Institute for Research on
Internet and Society

LOGIC GATES AND ACCESS RECORDS

FROM TECHNICAL POSSIBILITIES TO JUDICIAL REASONINGS IN BRAZILIAN COURTS

IRIS
Institute for Research
on Internet and Society

Institute for Research on Internet and Society

LOGIC GATES AND ACCESS RECORDS

FROM TECHNICAL POSSIBILITIES TO JUDICIAL REASONINGS IN BRAZILIAN COURTS

How to reference this paper
LIMA, Iara Vianna et al. **Logic gates and access records:** from technical possibilities to judicial reasonings in brazilian courts. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2017. Available at: http://bit.ly/36cGsyK. Access: DD mmm. YYYY

IRIS
Institute for Research on Internet and Society

SUMMARY

1. Introduction[1]

"The linkage between technical and public policy issues is of particular importance in the governing of the Internet."[2] The exhaustion of version 4 of IP (IPv4), the implementation of its version 6 (IPv6), and the sharing of IPs as a transitory solution reflect the relationship between the Internet architecture, its technical layer, and that of public policy, regarding access and the operability of the internet. This problem still results into legal consequences in cases where access records are required in criminal investigations and legal proceedings of a varied nature, in order to identify a specific user.

An Internet Protocol (IP) address is a numerical sequence used to identify a device connected to the Internet, and to guide the data packets that arrive and leave that device. In the process of transition of the IP versions, the problem of depletion of the IPv4s blocks has been solved by sharing among several users of the same public IP.This was the technical solution chosen in Brazil, and in several other countries, so that the expansion of the Internet was not interrupted in the transition period of protocols. Thus, it was the responsibility of the connection providers to implement the sharing techniques called Network Address Translation (NAT). With these techniques, additional difficulties have arisen to identify online users who use shared IP. In this regard, courts are being asked to provide so-called "logic gates", which designate an additional numerical sequence used in conjunction with an IP number to identify the location of devices connected to the internet.

As the term "logic gate" is not expressly written in the text of the Brazilian Civil Rights Framework for the Internet (Bill 12.965 / 2014), the Brazilian Judiciary has been requested to respond if:

- Is there a legal obligation to store data relating to "logic gate?
- If yes, who is responsible for storing and making these data available to the competent authorities: the connection providers, the application providers, or both?
- Is the logical gate data necessary to identify users who access the Internet through shared IPs (provided by the connection providers)?

Based on these questions, this study seeks to integrate technical issues, regulatory options and judicial interpretations on the responsibility of record and requests that reach the Judiciary related to the transition period from IPv4 to IPv6 in Brazil.

The study addresses first the technical aspects involved in logical gate record keeping, either by application providers or by connection providers, and how the issue has been addressed in the European Union and Australia. Then, the methodology of analysis and decision scanning, application of variables, and data collection are presented. Finally, the results of the research of judicial decisions on the subject are presented, in order to delineate the characteristics of the decisions, their devices and fundamentals. Thus, the study proposes to understand arguments and the solutions given by the Brazilian courts.

1 This study was carried out under the coordination of Fabrício B. Pasquot Polido, Lucas Costa dos Anjos and Luiza Couto Chaves Brandão, members of the Internet and Society Reference Institute (IRIS). Contributed as coauthors and researchers for this work Iara Vianna Lima, Lucas Costa dos Anjos, Luiza Couto Chaves Brandão, Odélio Porto Júnior, Pedro Vilela Resende Gonçalves, Victor Barbieri Rodrigues Vieira. Translated into English by Lucas Costa dos Anjos and Luiza Couto Chaves Brandão.

2 WEBER, Rolf H. *Shaping internet governance: Regulatory challenges.* Springer Science & Business Media, 2010, p. 187.

2. Some technical clarifications required

The IP, or *Internet Protocol*,[3] is the main communication protocol on which the internet is based as we know it today. The IP works by means of encapsulated data packets that can be transmitted via various means of telecommunication. It also defines the addressing mechanisms for identifying the source of these packets. A common analogy to IP is one that compares data packets to letter envelopes containing a given content. The IP Protocol would be compared to the mail system that identifies both the recipient and the sender and does everything necessary to take the letter from one system user to the other.

The IP identifies its recipients and senders from the so-called "IP address", represented by a set of four numbers up to three digits (e.g. 192.168.1.100) that allow data packets to be transmitted between terminals connected to a network. Currently, the predominant version of the protocol is the fourth, IPv4, widely used by the commercial Internet since its inception in the 1990s. IPv4, however, has a limited number of addresses, which have run out after increasing demand for access to the Internet in the decades following its implementation.

Already predicting the exhaustion of IP numbers, experts proposed in the 1990s a new version for the protocol. Internet Protocol Version 6, or IPv6, uses four hexadecimal digits that allow a virtually inexhaustible amount of addresses. While IPv4 predicted a total of 4.3 billion addresses (less than one for each person on the planet), IPv6 predicts a total of 3.4 × 1038 addresses (more than the estimated total stars in the known universe!).

The IPv4 addresses were distributed irregularly and arbitrarily among macro regions of the globe in the 1980s and 1990s. The IPs delegated to the body responsible for the macro-region of Latin America and the Caribbean (LACNIC) were exhausted in 2014. In other regions of greater Internet penetration, IPs have been depleted more quickly. Still in the face of asymmetric characteristics of global Internet regulation, the demand for new connections - and consequently of IPs - continued to grow. To circumvent the problem, a number of tools have been developed to allow connection providers to continue to expand access in their regions of operation. One of them is offered by the Network Address Translation (NAT) system, which allows the "sharing" of a single IP between several computers, as a way to mitigate the exhaustion of IPv4 until the complete implementation of IPv6.

The NAT (Network Address Translation) system

During the IPv4's development, a certain number of addresses were reserved for "private IPs", which would be used in private networks not connected to the internet as a whole. In addition to private IPs, a number of public (or global) IPs have also been assigned, and these IPs are used to perform most Internet connections. The NAT system bypasses the IP exhaustion problem by allowing multiple devices on a private IP network to share a single public IP when they want to connect to an external network, the Internet.

For the sharing to take place, the router, be it the home router, or the one used

3 Defense Advanced Research Projects Agency, "Internet Protocol: DARPA Internet Program Protocol Specification". *IETF*, RFC791. Setembro de 1981. Available at: <https://tools.ietf.org/html/rfc791> Acess: 20th September 2017.

by a larger connection provider, acts as an intermediary between the internal network connected to it and the Internet. By associating the private IPs used in the internal network and one or more public IPs assigned to that router, the NAT system directs the data packets in and out through it, using ports that allow it to identify which device connects with which external address. Ports are a number appended to the end of the IP address, which allow NAT to create a membership table and enable its function.

Private IP	Public/Global IP
192.168.1.103:3663	152.238.154.3:3663
192.168.1.101:4554	152.238.154.3:4554
192.168.1.105:2882	152.238.154.3:2882

Table 1. Example of Address Binding Table

According to the table above, it is possible to notice that the Public IP used by the three internal addresses is the same: what differs them, however, is the logical port at the end. In this case, the logical gate allows a kind of address variability. Private IPs, for their part, were already different from each other, and yet they have a logical gateway added to them to help the NAT system associate them with Public IP. The equivalence between the port added to the Private IP and that added to the Public IP, although a predominant practice, is not absolute.

For example, if a certain number of IPs were assigned to a connection provider, but this provider caters to a much larger number of clients and devices than it has IPs, a NAT system is required to communicate with the external network. Through logical port management, you can share a global IP between multiple connected devices, knowing the source and destination of each packet addressed to the router. Even if all packets are destined to the same IP, they will be differentiated by the router of the provider, through the connection table and the logical ports attached to them.

Let us suppose that John wants to obtain from a given website or application the weather forecast for Belo Horizonte. When sending a data packet containing the question “What is the weather forecast for Belo Horizonte?”, this package will leave your device marked with a source address and a destination address. By being connected to a router (which can only connect devices from the same home, or can connect dozens of clients from a connection provider), the source address will be a Private IP of that internal network (eg 192.168.1.2), and the destination will be the public IP of the server hosting the website, or application (for example, 40.41.42.43). The packet would then start from John’s computer as follows:

From: 192.168.1.2

To: 40.41.42.43

“What is the weather forecast for Belo Horizonte?”

