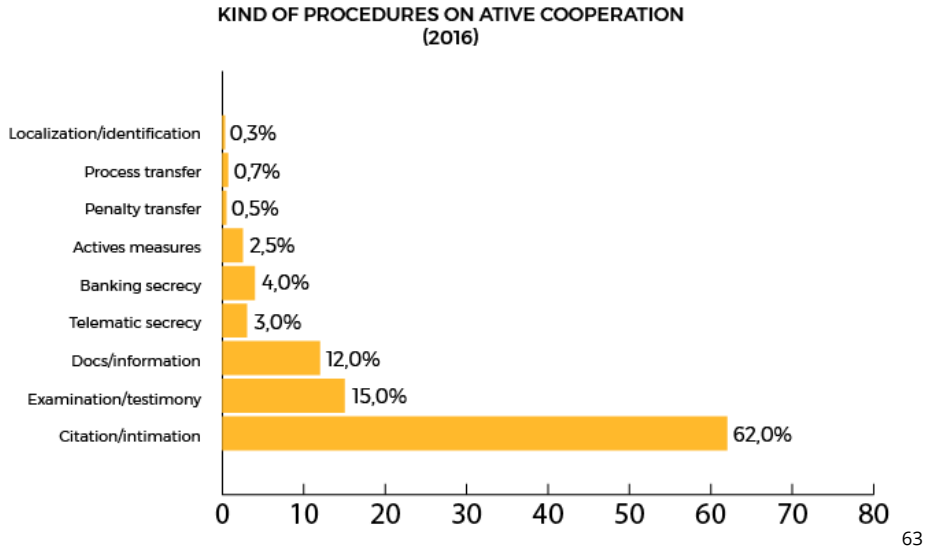
59 For specific agreements between specific countries, see: <https://www.mlat.info/>

60 Institute for Research on Internet and Society (IRIS). Workshop: Jurisdição e cooperação jurídica internacional nos conflitos da internet - Parte 3. Novembro de 2017. Between 00:00 and 26:00 minuts. Accessed in: 15/02/2018. Available in: <https://goo.gl/QZyv3H>

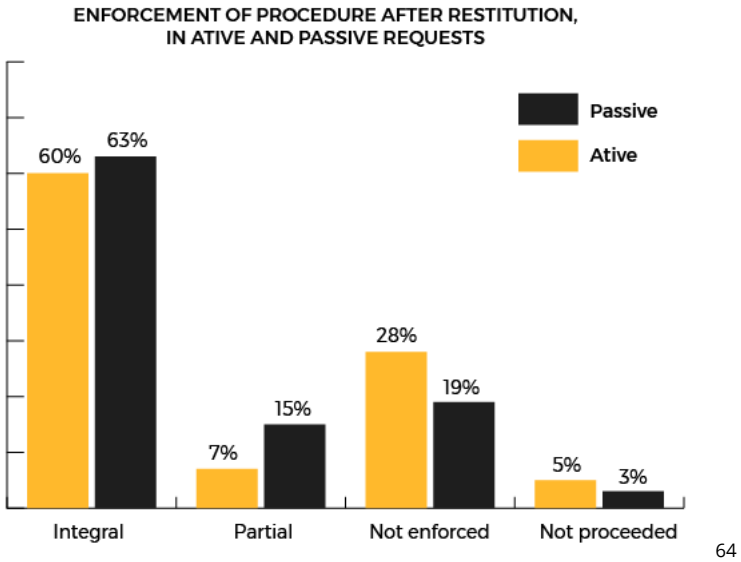


61

He adds that telematic procedures[62] (obtaining registration data, breach of confidentiality of communications, etc.) accounted for about 3% of criminal applications active in 2016; and that the full compliance rate for all orders reached 60%.



63



64

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

Comparatively, Google's 2016 transparency report for requests for information from Brazilian users, between January and June, presents 874 requests, with 59% being met; while between July and December there were 1,011 requests, with 60% being attended. Although there is no discrimination regarding the type of data requested (real-time "listening", private communications of e-mails, messages, etc.), it can be inferred that a significant part of the 1,885 requests for 2016, which involved a breach of private communications and telematic interceptions are probably among the unanswered requests (disregarding eventual emergency exceptions), since the company uses the same argument as that of ADC 51/2017 regarding the need for a MLAT procedure in such cases[65].

The Facebook transparency report, referring only to requests related to criminal cases in Brazil, between January and June 2016[66], said it had received 1,736 requests for user information and provided some information to the authorities in 50.58% of requests. Subsequently, between July and December of the same year, 1,808 requests were made, and some data were given in 50.58% of them. The report also categorizes emergency requests, of which about 12 out of 26 have been met for the year 2016. As the report also does not discriminate what types of data were requested, the logic applied above to the Google report can also be applied to the report. from Facebook. Thus, requests for private communications are likely to be mostly unsatisfied, as the company also states in its guidelines that, for content stored in an account, as messages, a search warrant is required, under US law.[67]

When comparing the number of requests made to the companies, with a percentage of only 3% of active criminal suits filed by the DRCI in 2016, it is inferred that a significant part of the requests for private communications to companies did not reach to become an international cooperation procedure by MLAT.

Finally, in order to strengthen the hypothesis that there is a repressed demand for requests for the provision of private communications from users to application providers, the number of wiretapping in Brazil is briefly analyzed. The website of the National Council of Justice, in the data section related to the wiretapping of 2016 for the state court, finds that 239,222 telephones and 18,251 telephones using VOIP (Voice over Internet Protocol) were monitored that year. [68] These data demonstrate how the practice of monitoring phones has still been a constant research tool in the country, a need that does not seem like it's being replaced by other instruments as traditional telephony has been giving way to forms of communication via the Internet. Thus, it is clear how, by 2016, the small number of requests for international cooperation carried out by the Ministry

65 "How does Google respond to requests from government agencies outside the United States? Through the Mutual Legal Assistance Treaties (MLATs) and other diplomatic and cooperation agreements, agencies outside the US can work with the US Department of Justice to collect evidence in the context of legitimate investigations. In some cases, the US Federal Trade Commission can provide assistance.

If US law is implicated in the investigation, a US body may open its own investigation and provide evidence gathered to investigators outside the US. Google may also disclose data in response to urgent disclosure requests if it believes that it is necessary to do so to prevent serious injury or death.

On a voluntary basis, we may provide user data in response to legal process from governmental bodies outside the US if such requests are in compliance with international standards, US law, Google policies, and the laws of the requesting country. "GOOGLE Inc. Frequently asked questions about the legal process for user data requests. (free translation). Accessed in: 23/02/2018. Available in: <https://goo.gl/4FfVKz>

66 FACEBOOK Inc. Transparency Repor. 2016. Accessed in: 23/02/2018. Available in: <https://goo.gl/aLZQZh>

67 "It is needed a search warrant issued pursuant to the procedures described in the US Federal Criminal Procedure Code or an equivalent state warrant is required upon proof of probable justification for forcing the disclosure of content stored in any account, including messages, photos, videos, publications in the Timeline and location information." (free translation). FACEBOOK Inc. Guidelines - Informações para Autoridades Policiais. Accessed in: 23/02/2018. Available in: <https://goo.gl/uYDvfX>

68 CONSELHO NACIONAL DE JUSTIÇA. Relatórios Quantitativos - Interceptações Telefônicas. 2016. Tabelas 5 e 6. Accessed in: 23/02/2018. Available in: <https://goo.gl/kE5ZAU>

of Justice contrasts sharply with the volume of telephone interceptions carried out. This reinforces Chapelle and Fehlinger's contention about the structural problems faced by the authorities in trying to use the current MLAT system. Thus, it is at least questionable to say that such an institutional arrangement has worked efficiently in Brazil.

Nevertheless, it should be noted that relevant actors involved in the debate about jurisdiction and the internet argue that the MLAT system, despite the current problems, must be strengthened through reforms. The Electronic Frontier Foundation, for example, recommends perfecting the MLAT system[69], because it believes that MLAT establishes stricter procedural safeguards and greater privacy protection, since an authority seeking data abroad has to respect the legal protections of the two countries involved. The efficiency problems, the EFF alleges, could be solved in part by a greater allocation of resources to the cooperation agencies, a simplification of procedures, and better training of the police and judiciary on cooperation mechanisms.

In this way, the lack of cooperation between countries may end up encouraging the adoption of diverse solutions, such as the invasion of electronic devices by the police directly, which presents serious risks to privacy and violation of the sovereignty of third parties. Or even the imposition that data is stored in the jurisdiction of the country (data localization), which has reckless effects on the efficiency and economic freedom of the technology sector.

By way of illustration, Ahmed Ghappour of Boston University warns that network intrusive techniques or hacking by the FBI in dark-web investigations often involve people located in other countries as targets of the surveys. Thus, he believes it is plausible to say that this phenomenon may be leading to the largest expansion of enforcement jurisdiction in the history of the FBI.[70]

6. Intentional conceptual confusions: identification of users and anonymity

In the brief manifestations of material law provided by the Society of Technology Users (**Sociedade de Usuários de Tecnologia - SUCESU Nacional)**, in the records of ADC 51/2017, there seems to be a clear confusion between the systematic identification of online users and the concept of anonymity. According to the SUCESU, the application of provisions of Decree No. 3.810/2001 (which incorporates the Mutual Assistance Agreement between the United States and the Federative Republic of Brazil) would "violate" the anonymity, art. 5, item IV, of the Federal Constitution.

In a number of judicial disputes concerning the Internet and new technologies, this is a commonly made association, even though mistaken, between the technical possibilities of secrecy and protection of personal data, to the detriment of freedom of expression since identified, as determined in our Constitution. In a certain part of the document of National SUCESO, it is said that "asserting the understanding advocated by the Author of the demand will remove the constitutional fence to anonymity," which simply does not fit the reality of argument and facts.

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

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

Defenders of user rights and organized civil society, as is the case of the Institute for Research on Internet and Society (IRIS), by requiring compliance with legally established safeguards and procedures for the breaking of telematic secrets and identifiers, such as those provided by Brazil's Internet Bill of Rights (Article 22 and Article 3, sole paragraph) and by Mutual Assistance Agreements between States, do not in any way propose breaches of the constitutional order, or the prohibition of anonymity. On the contrary, the submission made by IRIS, admitted as 'Amicus Curiae' in ADC n. 51, aims to protect the rights and guarantees of art. 5 of the Federal Constitution, including the intimacy, privacy and confidentiality of communications. In order to do so, it is proposed to safeguard the proper instruments of access to these data, legally foreseen and in accordance with the current legal order, and the affirmation of the observance of international law by the Supreme Court.

The supposed antagonism of the liberal binomial "privacy" vs. "security" is often criticized by national literature[71] and international[72], since on several occasions fundamental rights have been blatantly "flexibilized" in favor of a perceived need for social (and sometimes political and media) response to security issues. It so happens that privacy and security are not mutually exclusive, as the protection of personal data of users does not necessarily mean the right to anonymity. In addition, it should be kept in mind that the condition of "anonymous" on the Internet is not a binary and watertight phenomenon, but that it comprises several degrees of characterization, according to the greater or less technical difficulty for a user to be identified. This gradual characterization, even, is recognized in the General Personal Data Protection, both Brazilian (art, 5th, III, PLC 53/2018[73]) and the European (recital 26, *General Data Protection Regulation*[74]), which seek to encourage the processing of anonymous personal data in order to promote greater privacy and user protection, without prejudice to technological development.

The new technologies involved in communication and cloud computing platforms, such as those that provoke the debate in the news, have potentiated the storage of personal data (identification and communication) increasingly outside the citizens' habitual residence, in contrast of what was the praxis when one begins to discuss the right to privacy[75]. The concept of privacy itself evolves to accompany social transformations that establish and modulate it (privacy of children and adolescents, responsibility for the maintenance of large databases, allocation of safeguards for the conduct of online banking transactions, electronic judicial processes, etc.). This does not mean, therefore, that such data would not be subject to adequate legal regimes for privacy protection, especially a concept of privacy compatible with the reality of new technologies, which is

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

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

73 "Art. 5 For the purposes of this Law, the following shall be considered: ... III - anonymised data: personal data relating to a holder that can not be identified, considering the use of reasonable technical means available at the time of treatment;"

74 "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.." Regulamento(UE) 2016/679 do Parlamento Europeu e do Conselho. Available in: <https://bit.ly/2LsogHg>

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

also transnational, involving different actors and requiring multiple forms of protection.

Security and privacy are ideas that occasionally can be weighed, but not in a similar way to a zero-sum game. It is possible, **honestly and rationally**, to resume an intellectual debate without proposing this antagonism, precisely by the legal instruments (national laws and international agreements) which constitutionality is sought here. Brazil's Internet Bill of Rights itself, in its art. 3, covers **privacy and security** as disciplinary principles, and not competing or excluding the use of Internet in Brazil, which is reinforced in its article 8[76]. It seems to contradict, among some of the arguments fanned in the Manifestation of the SUCESO Nacional, that privacy and security are highlighted as if they were irreconcilable pretensions, as if they represented a panacea of the digital age.

On the contrary, the network society, characteristic of the present moment, is only structured thanks to the perfectioning of societal patterns of the long - and fateful - twentieth century and that have cemented respect for the value of the Democratic Rule of Law. Its institutions must preserve achievements in terms of human rights, such as online privacy and the security of Internet interactions, communication, business and operations.

What is proposed, through the affirmation and declaration of the constitutionality of Decree No. 3.810/2001, and of the immediate application of the human rights norms provided for in the treaties to which Brazil is a party (still pursuant to Arts 5, §§1 , and 2, of the Constitution and Art. 3, sole paragraph, of the Civil Code) is therefore not the prevalence of anonymity regarding the possibility of identification of users, but rather compliance with the procedures in force so that identification and telemails may occur.

In this context, if manifestations in constitutional procedures such as in ADC 51/2017 do not confide in such requests and demands to the current legislation and to the international commitments assumed, Brazil would be using the contradictory position in relation to the guarantees that institutionally built with regard to the Internet. More seriously, dispensing with the mechanisms favoring a due process, as pointed out in item 8 below, could entail risks of subjecting Brazilian society to procedures of mass surveillance, censorship and violations of privacy and freedom of expression online (art. 8 of Brazil's Internet Bill of Rights).

These procedures are also adopted - on a larger scale and with a different depth, but not in a way that de-legitimizes comparison - in countries such as Russia, China, Iran, Syria and Saudi Arabia[77]. In them, anonymity is also not allowed, to the detriment of individual guarantees and freedoms, but also and especially in defense of a supposed national security that, by the way, is not reached through even more vigilance[78]. Thus, it is observed that the fight against anonymity is not an excuse to be accepted by the STF

76 Regarding privacy and intimacy in the Internet Civil Registry, Giacchetta and Meneguetti affirm that: "The Brazil's Internet Bill of Rights reaffirmed the constitutional guarantee to the inviolability of privacy and privacy, as a principle and also as the right of the users of the Internet as a reaction to the international facts related to the collection and unauthorized use of personal data and communication of Brazilian users, even if dispensable before the provisions of the 1988 Federal Constitution. " Cf. GIACCHETTA, André; MENEGUETTI, Pamela. A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no Marco Civil da Internet. In: *Marco Civil da Internet.* LEITE, George Salomão; LEMOS, Ronaldo (coord.). São Paulo: Atlas, 2014, p. 390.

77 In this regard, cf. the indicators and results of analysis in FREEDOM HOUSE. *Freedom on the Net Report 2017*: manipulating Social Media to Undermine Democracy. Available in: <https://freedomhouse.org/report/freedom-net/freedom-net-2017>, acesso em 16 de junho de 2018. On the subject, see also 2015 Report of the Assembly of States of the Council of Europe on Mass Surveillance and Threat to Human Rights, Available in: https://pt.scribd.com/document/253848295/Mass-Surveillance-Report

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

in order to move away from the instruments of international cooperation, incorporated into the Brazilian legal system.