As there are other devices connected to that router, the NAT system will have to be triggered to connect the John device to the server from which the information will come. To do so, it will add a port to the private address (for example, 192.168.1.2:3662) and associate that private address with a public address, which will be used to receive the response later (for example, 10.11.12.13:3662). For the router, the packet would then be addressed as follows:

From: 192.168.1.2:3662

TO: 40.41.42.43:80

"What is the weather forecast for Belo Horizonte?"

Because the destination server will not be able to connect to the designated IP and port, because it is a Private IP, the router's NAT system will then redirect that packet to the destination through a Public IP. For the internet, whatever the recipient, the data seems to have come from the router itself. The packet would then leave the router addressed as follows:

From: 10.11.12.13:3662

To: 40.41.42.43:80

"What is the weather forecast for Belo Horizonte?"

Through the associated Public IP, the weather forecast application server can respond to the request. In the meantime, the router to which the John device is connected will have inserted the following association in its table::

192.168.1.2:3662 = 10.11.12.13:3662

The server containing the weather forecast information would then return a packet addressed in this way to the router:

From: 40.41.42.43:80

To: 10.11.12.13:3662

"Minimum of 15 degrees and maximum of 24"

However, the address in question does not identify the John's device for the external network, only for the router responsible for mediating communication. Upon receiving this packet, it will query its table to find out which internal network address was associated with the address 10.11.12.13:3662 and then redirect it to the John's device.

Using the letter analogy already mentioned above, the NAT system would function as the employee of a multi-family building, responsible for redistributing the incoming mail to that address. If Ana da Silva, who lives in apartment 303 of Solar Condominium, Guajajaras Street, n. 13, sends a letter to the City of Belo Horizonte, Av. Afonso Pena, n. 1212, she will leave the address with this addressee, but her sender would be something like: Guajajaras Street, n. 13, 303. Any response from the city hall that is sent to Guajajaras Street, n. 13, 303, will first pass through the hands of the employee, who will know that the apartment 303 is the residence of Ana da Silva, and then will deliver it.

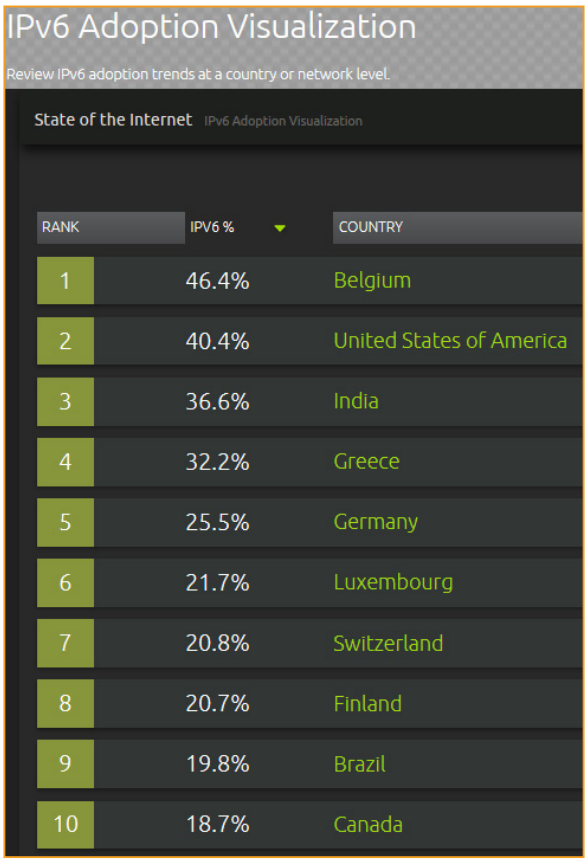
NAT and *Carrier-Grade* NAT

The first NAT applications were performed for Local Area Networks (LANs), when each client of a connection provider received its own IP and shared it between the devices of their residence or work. With the progressive depletion of IPs, NAT was also used by connection providers: from a system to share addresses among half a dozen devices, a system was developed that met the needs of thousands of users of the connection providers.

The NAT used on a large scale by connection providers is called NAT444, Carrier-Grade NAT (CGN) or Large Scale NAT (LSN). This last term is considered the most accurate because it is only a large-scale version of the same system used by local or small-sized networks.

Implementation of IPv6 in Brazil[4]

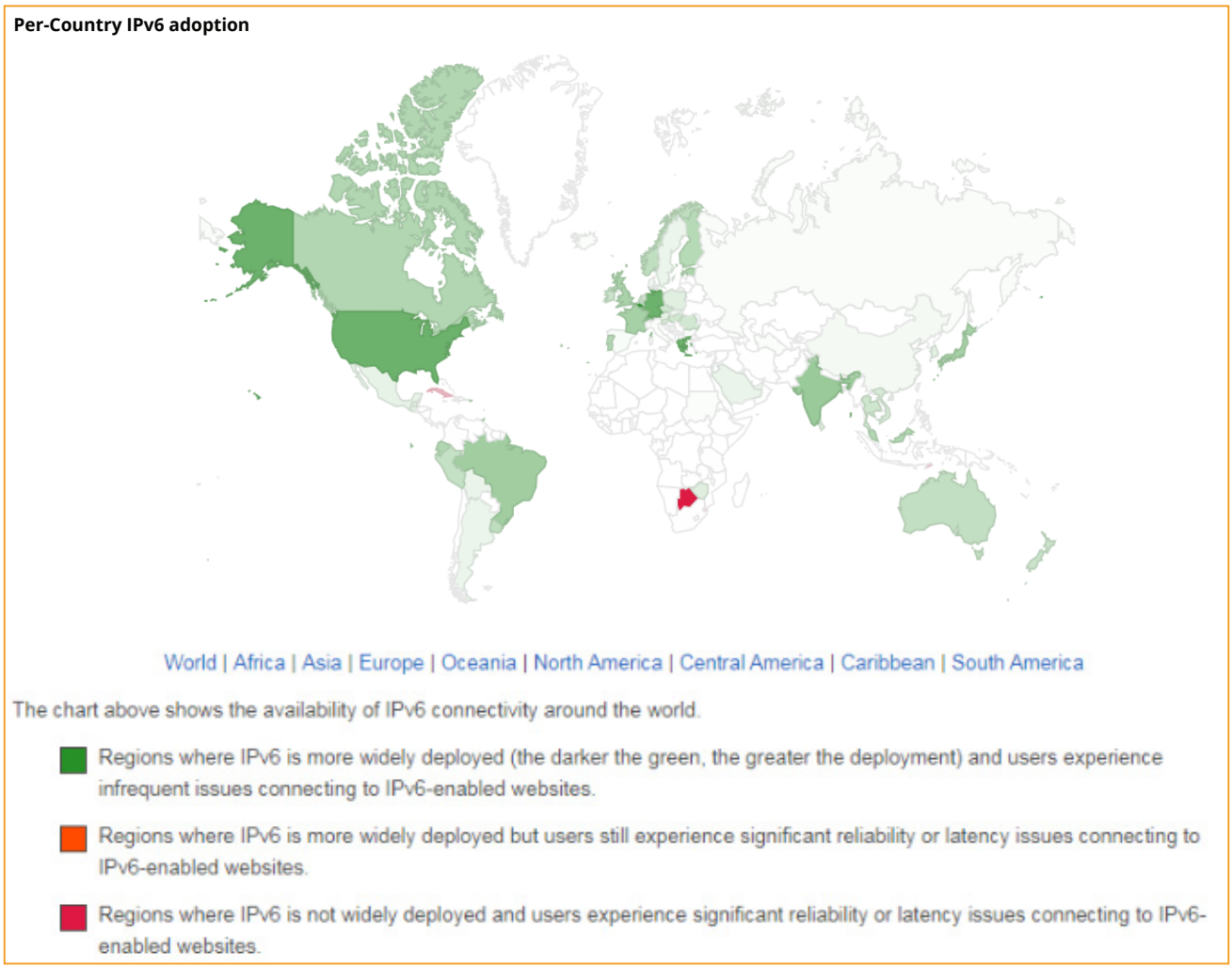
With the depletion of the IPv4 block around the world, as mentioned above, several countries and agents involved have sought to deploy IPv6 in their networks and services. The American company Akamai Technologies Inc. performs periodic measurements on the use of IPv6 in the world, based on the traffic in their networks. For Brazil, the company estimates that there is an adoption of 19.8% of IPv6, placing the country in 9th overall position:[5]



[6]

4 For more information about the IPv6 in Brazil and the world: <http://ipv6.br/>.
5 Table available at: <http://bit.ly/2kzWeRD>. Access: 09/10/2017.
6 Table available at:: <http://bit.ly/2kzWeRD>. Access: 09/10/2017.