7. The articles 3, sole paragraph and 11 of the Brazil's Internet Bill of Rights

There is a perception among certain lawyers, judges and academics that there is an apparent "conflict of laws" between Brazil's Internet Bill of Rights, with its unilateral application of Brazilian law (Article 11), and Decree No. 3,810 of 2001, which determines the process to be adopted in cases of international legal cooperation. This conflict, however, is only apparent, especially when analyzing more in depth the devices and structure of relationship or interaction between norms established by the legislative instruments themselves.

By rejecting compliance with requests for supply or delivery of data by Brazilian courts due to the restriction imposed by the Stored Communications Act, companies that provide applications with a transnational nature are not violating Brazilian sovereignty, nor are they in conflict with the Brazilian legal system. This is because Brazilian law itself, made up of Internet Bill of Rights, Decree 3.810 and the Constitution, provides for compliance with the international cooperation procedure through the support of Mutual Legal Assistance Treaties (MLATs), without discretion to the national court. In addition to legal obligations, there are bilateral and multilateral treaty-based international obligations, the non-compliance of which would lead Brazil to international liability for positive breach.

The initial misperception seems to be based on the isolated analysis of Article 11 of the Brazil's Internet Bill of Rights,[79] which determines the application of Brazilian legislation to any cases of collection, storage, custody and treatment of records in which one of the terminals is located in Brazil. Paragraph 2 again only accentuates the misconception about an apparent conflict[80], since it establishes that Brazilian (material) law applies even if the activities are carried out by a legal entity headquartered abroad and that has, in the same economic group, an establishment in Brazil.

From these two blocks of rules, it is evident that the purpose of the legislative formulas was to unilaterally submit to Brazilian law the regency (or discipline) of certain legal relationships involving Internet companies and users ("collection, storage, custody and treatment of records in which one of the terminals is located in Brazil "). That is, it is an issue of applicable law; it is not confused with jurisdictional issues, specifically as regards the definition of the jurisdiction of national courts to settle a dispute involving those parties. Taking the analysis to the precise delimitation of the objects of private international law, as Professor Jacob Dolinger observes, the underlying question is a question of law applicable to the case with international connection[81].The nature and classification of the rule contained in Art. 11 of the Brazil's Internet Bill of Rights, in turn, point to a "unilateral" (in terms of structure) conflict rule, that is to say, a rule designating a single applicable law solution, which refers, in the species analyzed, to the Brazilian

79 'Art. 11. All operations involving the collection, storage, retention or processing of records, personal data, or communications by Internet service and applications providers must comply with Brazilian law and the rights to privacy, protection of personal data, and confidentiality of private communications and records, if any of those acts occur in Brazilian territory."

80 "§2. The provisions of this article apply to activities conducted by foreign-based legal entities, if they offer services to the Brazilian public or at least one of the members of the legal entities' economic group has an establishment in Brazil."

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

law[82]. Of course, the legislative policy solution contained therein seems to be based on a very specific spatial criterion: "place of activity for the collection, storage, storage or treatment" of data in Brazil.

It would therefore be clear that Brazilian law would apply to any act relating to the collection, storage or processing of data in the presence of an objective connection element (at least one of the terminals located in Brazil) and therefore, any opposition to these provisions due to restriction by US law constitutes a violation of Brazilian sovereignty and norms. However, the Brazilian legal system itself **rejects this notion for the specific case of requesting data, information or, in the extreme, evidence located under foreign jurisdiction.**

It is important to point out that there are other devices in Brazilian Internet Bill of Rights, the Decree No. 3,810 of 2001 (Brazil-United States Cooperation Agreement) and in the Federal Constitution that validate the need to use the MLATs for cases involving the Internet. However, data relating to the **content of communication or conversations** between users with so-called access **metadata**, which are also required by Law n. 12.965/14, should not be confused. The Stored Communications Act only prevents companies from delivering the first, according to the American ruling.[83]

According to Pontes de Miranda, Law is a methodical system of rules and satisfies requirements of coherence and consistency. By analyzing intrinsically and extrinsically the social relations that are stamped by the legal order, the author explains:

> The legal rules will build a system. No legal rule is by itself, none is gout, even when it has been the sole article or paragraph of a law. [...] This requirement of systematicity of law meets the need for coherence and consistency in human conduct, especially in relation to the life of relationship[84].

Article 3, single paragraph[85] of Internet Bills of Rights, places international legislation within Brazilian legal system, and its respect for principles other than those established in the law itself, thus introducing a rule of openness to the system of treaties and conventions. It also incorporates procedural obligations, such as the duty to establish legal cooperation in the course of transnational civil proceedings. **Legal international cooperation, therefore, cannot be conceived as an act of mere discretion on the**

82 A typical example of a unilateral conflict norm is that contained in Art. 7, § 1 of the LINDB ("In the case of marriage in Brazil, the Brazilian law will be applied with regard to the dissident impediments and the formalities of the celebration"). In the words of DOLINGER (Direito Internacional Privado, cit., P.213), the tendency of the Brazilian International Private Law is to formulate bilateral norms, with exceptional cases of unilateralism. According to him, the proponents of unilateralism maintain that the legislator only has legislative competence over "the application of his own laws, and it is not incumbent on him to attribute competence to the law of another legislator, since only he will say of the scope of his law. According to this school, legislator only determines when to apply its own law ". (free translation).

This is exactly the case with the solution of Art. 11 of the Brazil's Internet Bill of Rights, whose normative scope is attached to the submission to Brazilian law of the legal relations emerging from the "collection, storage, storage or processing" of data, when at least one of them occurred or been carried out in Brazil.

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

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

85 "Art. 3. The following principles underlie Internet governance in Brazil: [...] §1. The principles set out in this Law do not exclude others related to the same subject matter under Brazilian law or international treaties to which Brazil is party."

part of the Brazilian administrative and judicial authority. It is established as direct command of treaties, by the Code of Civil Procedure, by the Constitution, and in the interest of achieving justice objectives.[86] It is also necessary to analyze the Federal Constitution, in its Title I, on **fundamental principles**.

Article 4[87] of the Federal Constitution lays down the principles governing the international relations of Brazil, and therefore provides the basis under which cases of legal cooperation should be analyzed. Among them is the so-called **Principle of International Cooperation** established by subsection IX of this article as "cooperation among peoples for the progress of humanity". On this principle, Hildebrando Accioly affirms:

> The principal, among the moral duties of States, is **mutual assistance**, which manifests itself in various forms. These include: [...] (d) assistance and cooperation for the administration of justice, in both civil and criminal matters, including the adoption of appropriate measures to facilitate the social action against crime[88].

Likewise, it is necessary to observe the immediate effectiveness of the norm contained in paragraph 2 of Article 5 of the Constitution,[89] which emphasizes the non-exclusion of other principles deriving from it, as well as the international treaties with which Brazil has committed itself.

Therefore, in compliance with the principle of international cooperation, as well as other principles of international law and treaty law (as explained in the previous chapter), no consistent interpretation of the Brazilian Internet Bill of Rights can be against the provisions of Decree No. 3.810 of 2001, which establish at various times respect for the legislation of the Requested State. This is because: (i) The Decree incorporates, in Brazilian legal system, a treaty to which Brazil has committed itself to follow; (ii) The Internet Bill of Rights establishes, in its Article 3, respect for other principles in force in the Brazilian legal system, in this case, that of international cooperation; and (iii) The Decree per se is part of Brazilian law, for which Brazilian Internet Bill of Rights - Law No. 12.965/14 - determines compliance with cases involving data collected in Brazil.

The Decree N. 3.810 of 2001 establishes compliance with the laws of the Requested State (R.S.) at three points:

(i) in Article I, 2., h),[90] to restrict forms of assistance prohibited by the laws of the R.S.;

(ii) in the article V, 3.,[91] to determine that requests for cooperation are carried out

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

87 "Article 4. The international relations of the Federative Republic of Brazil are governed by the following principles: IX – cooperation among peoples for the progress of mankind;"

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

89 "Article 5. All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms: [...] Paragraph 2. The rights and guarantees expressed in this Constitution do not exclude others deriving from the regime and from the principles adopted by it, or from the international treaties in which the Federative Republic of Brazil is a party."

90 "Article I. 2.Assistance shall include: [...] h) any other form of assistance not prohibited by the laws of the Requested State".

91 "Article V.3. Requests shall be executed in accordance with the laws of the Requested State except to the extent that this Treaty provides otherwise. However, the method of execution specified in the request shall be followed except insofar as it is prohibited by the

in accordance with the laws of the R.S.; and

(iii) in Article XIV, 1.,[92] to determine that the execution of search warrants and seizure warrants are justified under the laws of the R.S.

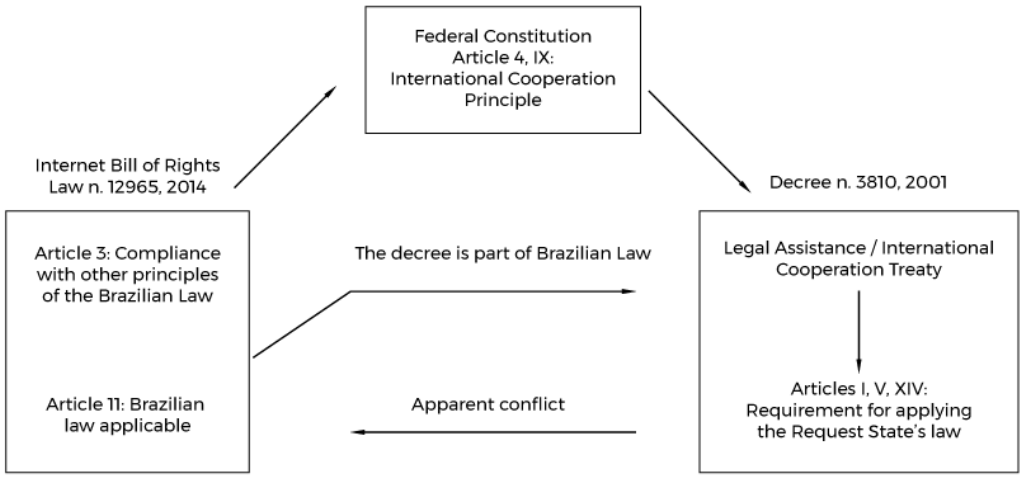


Figure I - Apparent Conflict between Law n. 12.965/14 and Decree n. 3.810/01

In the above scheme, we can observe the submission of the rule of article 11 of the Internet Bill of Rights to other provisions of the same law, the Constitution and Decree No. 3.810/2001. It is not, therefore, a case in which Brazilian law is silent and a foreign company would be benefiting from this omission. The Brazilian State has undertaken a commitment, namely to cooperate in mutual assistance and to respect the legislation of the requested State; it could not now exempt itself from it for the convenience of investigation authorities or criminal prosecution and in submission to infraconstitutional legislation.

As will be discussed below, the rules interpreted systematically - the Constitution, the Brazil-United States Agreement and the Civil Code - also point to the observance of rights and procedural guarantees for the parties in the civil and criminal transnational litigation, also involved in pluri-connected Internet disputes.

8. Protection of users' rights and fundamental safeguards

Another aspect that is very relevant to the consideration of the constitutionality of Decree N. 3.810/2001, which incorporates the Agreement on Mutual Assistance in Criminal Matters between the United States and the Federative Republic of Brazil, concerns the need for national courts to guarantee the users' rights online.

It is not for other reason that Law 12.965/2014 is often called the "constitution of the internet" in Brazil. Without the pretension of exhausting the safeguards contemplated by this legislation to the users, the Internet Bill of Rights reinforces important rights and fundamental guarantees, as the right t privacy, the protection of personal data (which is also subject of recently approved legislation in National Congress, in Draft Bill 53/2018[93]),

laws of the Requested State."

92 Article XIV. 1. The Requested State shall execute a request for the search, seizure, and delivery of any item to the Requesting State if the request includes the information justifying such action under the laws of the Requested State.

93 At the time this brief was offered to the Brazilian Supreme Court, The General Data Protection Law had not been sanctioned and that is why the text refers to the Law n. 13.709/2018 as then Draft Bill 53/2018.

the inviolability and secrecy of online communications, accessibility, freedom of business models, as well as **other principles "set out in this Law do not exclude others related to the same subject matter under Brazilian law or international treaties to which Brazil is party**" (article. 3, single paragraph).

That is, the "internet constitution" in Brazil, as well as the Federal Constitution, allows for the adaptation of the national legal regime to the international order, as well as incorporation of international treaties into its role as legislative instruments. Just as the Mutual Assistance Agreement between the United States and the Federative Republic of Brazil can be included in this category and according to its internalization process, declarations such as the one that treats access to internet as a human right[94], from the UN Humans Rights Council, which included Brazil.

A significant part of the literature also considers the model adopted in the elaboration of the Internet Bill of Rights as a warranty, which presupposes the subordination of public and private power to higher norms that establish fundamental rights, such as those contained in Articles 7 and 8 of the Internet Bill of Rights[95]. In this context, the recognition of rights as fundamental guarantees implies their primacy in the adequacy of formal acts to material issues, as also observed by the Italian jurist Luigi Ferrajoli[96], in a clear rupture with the traditional legal positivism, and in benefit of the systematic interpretation of the legal system, attentive to the concepts of validity, material validity and substantive democracy of the laws.

9. Respect for the due process of law

Consonant with theoretical and doctrinal approaches, international cooperation procedures bind the Brazilian State from the perspective of the Constitution, the Civil Procedure Code (CPC) and the treaties to which Brazil is a party.

The article 26, *caput*, from the CPC determines the opening of Brazilian procedural system to international law, establishing the **primacy of treaties and conventions in the regulation of acts and measures of legal cooperation,** in line with the principles offered therein. Among them, it is important to highlight that the legislator expressly provided for the observance of guarantees of due process of law in the requesting State (Article 26, item I), which may be Brazil, when formulating the active requests, or the foreign State, when it addresses the requests to the judicial authorities and administrative procedures for compliance (passive requests). Compliance with due process must contain both the right of the parties involved in the dispute to have the right to formulate their claims (right of action) and the broad defense and contradictory, as well as the guarantees that procedures in the forum and abroad develop with respect to the "fundamental rights of the process"[97].

The rights guaranteed by the treaties to which Brazil is a party in the field of human rights, such as the 1969 American Convention on Human Rights - San José, are

94 UN. Human Rights Council, *Resolution A/HRC/32/L.20*, 27 June 2016. Available in: <https://www.article19.org/data/files/Internet_Statement_Adopted.pdf>, acesso em 16 de julho de 2018.

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

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

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

protected by the domestic law (Federal Constitution and procedural laws). In Article 8, the American Convention ensures due process of law in the course of civil, criminal, administrative proceedings before the national courts of the States Parties, included as a judicial guarantee to be established in domestic legal systems.

In this sense, the Inter-American Court of Human Rights, to whose jurisdiction Brazilian State is subject, has already manifested itself in the concreteness and normative scope of art. 8, as in cases *Castillo Petruzzi/Peru*[98], *Baena Ricardo/Panamá*[99] and *Camba Campos/Ecuador*[100]. As a set of relevant precedents, judgments given by the Court point to the understanding of due process observance as a component of the fundamental rights of the disputing parties or in disputes adjudicated by the national courts; refer to the set of rules that also define the "procedural right of defense", with claims that may be invoked by the defendants not only in criminal cases but also in other matters (civil, labor, commercial, administrative), where there are incidence of procedural guarantees[101].

In accordance with the interpretation consistent with international human rights standards, including the decisions rendered by the Inter-American Court involving matters relating to art. 8 of the Pact of San José, whose hierarchy in the Brazilian order, despite the majority orientation of the Supreme Court, is of a constitutional nature (article 5, paragraph 2, Federal Constitution), at least some consequences can be observed. The immediate application of fundamental rights norms of Internet users - national or foreign resident in Brazil -, in the wake of art. 5, paragraph 1 of the Constitution, and the Internet Bill of Rights, does not, of course, exclude norms provided for in treaties and conventions to which Brazil is a party; on the contrary, include those which provide for procedural guarantees, such as due process (*ex vi* Article 8 of the Pact of San José), and which also concern the integrity of the civil/criminal proceeding brought before the Brazilian courts, if they involve the Internet issues such as search, retention or provision of telematic data, also in civil/commercial, criminal, administrative, security. From another measure, international legal cooperation is also organized based on the observance of the rights and guarantees of the parties in the transnational litigation.