The Google company points to similar data for adoption of IPv6 in Brazil. It estimates that 20.17% of data traffic in Brazil is in IPv6, ranking it as a high-level implementation country, and in which there are few connection problems with Google sites:[7]



As noted in the chart, Brazil's situation in terms of IPv6 adoption is similar to that of countries with considerable internet penetration and belonging to the group of developed countries of the northern hemisphere and developing countries of the southern hemisphere. In a similar estimate, the Asia-Pacific Network Information Center points to a capacity of 20.97% of IPv6 for Brazil, which places the country in 14th place in the ranking of this type of connection[8].

3. The Brazil's Internet Bill of Rights and the logic gates

The Brazil's Internet Bill of Rights establishes two categories of data that must be stored, necessarily: the **connection records** and the **records of access to the application**. The legal provision for keeping this data is to facilitate the identification of Internet users by the competent authorities and by judicial order (article 10)[9], because user responsibility is one of the principles of internet use in Brazil, according to art 3, VI[10], of the

7 Google IPv6. 2017. Available at: :<http://bit.ly/2yazwEE>. Access: 09/10/2017.

8 Ranking by the Asia-Pacific Network Information Centre: <https://stats.labs.apnic.net/ipv6>. Also available at: <http://ipv6.br/>.

9 Art. 10. Maintenance and disclosure of Internet connection logs and Internet application access logs contemplated in this Law, of personal data, and of the content of private communications must respect the privacy, private life, honor, and image of the parties directly or indirectly involved.

10 Art. 3. The following principles underlie Internet governance in Brazil: [...] VI - holding agents liable for their actions, as provided for by law;

same law.These records may also be used for commercial purposes, provided that with "free, express and informed consent" (article 7, VII)[11].

According to the Framework, connection records are defined as "the set of information regarding the start and end date and time of an internet connection, its duration and the IP address used by the terminal for sending and receiving data packets ". Your guard is up to the system administrator[12], which must ensure its protection, for a period of one (1) year (article 13)[13].

On the other hand, application providers[14] established "in the form of a legal entity and carrying out this activity in an organized, professional and economic manner" have the obligation to store for 6 months[15] the "set of information regarding the date and time of use of a certain internet application from a given IP address ", according to art. 5th, VIII of the Civil Framework of the Internet[16].

This difference in obligations between the two categories of agents, providers of connection and application, aims to guarantee the achievement of other principles: privacy and protection of the privacy of citizens Internet users. After all, in order for the user of an application to be identified, one of the possible techniques to be used is to perform the cross-referencing of the records data of both providers.

Let us suppose a case in which John uses an email created with false registration information for illegal sale of passages areas. If a police authority seeks to identify who is using this email, it requests from the e-mail company the application records that inform which IP is being used to access the application. With this IP, the investigative authority contacts the connection provider that provided that IP to one of its consumers to connect to the internet. Thus, in a scenario in which each user is assigned a single IP for Internet connection, the technique explained has no difficulty identifying a person.

With the use of NAT systems, however, the IP stored in an application registry can lead to a list with several users of the connection provider, who used that IP in a shared way. Thus, there are cases appreciated by the Brazilian Judicial Branch in which the party seeking to identify a user (usually the Public Prosecutor) has requested, besides the records explained in the Law, the number of "logical gate" associated to the shared IP. As the technical term "logical gateway" is not mentioned in the legal text of the Brazil's Internet Bill of Rights, it is judicially discussed whether this law allows for the extensive or broad interpretation that connection and / or application providers must also store data concerning the logic gates .

11 Art. 7. Internet access is essential for the exercise of citizenship rights and duties, and users have the right to: VII - non-disclosure of their personal data to third parties, including connection logs and Internet application access logs, except with their free, express, and informed consent or in the cases provided for by lawi;

12 Art. 5. For the purposes of this Law, the following terms have the meaning ascribed to them below: [...]: IV - autonomous system administrator: a person or legal entity that administers specific blocks of IP addresses and the corresponding autonomous routing system, and that is duly registered with the national authority responsible for registration and distribution of IP addresses geographically allocated to the country.

13 Art. 13. In providing Internet connection services, autonomous system administrators must keep connection logs for a period of one year, under strict confidentiality and in a controlled and secure environment, as provided for by regulation.

14 Art. 5. For the purposes of this Law, the following terms have the meaning ascribed to them below: [...] VII - Internet applications: the set of functionalities that can be accessed by a terminal connected to the Internet.

15 Art. 15. Internet applications providers that are legal entities providing applications in an organized, professional manner, for profit, must keep access logs to Internet applications for a period of six months, under strict confidentiality and in a controlled and secure environment, in the manner provided for by regulation.

16 Art. 5.For the purposes of this Law, the following terms have the meaning ascribed to them below: VIII - Internet application access log: a record of information regarding the date and time when a given Internet application was accessed from a certain IP address.

4. NAT and gateway systems in the European Union and Australia

Besides Brazil, other countries have also faced similar problems with identifying Internet users who connect through IP sharing. In order to provide comparative analysis bias in terms of regulatory and jurisdictional profiles, the work investigates how the issue of IP sharing and gateways is similarly discussed in the European Union and Australia (representatives of legal systems in which IPv6 is widely deployed).

The cases that will be demonstrated aim, therefore, to provide a greater contextualization to the debate, extrapolating the purely domestic visions on IP sharing and identification of users in the Brazilian environment. The study, however, states that the cases were selected because of the greater ease of access to information, and do not represent, at this stage of exploratory analysis, the defense of a certain regulatory model for Brazil.

The legal Framework of European Union

The European Union implemented Directive 2006/24 / EC[17], on mandatory data retention, which provided only general guidelines, which member states should continue to implement in their national legislations. In art. 5, the Directive established which categories of data Member States should ensure conservation, defining them as the "data needed to find and identify the source of a communication" and "to identify the telecommunications equipment of users, or what is considered to be your equipment. " At no time does the standard use the term "logical port" or gate. However, a more in-depth analysis of each country is necessary to verify how each national regulation deals with the subject, and whether there is an express reference to doorkeeping.

In 2014, the Court of Justice of the European Union (CJUE), in joint cases Digital Rights Ireland Ltd and Kärntner Landesregierung[18], considered Directive 2006/24 to be invalid because it contradicts articles 7 (right to privacy) and 8 (right to privacy). protection of personal data) of the Charter of Fundamental Rights of the European Union[19]. In 2016, still in a context of vacatio legis (in the sense of regulation applied to all EU members) left by the invalidation of the Directive, the Court of Justice ruled on two joint cases in which it established what general protections the Member States should apply to be in accordance with the Electronic Privacy Directive (2002/58 / EC) and the EU Charter of Fundamental Rights.

In the cases Tele2 Sverige and Home Secretary v. Watson,[20] the CJUE ruled that Member States can not impose a general obligation of retention of data for electronic telecommunication services (electronic telecommunication services)[21], in relation to the traffic of data and location of the users. The decision, however, did not ban the possibil-

17 EU - *Directive 2006/24/EC* of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Available at: <http://bit.ly/2fPZOWg>. Access: 04/10/2017

18 CJEU. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources Ireland and others and Kärntner Landesregierung.* Joined cases C-293/12 and C-594/12, Grand Chamber, 8 de abril de 2014. Available at: <https://goo.gl/fjqymW>. Acesso em: 04/10/2017.