The Brazilian legal system itself, made up of the Federal Constitution, Decree 3.810/2001 and the Internet Bill of Rights, provides for the observance of international cooperation procedures through recourse to MLATs, such as the Brazil-United States Agreement or the Brazil- Switzerland[102], without discretion for mere option or dispensation by the national court. The normative constellation that exists there - and in force - for the material and procedural regulation of facts, situations and juridical relations emerging from the Internet - admitted in its connecting elements of internationality - does not obviate the fulfilment or compliance with international bilateral and multilateral obligations based on treaties of which Brazil is a party. On the contrary, the fulfillment of conventional obligations is reinforced, especially by the express linkage of the Federative Republic of Brazil to principles of international cooperation in all its relations with foreign States.

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

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

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

101 According to the Inter-American Court of Human Rights, "el individuo tiene el derecho al debido proceso entendido en los términos del artículo 8.1 y 8.2, tanto en materia penal como en todos otros órdenes"(Caso Baena Ricardo y otros Vs. Panamá, 2001).

102 Legal Cooperation in Criminal Law Treaty between Brazil and Swiss, from 12 May 2004. Incorporated into the Brazilian legal system by Decree 6.974 / 2009.

10. Argument of the headquarters of the company is not enough to solve the demand

As has been shown above, the intensification of use of internet by the average citizen in the last 25 years has unquestionably questioned the traditional rules of jurisdiction. The digitalization of companies, in turn, accompanies the intensification of data flows between the territories of the States, in their respective jurisdictions. In this context, the frequency of administrative and judicial demands related to access to user data and involving more than one jurisdiction is increasingly common. The legal solutions to typical cases of "conflict of jurisdictions" have been twofold: (1) international cooperation, mainly through the MLATs; and (2) requests for data made directly to intermediaries.[103]

The ADC 51/2017 discusses exactly what should be the predominant solution mechanism to be applied by the Brazilian judiciary. Regardless of the solution defended, it seems necessary to define what should be the criteria for determining the jurisdiction, whether it refers to which law should be applied (applicable law), or which jurisdiction is to enforce (enforcement jurisdiction).

The inadequacy of current paradigms for resolving conflicts of jurisdiction in **cross-border Internet** disputes is evident when the difficulties faced by courts around the world are observed - see the cases already presented in this paper and the ADC itself - when faced with the need to elect a criterion determining competence for the delivery of personal data of users. In this sense, it is important to emphasize that more intense international discussions have been made regarding the delivery of **content data** (such as private communications, photos, e-mails, etc.) of users, and, on the other hand, there is greater consensus regarding provision of **cadastral data and traffic data of the information / metadata** (IP numbers, logic gates, etc.)[104].

At this point of STF analysis of the controversies raised by ADC 51/2017, distinctions between the **provision or retention of content data** and the **provision of user data and traffic data** should be very well delimited, especially as separate regimes are applicable, from the perspective of the validity of the Constitution, the Internet Bill of Rights and the treaties to which Brazil is a party.

However, the problem of determining jurisdiction in the broad sense seems to be aggravated when the courts examine a strict bias demand, taken only in the light of one of the possible criteria for determining the applicable law and enforcement of measures and judicial decisions. Thus, it is important to point out the shortcomings that arise when choosing the seat of the business company as the sole criterion of jurisdiction.

One of the main problems raised by the choice of "corporate headquarters" as a jurisdictional criterion lies in the fact that it often has no relation to the location of the parties and the assets involved in the litigation, with the place where was committed the illicit, or even with the place in which the effects of the illicit act were felt. As La Chapelle and Fellinger:

---

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

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

> Regardless of the physical location of actions or involved parties, the MLAT system de facto imposes the law of the recipient country over the law of the requesting one, even if there is no territorial connection to the latter other than the incorporation of the targeted platform or operator.[105]

The adoption of the company's headquarters as the only jurisdictional criterion has generated frustrations in numerous investigative and law enforcement agencies around the globe (the so called "law enforcement authorities - LEAs"), especially when it is considered that most of the online or digital services of the globe concentrate its headquarters or source of supply in the USA.

Professor Paul Berman, of George Washington Law School, also criticizes the use of the company's headquarters as sole jurisdiction. He states that this element may be arbitrary in certain cases, although it may still be relevant in a broader context. Berman fears that the criterion of the company's headquarter alone can be used to avoid access to certain jurisdictions, based on a deliberate strategy of the parties (forum shopping), analogous to the exclusive use of the criterion of jurisdiction of the place where the data is stored:

> Yet, sometimes, place of incorporation is just as arbitrary and manipulated as data or server location. Individuals with no connection with the United States can easily create a U.S. company and then claim protection of U.S. law (and U.S. courts) even though nothing about the dispute at issue really evinces a connection with the United States.[...] **Thus, if jurisdiction is automatically tied to place of incorporation without any further analysis of the underlying social or economic reality, distortions may result**..[106] (our highlight)

The construction of a solution entails recognizing that it is possible, and often necessary, to analyze more than one criterion for determining the jurisdiction, in a broad sense, depending on the concrete case with which judgment is to be found. International literature and jurisprudence have pointed to the following criteria for determining that a State has a substantial connection and a legitimate interest in requiring certain data stored by a foreign application provider (company), therefore, within the **category of supply or retention of user data abroad**:

1. Nationality of victims and investigated / suspects;[107] [108]

105 LA CHAPELLE, Bertrand de; FELLINGER, Paul. Jurisdiction on the internet: How to move beyond the legal arms race. Observer Research Foundation. 14/10/2016. Accessed in: 10/04/2018. Available in: <https://bit.ly/2Hxy84k>

106 BERMAN, Paul Schiff. Legal Jurisdiction and the Deterritorialization of Data. GWU Legal Studies Research Paper Nº. Maio de 2018. Accessed in:14/04/2018. Available in: <https://bit.ly/2EUqdsq>

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

108 "(3) COMITY ANALYSIS.— For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into

2. Habitual residence of victims and investigated / suspects;[109]
3. The place where the effects of the act or crime were felt;[110]
4. If the online service is directed or accessible to a particular territory[111]
5. Location of company headquarters;[112]
6. Location of the data (servers);[113]
7. The location of those responsible for registering domain names (registrars and registries).

This variety of criteria, not exhaustive, has been developed over some 30 years doctrinal and jurisprudential developments in Europe and the United States, since the commercial expansion of the Internet since the 1990s, which shows that the difficulty of determining jurisdiction, if not relatively new, still remains a controversial issue[114]. The lack of consensus emerges as litigation involving the Internet has multiple dimensions that cannot be ignored by a pragmatic adoption of a single short-term jurisdictional criterion.

11. Additional measures to solve the issue

The various actors that have been debating the topics of internet and international data transfer claim that there are, basically, two solution poles to the problem of jurisdiction, which have varied in different shades of application and combination.

A set of solutions sought to reaffirm the power of regulation and application of sovereign states, whether by means of extraterritorial extension of sovereignty or through reimposition of national borders on the internet. This tendency, named a legal arms race by La Chapelle and Fehlinger, translates, in practice, in laws that establish that

account, as appropriate — [...] (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States[...];". 115th UNITED STATES CONGRESS. The Clarifying Lawful Overseas Use of Data Act (H.R. 4943). 2018. Accessed in: 22/04/2018. Available in: <https://bit.ly/2qXL0WQ>

109 Ibid.

110 Ibid.

111 "The Court of Appeal held that Yahoo! is territorially present in Belgium through its active participation in the Belgian economy and is thus voluntarily submitting itself to the jurisdiction of the Belgian authorities. In particular, the Court of Appeal maintained that Yahoo! participated in the Belgian economy through the use by Yahoo! of the domain name "www.yahoo.be", the use of the local language(s) on that website, pop-up advertisements linked to the location of the users and accessibility in Belgium of Belgium-focused customer services. The Court of Appeal thus concluded that Yahoo!'s refusal to provide IP addresses of the alleged criminals violated Belgian criminal procedure law. [...] For its part, the Supreme Court confirmed all of the Court of Appeal's considerations, essentially linking them to the objective territoriality principle.".L'ECLUSE, Peter; D'HULST, Thibau. Belgium: Supreme Court Condemns Yahoo For Failure To Cooperate With Belgian Law Enforcement Officials. Mondaq. 11 de janeiro de 2016. Available in: <https://bit.ly/2LDFNAO>. Ver também: <https://bit.ly/2O18iVZ>