19 CJEU. The Court of Justice of the European Union. *Press Release Nº 54 /14.* Luxemburgo, 8 de Abril de 2014. Available at: <http://bit.ly/2tBS4IV>. Access: 04/10/2017.

20 CJUE. *Tele2 Sverige AB contra Post- och telestyrelsen e Secretary of State for the Home Department contra Tom Watson.* C-203/15.2016. Available at: <http://bit.ly/2yxxiNR>. Access: 18/10/2017

21 European Union Agency for Fundamental Rights (FRA). *Data retention across the EU*. Available at: <http://bit.ly/2zhJIZu>. Access: 18/10/2017.

ity of retention of data, since it is used for specific purposes (eg in the case of a specific suspect in a specific criminal action). The court also contends that counter-weight criteria are required for storing and accessing stored data. And it was also stated that it is necessary to have limitations to the storage of certain categories of data, looking for only those strictly necessary to a certain case; it has been pointed out that there is a need to clearly limit which persons have access to the registers; and to limit retention to a proportional period of time.[22]

Despite the trials of the CJUE, States do not have a strict legal obligation to implement the recommendations, with only four member states making changes to their legislation after their trials.[23]

It is also important to mention the judgment of the Breyer case[24], which was addressed by the CJUE in 2016, which sought to answer whether IP addresses are personal data, and whether their storage would be permitted only for the cases provided for in the former Data Retention Directive, or whether they could also be stored for the sake of a legitimate interest (legitimate interest). The CJUE understood that IP addresses are classified as personal data, provided that it is possible to identify the individual associated with their use; even if the data required for identification are in the possession of a third party. E has established that online media service providers can store their users' personal data, such as IP address, as long as they are used for a specific legitimate purpose.[25]

The General Data Protection Regulation (2016/679), which will be applied from 2018, does not specifically address the issue of mandatory retention of electronic data[26]. So the regulation in the European Union still lacks a general standardization, with each country having specific laws on the subject. The European Union Agency for Fundamental Rights evaluated in 2017 that:

> All in all, Member States' progress on the issue since the CJEU's invalidation of the Data Retention Directive remains limited. This may partly be due to the absence of harmonised rules at EU level. Eurojust, the EU agency for judicial cooperation in criminal matters, has stated that, while data retention schemes are considered necessary tools in the fight against serious crime, there is a need to create an EU regime on data retention that complies with the safeguards laid down by the CJEU.133 In any event, regardless of whether at European or national level: as long as data retention measures continue to be deployed, adequate protection measures must soon be implemented to prevent fundamental rights violations[27]

22 European Union Agency for Fundamental Rights (FRA). *Fundamental Rights Report 2017*. 2017. p.162-165. Available at: <http://bit.ly/2yvAxoY>. Access: 18/10/2017.

23 Bélgica, Dinamarca, Luxemburgo e Hungria buscaram reformular suas legislações após as decisões. *Ibid*, p. 164.

24 CJUE. *Patrick Breyer v. Bundesrepublik Deutschland*. Case C-582/14. 19 Outubro de 2016. Available at: <http://bit.ly/2gsdqaf>. Access: 18/10/2017.

25 European Union Agency for Fundamental Rights (FRA). Op. cit. p. 163

26 For example, the term "retention" is mentioned only twice throughout the text of the law.

27 Ibid, p. 164.

The Europol[28], the European Union's international law enforcement agency, is one of the European state agents who warns about the problem of identifying online users using IP-sharing through Carrier-Grade NAT (CGN). In 2016, the institution published the report The Internet Organized Crime Threat Assessment (IOCTA), which recognized with one of the main problems of Internet governance that year the use of CGNs by connection providers.[29] The report assesses that the use of CGN has led European police officers to struggle to associate an investigated online user with a single IP address. Trying to measure the extent of the problem, Europol cites a questionnaire by the European Cybercrime Center alleging that 90% of cybercrime police investigators, found in the research, claim to regularly encounter problems of identification of users due to CGN technologies.[30]

The report also points out that waiting for the IPv6 transition would be impracticable because it is estimated that the process will still take several years due to the lack of commercial incentives for implementation of the new protocol and the need for numerous investments in the IPv4 structure. Thus, it is recommended that police forces investigating CGN request, through legal channels: 1) the IP addresses of Origin and Destination; 2) the source logic port; and 3) the exact time of the connection (including seconds).[31]

The IOCTA uses as one of its specialized sources the recommendations of the Technical Memorandum Request for Comments 6302 - Logging Recommendations for Internet-Facing Servers, produced by the Internet Engineering Task Force - designated in 2011. This memorandum suggests that:

> *It is RECOMMENDED as best current practice that Internet-facing servers logging incoming IP addresses from inbound IP traffic also log: - The source port number. - A timestamp, RECOMMENDED in UTC, accurate to the second, from a traceable time source (e.g., NTP [RFC5905]). - The transport protocol (usually TCP or UDP) and destination port number, when the server application is defined to use multiple transports or multiple ports.*[32]

Finally, the IOCTA concludes that:

> *Regulatory/legislative changes are required to ensure that content service providers systematically retain the necessary additional data (source port) law enforcement requires to identify end users. Alternatively, practical solutions can be developed through collaboration between the electronic service providers and law enforcement. Some electronic providers Europe do store the relevant information (source port). A European- wide portal could maintain an updated list of those providers and a list a contact points to address in case an investigation is stalled by CGN*.[33]

28 The European Police Office (Europol) is an EU agency with no executive powers which seeks to promote coordination between the civil police of the 28 EU members. Its focus is on combating international crimes such as cybercrime, terrorism, money laundering, among others. EUROPOL. "About Europol". Available at:<http://bit.ly/2jWsUV8>. Access: 29/09/2017.

29 EUROPOL. "IOCTA 2016 - Internet Organised Crime Threat Assessment". Available at: <http://bit.ly/2fCum7o>. p. 57 e 58. Access: 25/09/2017.

30 *Ibidem*.

31 *Ibidem*.

32 *Ibidem*.

33 *Idem*, p. 58.

In January 2017 Europol launched a Working Group entitled "European Network of Law Enforcement Specialists in CGN" whose main objective is to study practical solutions to the issue of the use of shared IPs and identification of users. In public note were established as Group objectives:

> *On 31st January 2017 a European Network of law enforcement specialists in CGN will be established, the secretariat of which will be established/provided by? at Europol. The aim of this network is to: document cases of non-attribution linked to CGN in EU; document existing best practices to overcome CGN-related attribution problems currently in place in some Member States; raise awareness of European policy-makers about the problem of attribution linked to CGN technologies; represent the voice of law enforcement developing a common narrative and advocating for a voluntary scheme at EU level to improve traceability by engaging in a coordinated fashion with ISPs and application providers*.[34]

In the same note, the agency maintained the IOCTA 2016's diagnosis that the use of CGN has made it difficult to identify cyber criminals, warning that this issue could lead research forces to resort to more invasive means of privacy research. In addition, the note notes that the use of CGN by connection providers in the world is still high, especially by the mobile operators, supporting the hypothesis of Europol that some years will be necessary for the full transition to IPv6:

> *According to a recent a survey carried out among 70 traditional ISPs (cable, fiber and ADSL) worldwide, 38% of these traditional ISPs have CGN in place and 12% are planning to deploy it[1]. The situation is even worse for GSM [Global System for Mobiles] providers: according to the same study, 95% of mobile ISPs (i.e. IP addresses provided by GSM providers) use CGN technologies. [...] This means that CGN is here to stay and that the old policy response (i.e. wait for the transition to IPv6) is not the right approach from the perspective of the victims. The use of CGN will continue to grow in spite of the transition to IPv6, further impeding the law enforcement ability to perform a trace back to an individual end-user of an IP address*..[35]

In the search for solutions to the problem of **identifying online users**, Europol says that there is a need for greater debate and cooperation between the actors involved (ISPs, application providers, data storage providers, and police forces). In an absence scenario of harmonized data retention rules among European countries, the institution affirms the urgent need to seek:

> *"[...] practical solutions can be sought through collaboration between the electronic/Internet service providers and law enforcement using already established channels for cooperation such as the EU Internet Forum. The latter could provide an excellent platform for discussion with the most important ISPs/application providers the need to implement the traceability of source port numbers and to provide these numbers on a voluntary basis when requested (directly or by legal process) by law enforcement and judiciary authorities in order to facilitate the attribution of crime.*[36]

34 EUROPOL/EC3 - 5127/17. *"Carrier-Grade Network Address Translation (CGN) And the Going Dark Problem"*. 16 de Janeiro de 2017. p. 7. Available at: <http://bit.ly/2hw37OX> e <http://bit.ly/2yDviCI>. Acesso em: 29/09/2017.

35 *Ibid*, p. 5.

36 *Ibid,* p.6.

Australia

In 2015, the Australian Parliament passed a data retention law for the country, which was amended to the "Telecommunications (Interception and Access) Act" of 1979.[37] The law requires that certain telecommunication service data[38] and the provision of Internet access are stored for a minimum period of 2 years (counted from the date of creation of the information), and may be exceeded for commercial purposes.[39] By comparison, EU Directive 2006/24 / EC established 2 years as the maximum time for storing telecommunication data.

First, the **concept of a application provider** according to Australian law needs to be clarified. It is a gender, which is divided into two species: (a) carriage service provider and (b) content service provider.munication.[40] A *carriage service provider* provides telecommunications services by means of electromagnetic energy[41]. An application provider provides online content to the public (streaming videos, online games, etc.), which travels through the structure provided by carriage service provides.[42] The Data retention law applies only to carriers, carriage service providers and internet service providers (ISPs),[43] that is, to the companies of telecommunications and providers of connection to the Internet.

The Telecommunications Act determines six types of information that must be stored relating to a communication session[44], which is associated with a specific service providers offer[45]. It should be emphasized that these records need to be encrypted and stored securely and may be requested by a limited number of investigating authorities. Examples of services are the provision of Internet access, Voice Over Internet Protocol (VoIP) services, SMS, among others, each having certain specificities in the data retention obligation. The six types of information subject to the request / requisition are:

> 1.The data to be retained is set out in six categories: 1. the subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service; 2. the source of a communication; 3. the destination of a communication; 4. the date, time and duration of a communication, or of its connection to a relevant service; 5. the type of a communication or of a relevant service used in connection with a communication, and; 6. the location of equipment, or a line, used in connection with a communication.[46]

37 AUSTRALIA, "Telecommunications (Interception and Access) Act" Nº 114, 1979, Compilation Nº. 96. Available at: <https://www.legislation.gov.au/Details/C2017C00308>. Access: 05/10/2017.

38 "*What is telecommunications data? - Telecommunications data is information or documents about communications, but not the content or substance of those communications*." AUSTRALIAN GOVERNMENT- Attorney-General's Department. *Data retention - Frequently Asked Questions for Industry*. Julho de 2015. p. 11 . Available at: <http://bit.ly/2gOWCJG>. Access: 06/10/2017.

39 AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Guidelines for Service Providers* . Julho de 2015. P.4. Available at: <http://bit.ly/2gOWCJG>. Access: 06/10/2017

40 Section 86. Telecommunications Act 1979.

41 Sections 7 e 87. Telecommunications Act 1979.

42 Sections 15 e 97. *Telecommunications Act 1979.*

43 *"Only carriers, carriage service provider and internet service providers (C/CSP/ISPs) have obligations under the data retention regime."* AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Data retention - Frequently Asked Questions for Industry*. Julho de 2015. p. 11 . Available at: <http://bit.ly/2gOWCJG>. Access: 06/10/2017.

44 *"The meaning of communication or session depends on each particular relevant service. For instance, for VoIP services, obligations are applied to each call scenario. For SMS, each SMS is a separate communication. For email, the session is the customer's log-in to the email service and the communications are each email. For internet access services, the session will typically be the period for which a private IP address is allocated." Ibid*, p.8.

45 AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Guidelines for Service Providers*. Julho de 2015. p.4.

46 *Ibid,* p. 4.

There are situations where a service provider is not required to store all six categories. For example, ISPs can not store destination data for a communication, nor data relative to the user's browsing history[47], in the context of provision of Internet connection services. A similar rule is established in art. 14[48] of the Internet Cvil Framework, which prohibits connection providers from storing access data to Internet applications. In the Brazilian case, the fence seeks to limit the amount of data that a single agent can store, aiming for greater protection of the privacy and personal data of the user. In the limit, it is a rule that aims at a balance between economic power held by connection providers and user rights related to Internet use.

For comparison purposes, in the Civil Registry of the Internet there are two categories of agents that have the obligation of record keeping: connection providers, arts. 5, IV, V, VI and 13; and application providers, arts. 5, VII, and 15. The concept of application provider is more similar to the Brazilian concept of application provider. OTT services (over-the-top-content) in Brazilian law, for example, would also be classified as application providers. However, in Australian regulation, some types of OTT services[49], such as the VoIP, chat and online messaging must have metadata stored under the Telecommunications Act if provided by telecommunications companies and Internet connection providers.[50]

For the s**ource of a communication**, ISPs are required to store the IP address and **logical port** allocated to the subscriber or to the Internet-connected device at the time of communication.[51]It is important to note that the Telecommunications Act does not cite the technical term "port number", which is an executive rather than legislative regulation.

Another important point is that the Australian Attorney-General's Department makes express reference to agents using NAT systems and their obligation to store the logical gates. This obligation derives from the interpretation of the legal term "identifier allocated to an account or service, pursuant to Paragraph 187AA of the Telecommunications (Interception and Access) Act:[52]

> *For the avoidance of doubt, the requirement to keep NAT records will (at minimum) apply to the [Internal IP address; Internal Port; External IP address; External Port] elements of a NAT table. Whatever elements are kept as part of a provider's NAT records, it must be possible to uniquely identify and associate the*

47 *Ibid*, p. 12.

48 Art. 14. It is forbidden to keep Internet application access logs in providing Internet connection services.

49 The Body of European Regulators for Electronic Communications defines OTT as a content, service or application that is provided to the end user through the public internet. The availability of this service, content or application occurs without the involvement of those who provide the connection to the internet. BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATION *Report on OTT services*. 2016. p. 14. Available at:<http://bit.ly/2yRFc3s>. Acessado em 08/10/2017.

50 "*Will off-shore over-the-top (OTT) providers that don't own or operate infrastructure in Australia be captured by the data retention obligations? The data retention obligations only apply where the service meets all three of the following criteria: 1. the service is for carrying or enabling communications to be carried by electromagnetic energy; 2. the service is operated by a C/CSP or an Internet Service Provider (ISP); and 3. the provider owns or operates infrastructure in Australia that enables provision of any relevant service. Criterion one captures a broad range of services including OTT services like VoIP and chat or other online/application messaging services. Criterion two acts as a limitation on the first criterion. That is, a person might host a website or an FTP server that facilitates communications via electromagnetic energy. But if that person does not have a carrier licence and does not meet the CSP or ISP definition, that person does not attract data retention obligations. Criterion three provides a further limitation by excluding providers that do not have any communications infrastructure in Australia. Infrastructure means any line or equipment used to facilitate communications across a telecommunications network. This includes servers that host websites or services furnished by OTT providers, as well as line links and network units.*". *Idem*, p. 18

51 "*What are the data retention obligations relating to a provider who only offers an internet access service (i.e. no additional OTT) services offered)? [...] all IP addresses and, where applicable, port numbers allocated to the subscriber during that session, including the associated dates and times*". AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Data retention - Frequently Asked Questions for Industry*. Julho de 2015. p.21 . Available at: <http://bit.ly/2gOWCJG>. Access: 06/10/2017.