112 Ibid.

113 SUPREME COURT. United States, Petitioner v. Microsoft Corporation. 27/06/2017. Accessed in: 25/06/2018. Available in: <https://bit.ly/2o42Jhl>

114 From the point of view of private international law itself, transnational issues of the internet offer the development of so-called "pluralism of methods", to affect distinct variations in the determination of applicable law and jurisdiction, particularly by the trend towards modernization of connection rules, such as occurs in the case of pluriconected contractual and noncontractual obligations (torts). This movement has been critically revisited by the excellent work of Professor Horatia MUIR WATT, of the School of Law of Sciences Po, France. About this, cf. CONFLICT OF LAWS.NET, Guest Editorial: Muir-Watt on Reshaping Private International Law in a Changing World. In: http://conflictoflaws.net/2008/guest-editorial-muir-watt-on-reshaping-private-international-law-in-a-changing-world/ Accessed in: 25/06/2018.

servers should be located in national territory (data localisation); blocking of applications by connection providers; enforcing national decisions with extraterritorial effects (for instance, the right to be forgotten - *Google Spain v Costeja*); tighter legal regimes of intermediary responsabilisation (for instance, draft legislation of a Directive and a Regulation in the European Union to oblige internet companies headquartered abroad to designate a legal representative in the EU for data processing requests by authorities); among others[115].

The other solution pole has the goal of fomenting greater international cooperation between countries. In an extreme of this pole are found few advocates for an international treaty of global reach that would regulate the matter substantially, as in the United Nations Convention on the Law of the Sea and in the Outer Space Treaty[116].

The Internet & Jurisdiction organization believes that the most viable solution would be the creation of a permanent institutional multistakeholder environment (with States, companies, civil society, and the technical and academic community) that allows representatives of the several groups affected at a global level to develop efficient standards and mechanisms for international cooperation together, going further than the current models. The organization's position is inspired in the open, multistakeholder and transnational governance process of the technical layer of the internet (IPs, domain names, protocols, etc) which allowed for the exponential growth of the network through the adoption of universal standards.

Due to the understanding that a harmonizing of substantive law is unrealistic regarding the traditional mechanisms of international law, the organization advocates that the focus of the multistakeholder network should be seeking: (1) common procedural patterns, in order to ensure a minimum of interoperability between jurisdictions;[117] and (2) ensure due legal transnational process concerning cooperation requests, with an emphasis in answering "how the requests should be submitted" and "how they should be evaluated"[118]. In this sense, the norms and standards created through multistakeholder consensuses would have the status of public policy standards that could be adopted in scale and implemented either through simple best practices guides as well as through normative obligations derived from national law or international treaties. As La Chapelle and Fehlinger conclude:[119]

> Addressing issues related to governance "on" the Internet requires a paradigm shift: from international cooperation only between states, to transnational cooperation among all stakeholders; from pure intergovernmental treaties to policy standards; and from intergovernmental institutions to issue-based governance networks. Far from a rejection of traditional international cooperation, however, this is proposed as a constructive extension – a way to look at current practices in a new, generalized light.[...] Both have their respective zones of

115 CHAPELLE, Bertrand de la; FEHLINGER. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. Abril de 2016. pp. 10-11. Accessed in: 26/04/2018. Available in: <https://bit.ly/2uh34Li>.
116 Ibid, p. 11 e 17.
117 CHAPELLE, Bertrand de la; FEHLINGER. Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. Abril de 2016. pp. 21-22. Accessed in: 26/04/2018. Available in: <https://bit.ly/2uh34Li>.
118 Ibid, pp. 23.
119 Ibid, pp. 24.

> validity. Likewise, the type of transnational cooperation envisioned here in no way suppresses or reduces the relevance and authority of existing governance frameworks, in particular national governments. On the contrary, multi-stakeholder processes can produce policy standards that inform the reform of existing interstate cooperation mechanisms, and policy standards can even later be enshrined by traditional multilateral organizations. **The global community needs to step up efforts to avoid the negative consequences of a legal arms race, preserve the global nature of the Internet and address its misuse. We need innovative cooperation mechanisms that are as transnational as the Internet itself and the necessary policy networks and ongoing dialogue processes to produce them.** (emphasis is ours)

Still on the international cooperation pole, new initiatives that focus on fomenting greater bilateral cooperation emerge, such as bilateral treaties to provide data directly from companies to foreign authorities, as established by the recently passed CLOUD Act.

The questions raised by ADC 51/2017 clearly reflect existing concerns regarding unilateral taking of solutions by countries around the world. If ADC 51/2017 is granted, it will ensure both legal certainty for companies operating in the internet segment in Brazil and higher levels of protection for the private communications of Brazilian users, particularly in view of the nature and location of the data accessed.

However, dilemmas faced in the obtention of digital communication by jurisdictional bodies in criminal investigation, which, in many cases, result from legitimate necessities, will remain still. The very realist scenario could lead such bodies to adopt direct invasion techniques to electronic devices of those investigated, in other words, hacking techniques or clandestine obtainment of communication contents as a way to bypass the problems of cooperation and evidence seizure, since the current mechanisms for international cooperation become inefficient in many cases. Such investigative techniques do not have specific regulations in Brazil, and may therefore represent another door to various institutional abuses, if not accompanied by checks and balances and adequate judicial oversight.

The fear of organizations dedicated to regulatory and social internet issues, such as IRIS, is that unilateral practices of criminal prosecution authorities in Brazil might forward a negative tendency of criminalisation abuses of legitimate uses of the internet and punishment of citizens-users, without due legal process, all still present in Brazilian reality and of other countries around the globe.

On the other hand, should ADC 51/2017 be held invalid - with the understanding that international cooperation agreement would be only an option for cases of involving breach of confidentiality regarding Brazilian data in foreign territories due to alleged criminal acts practiced in Brazil - a double risk emerges: on one hand, the attribution of liability to the Brazilian State regarding positive international law violation because of unilateral practices adopted, including non-observance of rights and guarantees of the parties of the legal process; on the other hand, the risk of imposing obligations to companies that violate foreign laws. This is because they would be susceptible to conducts that don't conform to national law of the States involved and in which jurisdiction data is

reached and accessed. In addition, legal uncertainty can be a factor of disistimulation to investments of those companies in the country, being also a barrier to the entrance of small and medium sized companies.

Due to the cross-border and multistakeholder nature of the internet, it is likely that any unilateral attempt of solution in matters regarding obtainment of data will be inefficient in medium and long term. Thus it is necessary the acting of the Three branches of power, representing the State, as well as several other actors involved (civil society, companies, academic community and international organizations) in seeking an active solution, regardless of which pole Brazil approximates in attempting to address the matter of ADC 51/2017.

12. Modernization perspectives and the complementarity of international engagement of the three powers

Notwithstanding its acknowledgement in several fields of the Brazilian internal legal system, the debate over the relationship between international law and domestic law demands a revision, as the one provoked by the ADC 51/2017. In times of so-called "global governance", States, international organizations, non-governmental organizations, companies and individuals are increasingly bind to the observance of international norms. As recipients of rights and obligations in the international order, these subjects occupy a prominent position in the abidance, support and guarantee of the application of international law by State bodies.

Especially with regard to the Federal Constitution of 1988, it is necessary to revise the roles attributed to the three branches of power in the organization of the Brazilian State in international relations, in order to bring them closer to the idea of a global constitutionalism. Even if Brazil currently privileges a consented solution with the acceptance and compliance with international norms, in particular in the domain of international human rights law, the divergences between monism and dualism raise incongruencies.

Besides the interdisciplinarity that the theme of treaties application presents (political science, international relations and constitutional law), it also demonstrates the lack of dialogue between the powers constituted in the State. As occurs in other legal systems, this controverted relation appears to be a problem both of conflict or convergence between political and constitutional attributions, with effects concerning both the compliance of State obligations internationally and the application of international norms by domestic courts. Thus without balance or complementarity of attributions, it is possible that there are distortions and that this model is not desirable or convenient to countries that claim space and insertion in international relations, as is the Brazilian case.