52 *Idem*, p. 13

> *Internal IP address/Internal Port to an External IP address/External Port and vice versa. If a carrier's NAT tables also include [Destination IP address; Destination Port] elements (for example, under a Symmetrical NAT model), data retention obligations will not apply to those elements. Whether a carrier wishes to retain those additional elements is a decision for the carrier.*[53]

Strangely, the Telecommunication Act is silent on data retention obligations by companies offering OTT services other than ISPs.[54] Therefore, there is no provision in the Australian law on the storage of logical portfolios for these agents, which could result in a kind of asymmetry in the allocation of obligations for economic agents operating in the access and application provision segments:

> The complex way that 'over the top' services are excluded creates an unusual distinction in the Act where services that are provided by Australian ISPs themselves will actually be included within the scope of the obligation. So, for example, if a subscriber accesses email through a third party provider, like Google, or makes a call through a VoIP service like Skype, these are 'over the top' services, and the provider is under no obligation to retain any information about their use. But, where email or VoIP services are provided by the ISP itself, it is required to store any information about the communications its users make – including addresses to which emails are sent or calls placed.[55]

5. Methodology for data collection and analysis of Brazilian courts on access to logical gates

Scan method

The data on **lawsuits involving requests for access to logic gates** analyzed in this study were collected on the websites of all Brazilian State Courts of Justice, in the Federal Courts of Justice, as well as in the Superior Court of Justice (STJ). The choice of these instances is justified by the availability of the decisions, as well as of their contents, through online jurisprudential research mechanisms, unlike what occurs, for example, in the first instance. The searches were performed using the expressions "logic gate" and "logic gates". The study, therefore, did not have access to processes not included in the databases of jurisprudence in electronic format, or to those that may exist in the form of physical records.

Shared tables (in the Google Drive tool) were then built so that the researchers involved could record the information found in online searches and observations. This allowed the data to be selected, identified, analyzed together (by all researchers) and the information could be viewed in aggregate form at a later stage of research. In the first database, the decisions that brought the cases to the lower courts, or to the STJ (Table 01), are gathered together. In the second, there are references to Requests for Clarification, when interposed, against the decisions analyzed (Table 02).

53 *Ibidem*.

54 HURST, Daniel. *Telcos question data retention plans that exempt Facebook, Gmail and Skype*. The Guardian. 2015. Available at: <http://bit.ly/2xqggnn>. Access: 08/10/2017.

55 SUZOR, Nicolas; PAPPALARDO, Kylie; McINTOSH, Natalie. *The passage of Australia's data retention regime: national security, human rights, and media scrutiny*. Internet Policy Review- Journal on Internet Regulation.Volume 6, Edição 1. Março de 2017. Available at: <http://bit.ly/2y4aUeB>. Access: 08/10/2017.

Time frame

This research has as time frame the validity of Law n. 12,965, dated April 23, 2014, the Civil Internet Framework in Brazil[56]. This is because, in a previous scenario, there was no specific legislation in Brazil[57] that would oblige agents to keep records of access to the internet application, or registration data of users, but only sparse decisions and without any uniformity required by special law. Decisions were taken as from 2014 and, therefore, already included in the context of the validity of the Civil Framework. The final term of the survey was August 31, 2017. The choice of this criterion for the time frame, despite disregarding a group of decisions prior to the entry into force of the Internet Civil Registry, imposing obligations to guard access records, allows to establish an analytical reference for the continuity of the monitoring of future decisions on this theme.

Variables - Data base 01

The following variables were registered (measured) in the information gathering effort:

1. Lawsuit number

The cases collected were identified through the numbers assigned by the courts themselves. This field was used only for the researchers involved to refer to the other fields.

2. State (Federal entity)

The objective of this variable is to investigate the forum for processing the demands on logic gates in Brazil. With the use of the keywords chosen for this research, the results in federal courts did not produce results that were actually relevant to the object initially proposed by the study. Thus, in practice, this field corresponds to the results obtained in the courts of appeal of each state of the Brazilian Federation, in addition to the Brazilian Superior Court of Justice (Superior Tribunal de Justiça - STJ), whose field was thus filled, since it is a higher court of appeals not directly linked to the states.

3. Year

The research was carried out with reference to the time frame of decisions promulgated starting in 2014, in which Brazil's Internet Bill of Rights was already in force. Therefore, decisions were found in 2014, 2015, 2016 and 2017.

4. Appellant

We systematized the parties involved only in courts of appeal and that specifically integrated each of the decisions collected. By "appellant", it is understood not the plaintiff on the lawsuit, but the one that brought the appeal. In Table 01, the "appellants" are the ones bringing interlocutory appeals, regular appeals or other appeals, depending on the request for review, and, in Table 02, are the ones bringing requests for clarification.

56 The efficacy of Law n.12,965 was given 60 days after its publication, on June 23, 2014.

57 Precedents prior to Brazil's Internet Bill of Rights justified the obligation to provide access data through consumer legislation. In this sense, the providers, because they were profitable using the Internet, assumed the obligation to provide, for example, IPs and registration data. In this sense, see STJ, *Special Appeal nº 1403749/GO,* Justice Nancy Andrighi, Third Chamber. Trial date: 22/10/2013. However, the period relevant to the research and such obligations are discussed in light of Law n. 12,965/2014.

The parts have been categorized in order to allow graphical processing of the data. The following categories were used:

- **AP**: employed when part is an **application provider**;
- **CP**: employed when the party is a **connection provider**;
- **LE**: refers to the **legal entity that is not an application or connection provider**;
- **NP**: used in cases where the party is a **natural person**;
- **UN**: refers to cases where the **parties have not been identified** because of the anonymity of the data.

5. Respondent in appeal

Considering the same system of identification and categorization of the appellant, the respondent variable sought to consider who were, in Table 01, the respondents in interlocutory appeals and regular appeals, and, in Table 02, the appealed parties in requests for clarification.

6. Fine

The objective of the "fine" variable was to identify how many appeals had reached the courts and dealt with dealt with fines, both of an interlocutory nature, and a final decision on merit. The field was filled with the "yes", "no" and "unidentified" options when the analysis was inconclusive.

7. Amount of the fine established

In cases where the fine arbitration was identified, the researchers also sought to discriminate the defined value.

8. Provisory preliminary protection

We tried to identify which decisions represented the matter regarding provisory preliminary protection. This is because the obligation to provide a logic gate can be defined in an interlocutory decision, by a judge, and subject to appeal from the parties, taking the case to the analysis of a court of judges in the appellate level.

9. Legal devices

The field on legal provisions gathered information on the instruments referred or invoked in the decision. They were identified by the research team by means of acronyms. For example, "BIBR" refers to Brazil's Internet Bill of Rights, while "CR" to the Constitution of the Federative Republic of Brazil.

10. Strictly procedural argument

Secondly, the variable also allows one to gauge the extent to which certain interlocutory or meritorious decisions fail to make any contribution in terms of the formation

of materially consistent precedents over the interpretation of substantive rules of the Civil Code.

The objective of this variable was to verify how many of the decisions about the obligation, by the application providers, to supply the logical gate of origin for identification of a user materially discussed the controversy or were limited to adjective questions and procedural rules. Secondly, the variable also allows one to measure the extent to which certain interlocutory or final decisions fail to make any contribution in terms of the formation of materially consistent precedents over the interpretation of substantive rules of the Brazilian Civil Code.

11. Reference to Brazil's Internet Bill of Rights

Considering that Brazil's Internet Bill of Rights is the normative instrument in Brazil that deals with data storage by providers, it was necessary to investigate how many decisions about logic gate considered it in its rationale.

12. Article of Brazil's Internet Bill of Rights referred or invoked

In cases where Brazil's Internet Bill of Rights was mentioned, we sought to distinguish the devices in order to analyze their relevance to the subject under discussion.

13. Obligation to supply logic gates

The "obligation to provide logic gate" corresponds to the operative part of the decision, as the outcome of the appeal. This obligation refers specifically to the **application providers**, since they are at the center of the disputes over the responsibility for guarding and delivering logic gates. The field was filled with "yes", "no" and "UN", in cases where the definition of the obligation was not clear.