The norms of domestic law are created according to competencies and procedures acknowledged by the domestic constitutions of the States (therefore, according to constitutional provisions), and are intended to regulate facts and legal relationships subject to a territorial supremacy. International law norms, on the other hand, are elaborated and produced, from a traditional perspective, by States and international

organizations. They are destined to regulate international relations, and according to the respective competencies attributed to these subjects in the international order, as the powers conferred by domestic constitutions (States) and the powers conferred by constitutive statutes (international organizations).

The most important consequence of this interaction results from international social reality: States, international organizations and individuals become **bound to comply with international norms and enforce them**, especially as long as they are recipients of rights and obligations in the international order. The contemporary tendency is to reject the theory of transposition of international norms and admit its automatic incorporation and mandatory efficacy in the domestic legal systems[120].

There is a distinction between norms of immediate application (or *self-executing*) and norms of non-immediate application. This difference always presupposes that international standards are capable of producing effects in the domestic system, so that the State is bound to comply, in accordance with the requirements established in its Constitution and with the very provisions of the international act under consideration[121].

This matter, especially, is often left to interpretation by higher courts (or by the constitutional review body) in States that admit the automatic incorporation of treaties, diverging, mostly, over the moment in which it occurs: since the ratification of the treaty, which is authorized by the legislative body (minority of cases); or (ii) from the moment of the effective deposit of the instrument of ratification by the Executive Branch with the receiving authority, with which the treaty enters into force at the international level. However, it should be noted that there should be greater participation among the different Powers in the elaboration, assumption, and application of international obligations. In the courts, there is a need for greater reflection on international norms and their effective status in the national legal system, as well as for the development of cooperation networks between courts, magistrates' associations and judicial auxiliaries.

Within the Legislative Branch, it is necessary to call for greater involvement of congressmen in Brazilian foreign policy agendas. This could be accomplished, initially, through initiatives such as the White Paper of Brazilian Foreign Policy of the Ministry of Foreign Affairs, which called for members of civil society and various sectors of the Government in its elaboration[122]. In National Congress, in turn, there is a clear demand surrounding draft legislation that is in conformity with current trends of sensitive issues of international contemporary agenda. In this perspective, it becomes crucial to monitor

120 On this subject, Napoleon Miranda states that: "The way this process is occurring, in particular due to the increasing binding of States to international bodies with the power to interfere over the definition of internal public policies, would be producing, in practice, a limitation to the sovereignty of States, thus requiring a redefinition of the sovereignty of States at the international level, in order to take account of the new reality. The most meaningful example of this phenomenon, it seems, is that which relates to the long process of constitution of the European Union, which, for over a decade – since the Maastricht Treaty in 1991, with the constitution of the European Central Bank, responsible for the formulation of a unified internal monetary policy in the eurozone – has been forming a broad set of legal, political and economic instruments that demand from States that adhere to them a limitation, albeit not elimination, of their sovereignty in order to autonomously define the various mechanisms for the management of national public order". MIRANDA, Napoleão. Globalização, soberania nacional e direito internacional. In: Revista CEJ, 2004. Available in http://egov.ufsc.br/portal/sites/default/files/anexos/21938-21939-1-PB.pdf>. Access in November 29, 2014.

121 Observing the technique of Public International Law and Constitutional Law, in terms of treaties, express and formal manifestation of the will of the State is required, which is concretized through a complex act exteriorizing the internal sovereignty in the plan International. In general, the Executive Branch, represented by Heads of State, Heads of Government and Ministries of Foreign Affairs, negotiates and concludes treaties; the legislature (parliament or congress) may authorize the conclusion and ratification of the treaty agreed by the State in its external relations. With regard to the customary international norm, respect is fulfilled through observance, practice of internal bodies or acceptance, through silence, of the practice of others.

122 So far, however, there is no information on the launch of the publication by the Ministry of Foreign Affairs, which has been systematically levied since 2014 by civil society organizations and government entities. See status at: http://www.ebc.com.br/livro-branco-da-politica-externa-brasileira.

the debates in course in the International Labor Organization (ILO), the United Nations Human Rights Council, the Organization for Economic Co-operation and Development (OECD), the Internet Governance Forum (IGF), among others.

By means of coordinated and symbiotic actions, and not merely subordinated actions, it is possible to promote effective participation of all three powers in the formulation of the Brazilian international agenda. The Judiciary cannot distance itself from the contemporary paradigms of legal pluralism and discursive legitimacy of international norms. Although the incorporation of international acts into the Brazilian legal system leads to the possibility of its constitutional control, the decisions must consider its repercussion, for Brazil, in the international system. In this way, it is necessary to have symbiosis between the three powers in the treatment of issues related to foreign relations simply to avoid that a unilateral act of Brazil impacts the international system. Decisions, such as that of ADC 51/2017, should avoid exposing the Brazilian State to the risk of non-compliance with international obligations and eventual responsibilization at an international level.

13. Recomprehension of sovereignty and jurisdiction sharing

The internet not only figures as an improved technical structure based on modern communication and connection standards. In the course of its evolution for civil and commercial uses since the ending of the decade of 1990, it has been a true space of transnational information and technologies. State and non-state actors, as well as organizations, companies, and individuals, participate in distinct interactions that project themselves beyond merely territorial borders. While the State remains with certain regulatory, adjudicatory and executive powers, it is also possible to verify that the traditional understanding of sovereignty, a legacy of the Westphalian order, undergoes conceptual and operational relativizations that are very concrete.

States can no longer exercise full control over behaviors, practices, and transactions over resident and domiciled people in their territories without recurring to compliance with international obligations and cooperations with other States and organizations. The notion of sovereignty immediately related to this system has been mitigated in the last thirty years, with the advancement of globalization and information and communication technologies, in favor of transnational processes centered on actors other than the State[123].

Part of this process of transformation of the traditional sovereignty paradigm stems from the effects of globalization on the organization and projection of multinational economic groups and the new dynamics in capital and services flows. The traditional structure of these multinational economic groups has undergone a transformation that, at first glance, may seem paradoxical. At the same time that its expansion and projection radius increased considerably around the globe, a number of essential structures that were to be distributed together with the transnationalization of the company ended up, instead, concentrating heavily on regional high-tech centers, qualifications, and

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

services[124]. The international reach of firms becomes, therefore, inversely proportional to the centralization of their most essential value-producing hubs[125].

In the case of internet companies, these centers take the form of their research and development (R&D) departments, data centers and technical operation centers, to the detriment of foreign subsidiaries that serve only as a spearhead for the conquest and better use of new markets. An illustrative analogy would be the comparison with the colonial empires of the Modern Age: although their territorial extensions had reached proportions dozens of times greater than their original territories, and their presence was considerably more spread throughout the globe, wealth and political power were almost completely centralized in the metropolis. Unlike these empires, however, States are increasingly obliged to cooperate with – not to impose themselves on – one another as a way of safeguarding their interests (and even their material sovereignty) in the best possible way.

The essence of cooperating – and not simply coexisting (as was characteristic of the international order prior to the emergence of the United Nations in 1945, among the stated reasons for peace and international security), is that it still characterizes the dynamics of transnational relations today. This factor is connected to the reality of increasing regulatory, adjudicatory and executive jurisdictional interdependence between state and non-state actors - and is still based on **compliance with treaties and conventions**, but also on meeting certain legitimate expectations involved in international economic transit[126]. They are manifested in several areas of intense factor mobility: goods, capital, services, technologies, and information – in the fields of trade, environment, intellectual property, taxation, investments, protection of human rights and global anti-corruption efforts.

The internet's architecture, as it is known, from a global and multi-territorial nature, and a decentralized and reticular structure, seems to advocate specifically for a change of conception of sovereignty and jurisdiction, from different perspectives: political, economic, juridical-substantive and procedural. Jurisdictional spaces between States are no longer exclusive or in conflict; they organize themselves in sharing. Such sharing is necessary so that domestic and intercommunity (as in the case of the European Union) administrative and jurisdictional authorities can solve issues involving both the regulatory and the litigious side of interactions between governments, companies and internet users[127].

One of the most concrete manifestations of **jurisdictional sharing** is the coordinated decision between States and organizations to regulate substantively and procedurally the relationships and interactions that emerge from the internet, such as in commerce and electronic contracts, data processing, private communications,

124 About this topic, see, cf. SASSEN, Saskia. *Global city*. Princeton, NJ: Princeton University Press, 1991.

125 From the phenomenon of internationalization of economic groups business activity - especially those that include internet application providers – one can observe the emergence of various legal debates. Among them, one of the seemingly most controversial nowadays concerns the possibility of holding a company belonging to an economic group – most often a subsidiary or affiliate - accountable, as a result of a conflict that relates, in fact, to the company that controls that particular group of companies. National jurisprudence, from second instance decisions to decisions of higher courts, finds itself in dissent on the subject, presenting grounds often discordant for decisions even when they lead to the same factual outcome. For example, one can cite the decisions of the interlocutory appeal nº 2184235-15.2016.8.26.0000, from the Court of Justice of the State of São Paulo, and of the Crime Warrant nº 1.396.365-4, from the the Court of Justice of the State of Paraná - these decisions, diametrically opposed in their results, demonstrate, in short, the central merit of this argumentative divergence.

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

127 Idem, p.75.

and intellectual property. The explanation seems more intuitive, since it is the option provided by international law and Community law (eg European Union law) to facilitate and promote models of harmonization, standardization, unification of private law - civil and commercial - especially for facts, situations and legal relationships that are linked to different legal systems, affecting, therefore, human interactions that transcend borders and are of global concern.

Since the end of the 1990 decade, with the advent of the Internet, the United Nations Commission on International Trade Law (UNCITRAL), for example, has intensified its work on preparing treaties, conventions and model laws to bring the legislative formulas in electronic commerce, form, certification of signatures, data security and trust in electronic contracts[128]. The role played by UN Members in these fields, as revealed by UNCITRAL's competencies, demonstrates the need for ongoing studies and efforts around the understanding and maturation of integrated communication and information technologies in e-commerce. These solutions still could not remain unilateral by domestic legislative models, under the risk of normative fragmentation.

The same can be claimed in relation to the limits that can be posed to the tendencies of unilateralization of law application or the extension of its effects to reach facts or situations that occurred in foreign territories (such as the extraterritorial application of domestic law). They should guide restrictively the choices of prescriptive/regulatory jurisdiction because there are areas of sensible regulation and public interest that can justify them (e.g. taxation, antitrust, environment, criminal persecution, and cross-border violation of human rights). However, this choice could not be merely adopted by States without a balance with respect to political, economic and social repercussions inside their territories and beyond their domestic borders.

Another expression of jurisdictional sharing results from the aspect of **legal cooperation** for the application of legislation, acts and decisions through which administrative authorities and domestic courts of states and regions/communities. It is a key piece in understanding the issues raised in the controversy regarding ADC 51/2017.

In the course of the transnational civil procedure (or international private contentious), it is possible to verify how cross-border litigations on the internet depend on the sharing of jurisdictional spaces, particularly to the adequate functioning of justice and access to jurisdiction by internet users and companies.

States, in the same manner, remain supported by structures of international legal cooperation which present themselves positively regulated, as in the formulas offered by treaties and domestic laws (In Brazil, the Constitution, procedural codes and regulations) and centered in cartorial-bureaucratic models, because they depend on the action of central authorities, courts and, residually, diplomacy. On the other hand, they also depend on the entanglement and participation of non-state actors for legally solving litigations, particularly in specialized domains involving organizations, individuals, civil society and industry.

In the field of internet and jurisdiction, governance matters are also primary and admit today the necessity of multistakeholder dialogue that wouldn't be far from

128 See, for instance, the normative products developed by UNCITRAl in treaties and model laws and principles, recommendations: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html. For the theme's evolution, see POLIDO, Fabrício B. P. e OLIVEIRA DA SILVA, Lucas Savio. Contratos internacionais eletrônicos e o direito brasileiro: entre a insuficiência normativa doméstica e as soluções globais. In: *Seqüência: Estudos Jurídicos e Políticos* vol. 38 (2017), p.157-188.

the goal of seriously discussing forms of control and effectiveness of the mechanisms in force for international legal cooperation for solving transnational litigations on the internet.[129]

14. Conclusions

In light of what was exposed, and as formerly expressed by IRIS in its participation as 'Amicus Curiae', one observes a necessity for the legal controversies concerning the ADC 51/2017 and its repercussions in constitutional matters to be scrutinized by the Supreme Court with due urgency and interpretative precautions concerning constitutional norms and treaties and conventions to which Brazil is a party.

With ADC 51/2017, the Supreme Court has also the opportunity to consider emergent issues of multistakeholder nature regarding internet regulation and compliance with international legal cooperation regimes in the course of civil, commercial and criminal transnational litigation concerning the world wide web.

It is true that the lack of coordination in international legal cooperation structures and the lack of standard jurisdiction criteria to the solution of litigations on the internet could raise difficulties even more present in the daily life of courts and administrative authorities dealing with transnational litigation. Such flaws, however, could never be taken as grounds for overruling justice and suppressing fundamental steps in the process regarding fundamental rights of the parties and of those that are daily affected by the claims adduced in court - internet users, their personal data, and the content of their private communications.

In the same manner, as has been noted through the Memorial, the Brazilian legal system, which integrates norms from the Federal Constitution, the Civil Process Code, the Decree nº 3.810/2001 and Brazil's Internet Bill of Rights, establishes - and does not exclude - the observance of international cooperation procedures through the use of cooperation agreements and mutual legal and administrative assistance, as represented by the Brazil-United States Agreement and the Brazil-Sweden Agreement. From IRIS' point of view, the normative constellation that exists in force for the material and procedural regulation of facts, situations and juridical relations emerging from the internet - admitted in its elements of connection, of internationality - **does not repeal abidance to international bilateral obligations and multilateral agreements based on treaties of which Brazil is a party**.

On the contrary, compliance with conventional obligations is emphasized and assured through express binding of the Federal Republic of Brazil to the principles of sovereignty, non interference in internal affairs, and international cooperation in all of its relations to foreign states, as established in the article fourth of the Constitution. As in other areas - environment, human rights, global anti corruption efforts, taxation, antitrust efforts - with strong appeal to extraterritorial application of national legislation (an exceptional aspect of jurisdiction), the internet would not be immune to the incidence of international legal cooperation rules. This is, in short, due to the fact that cooperation is what ensures both dialogue between and sharing of jurisdictions in the global order.

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

15. Bibliographic references

Books and papers

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Laws and rulings

BRASIL, *Decreto nº 3.810*, de 2 de maio de 2001. Available in: <https://goo.gl/oiE1G3> Accessed in: 02/04/2018.

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

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

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

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

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

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

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

CONVENÇÃO SOBRE O CIBERCRIME - Budapeste, 23/11/2001. Accessed in: 05/03/2018. Available in: <https://goo.gl/twrwQu>.

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

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

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

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

Data (CLOUD ACT). 2018. Accessed in: 22/03/2018. Available in: <https://goo.gl/4gn81j>.

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

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

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

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

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

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

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

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

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

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

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

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

561 U.S. 247 (2010).18/07/2012. Accessed in: 05/03/2018. Available in: <https://bit.ly/2GbTd08>.

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

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

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

Other documents and news

Coalition Letter Opposing the CLOUD Act. 12/03/2018. Accessed in: 23/02/2018. Available in: <https://goo.gl/qYB2EG>.

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

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

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

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

FACEBOOK Inc. Relatório de Transparência. 2016. Accessed in: 23/02/2018. Available in: <https://goo.gl/aLZQZh>.

FACEBOOK Inc. Guidelines - Informações para Autoridades Policiais. Accessed in: 23/02/2018. Available in: <https://goo.gl/uYDvfX>.

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

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

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

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

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

SYMANTEC CORPORATION. Norton Cyber Security Insights Report 2017 Global Results. 2018. Accessed in: 15/02/2018. Available in: <https://goo.gl/RC7q5i>

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

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

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

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

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