14. Use of jurisprudence

Due to the growing importance of precedents in Brazilian law, especially since the entry into force of the New Code of Civil Procedure, our research considers the frequency in which decisions quote previous solutions on the controversial matter. The fields in which they are deemed to be concerned with the obligation of the application providers to provide logic gate of origin have been completed as "yes".

15. Use of technical opinions

The technical aspects are relevant to the decision on the guarding and delivery of logic gates. For this reason, it was verified whether the decisions quoted technical opinions or reports in its reasonings. As a technical opinion, the researchers considered both reports from state agencies and civil society organizations, as well as the use of specialized authors and legal opinions on the subject in the decision.

16. Teleological interpretation of Brazil's Internet Bill of Rights

In cases where Brazil's Internet Bill of Rights was quoted, we verified what kind of interpretation was accomplished by the court regarding the law. The teleological interpretation, for the purposes of this research, was understood as the one that bases the decision on the purpose of the law, discussing what it would be and how it should

be ensured. Thus, when the decision establishes the obligation, for example, in order for Brazil's Internet Bill of Rights to identify users accused of illegal acts, the field was completed as "yes". When the interpretation was distinct from the purpose, the result was "no" and when, despite the law being quoted, its interpretation was not clear, the field was completed with "UN - unidentifiable".

17. Literal interpretation of Brazil's Internet Bill of Rights

Another possible interpretation of Brazil's Internet Bill of Rights as a research variable, according to the methodology adopted by our team, was the literal interpretation. When it is identified that the reasoning of the decision from the bill represents its literal transcription and is limited to what the cited articles define, the field "literal interpretation" was filled in as "yes". When there were several interpretations, "no", and in cases where it was not clear, "UN".

Variables - Data base 02

Correspondants to data base 01

Table 2 includes the group of Requests for Clarification and has the following variables also presented in table 1, under the same justification:

- Number of the case - and also of the appealed decision, for identification purposes only;
- State;
- Year;
- Appellant;
- Respondent.

Strictly procedural argument

In this field, it is sought to verify whether the requests for clarification serve as a means of material review of the decisions, or are restricted to procedural arguments regarding the function of the appeal filed, or the identification of the lingering nature of one of the parties.

Review of the contested decision

The objective is to investigate the effectiveness of the appeal for the reform of the appealed decisions. The field was again filled with "yes" and "no" in cases where the legislative device was clear, or with "unidentified" when the contested decision was not found by searches, and therefore the variable about the review remained unfinished for the researchers.

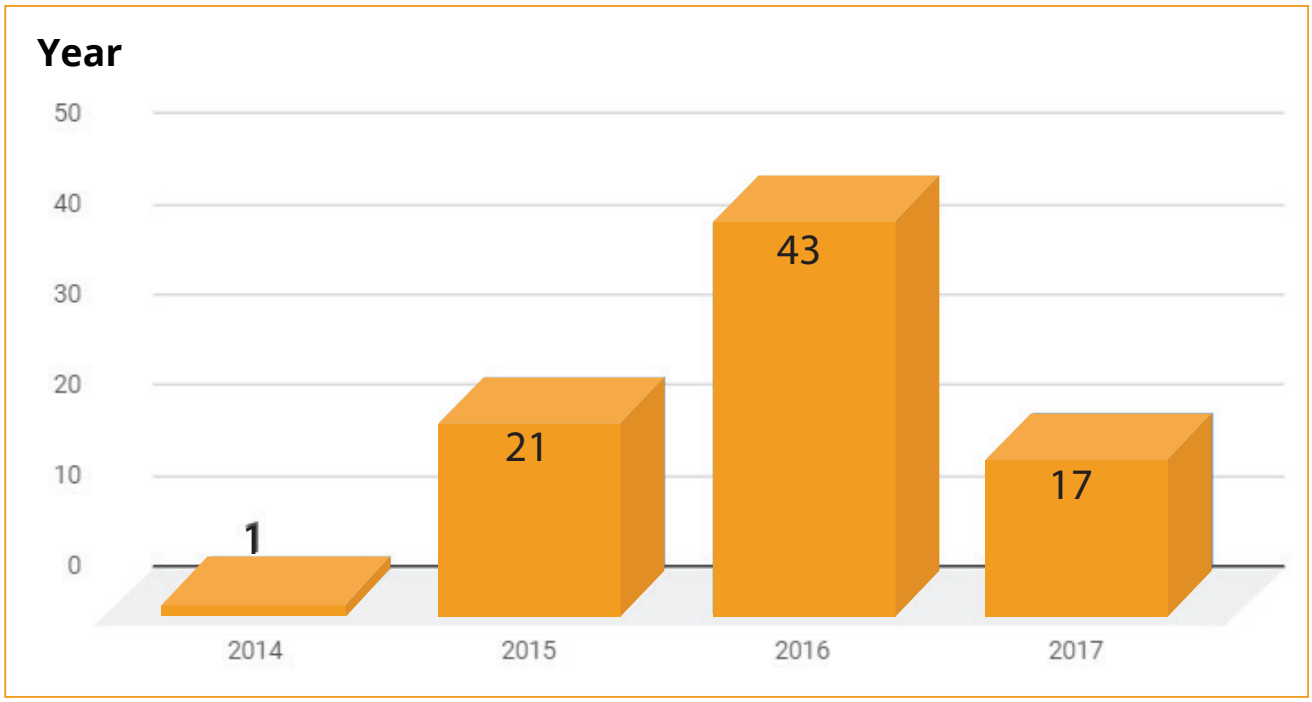
6. Analysis of results regarding profiling of judicial decisions

Profile of the decisions

Considering the option to investigate the cases from the court of appeals, at first, 80 (eighty) Interlocutory Appeals, Appeals and Suspension of Execution were analyzed, all identified and selected from the databases of state courts of justice. In the Brazilian Superior Court of Justice, only two Interlocutory Appeals in Special Appeals were found,[58] in monocratic decisions, which did not discuss the matter of logic gates and, therefore, did not serve to guide the standardization of the controversy and to form jurisprudential understandings on the subject. In both, in fact, procedural arguments were used to prevent the Brazilian STJ from considering the substance.

In the case of Interlocutory Appeal in Special Appeal n. 897,089-SP, the reason given was the supervenience of a sentence appeal, which suspends other appeals filed before it. On the other hand, the justification for not being discussed in Special Appeal No. 1011826-SP is in the interpretation that it would require an analysis of facts or of evidence, purposes that this kind of appeal does not lend itself for.[59]

Considering the appeals presented in the state courts of appeal, in which it is effectively analyzed the obligation of the application provider to provide a logical gate, between 2014 and August 2017 (period of analyses), one can notice a greater concentration in 2016:

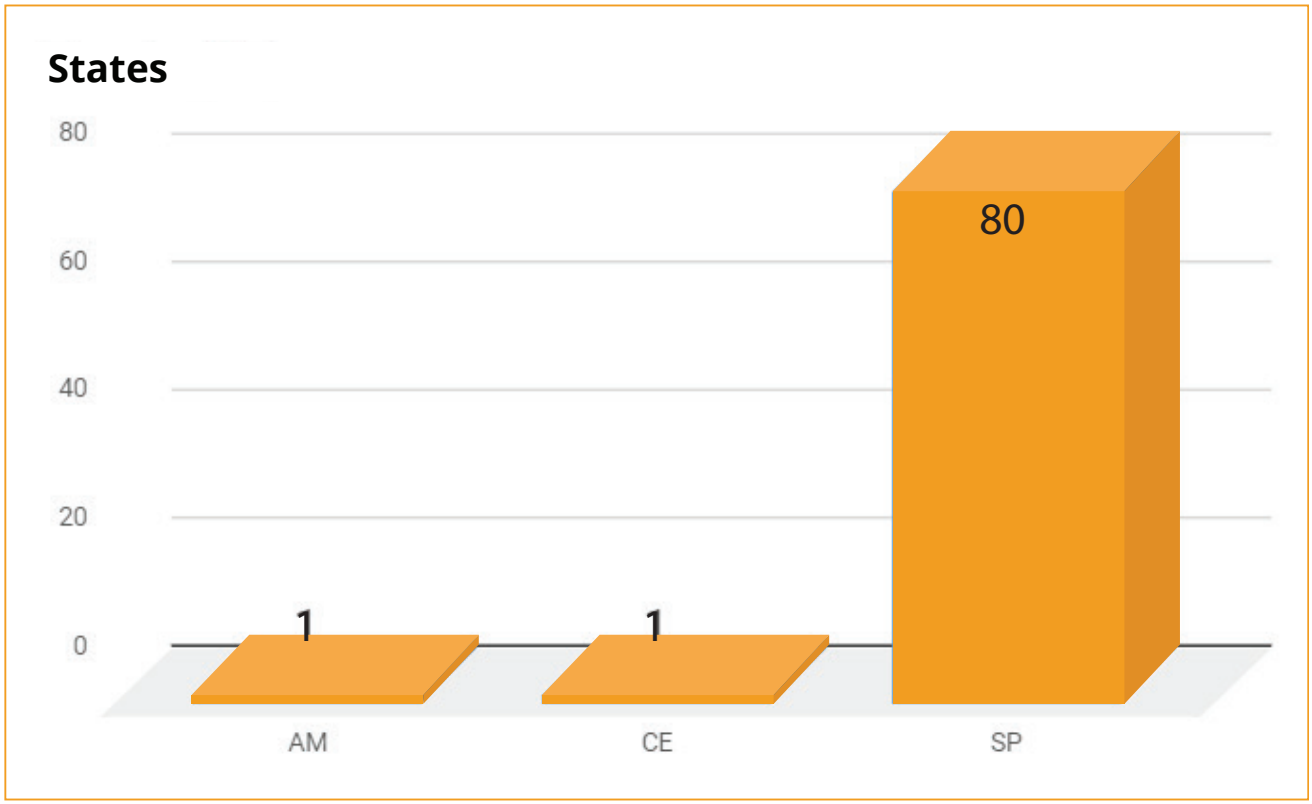


58 Brazilian Superior Court of Justice - STJ, *Interlocutory Appeal in Special Appeal n. 897.089 - SP (2016/0087515-0)*, Monocratic Decision, Judge Moura Ribeiro, trial date: 16/09/2016 e STJ, *AREsp nº 1011826 - SP (2016/0293419-7)*, Monocratic Decision, Justice Nancy Andrighi, trial date: 28/06/2017.

59 Due to the strictly procedural grounds, without material analysis of the object of this study, the cases found in the Brazilian Superior Court of Justice (STJ) were not included in Table 01, which served as a basis for the variables explained in the methodological notes.

A first observation would lead to the impression that the number of demands has increased.[60] However, it can be expected that this growth will not be maintained if the process of IPv6 implementation in the country is accelerated (considering that there is no use of NAT systems in an IPv6 scenario), leading to a decrease in the use of logic gates. Although still incipient, the use of IPv6 in Brazil is among the most expressive in the world, as shown by the data of the "Implementation of IPv6 in Brazil" item of this study. Despite this, the pace is slow and even though the use of logic gates is a transitory measure, the controversies will still reach courts as long as the transition has not been completed.

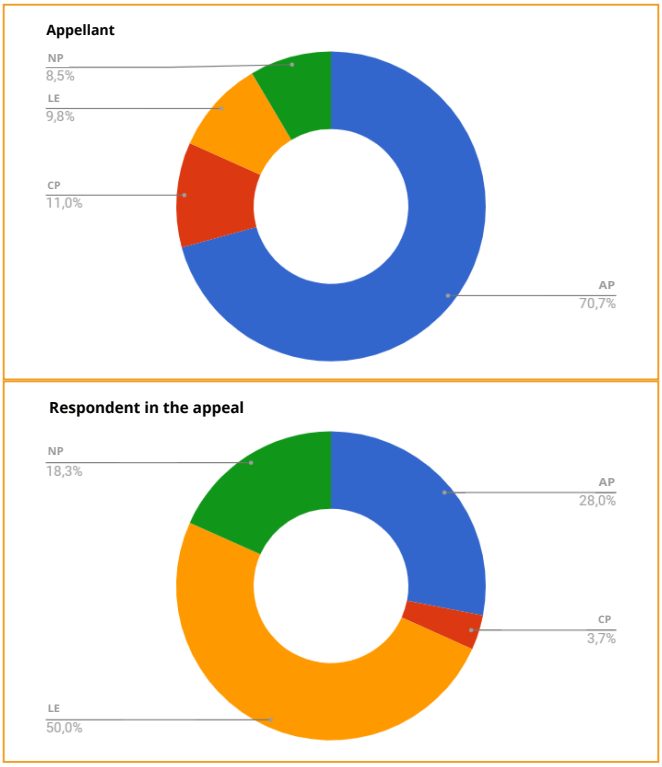
It was observed that the São Paulo Court of Appeals concentrates a high degree of litigation in claims on the obligation, by application providers, to provide logic gates.[61] The vast majority of the cases that reach appeal courts, in Brazil, is in the state of São Paulo (SP):



In relation to litigants, the parties are both natural persons and legal persons. Among these, connection providers and application providers were differentiated, in order to establish analysis parameters. After all, the matter of logic gates and the definition of one's obligation to provide them, or to both of them, directly affects them. Specifically, the controversy about application providers supplying or not logic gates can be pointed out as the reason why they are the majority of the parties, both appellant and respondent.

60 It is important to reinforce that the scan for the year 2017 ended on 08/31/2017, as presented in the session on the time frame of the research.

61 Some of the hypotheses for the concentration of demands involving the provision of logic gates in São Paulo's Court of Appeals would be the location of the offices of large application providers, such as Facebook and Google, which would facilitate possible execution or coercion procedures against them, and the concentration of law firms in the city specializing in these demands.



In addition to the application providers appearing as the majority of plaintiffs, they are also the majority of the respondents. The justification for this may be due to the fact that the decisions analyzed are not homogeneous. One party or another may file different appeals in order to reform, for example, interlocutory decisions contrary to their interests. Everything will depend, therefore, on the instruments of appeal made possible by Brazilian law.

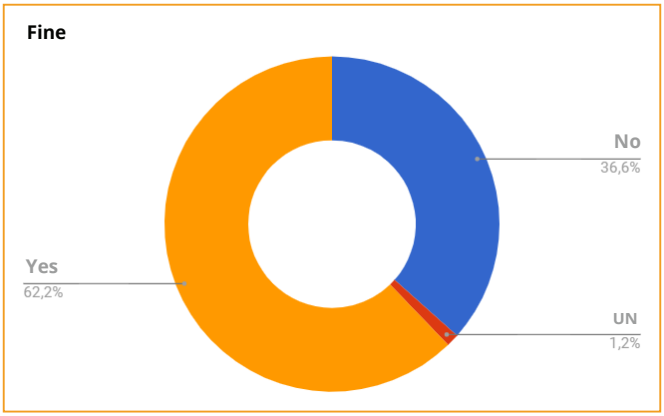
Most of the sampling of the decisions analyzed is comprised of judgements in appeals against interlocutory decisions. Of these, 82%[62] refer to interlocutory appeals filed to challenge courts' decisions that granted, or refused to grant, provisional preliminary protection for the delivery of information about logic gates. Provisional preliminary protection is a procedural instrument used to protect both the material right that is the subject of the lawsuit and the judicial procedure itself, due to the urgency or the damages that may be caused by the passage of time. It is sought to obtain the logic gate that allows to identify a user unequivocally before the end of the process, when it is possible that this measure is moot. It is important to emphasize that provisional preliminary protection occurs without all of the evidences being exhausted and exposed, or that the solution is definitive. Nevertheless, it obliges the parties to comply with the decision and, therefore, can be observed as the cause of most of the resources involving the provision of logic gates by the application providers.

Decisions that define an obligation to do something, as is the case of "delivering logic gate", have instruments to constrain the debtor to comply with them. One of them is known as *astreinte*. Determined by article 537 of the Brazilian Code of Civil Procedure (CPC),[63] it is a fine determined judicially, in general daily, that is due while the obligation is not complied with. Its fixation can occur both in the sentence, and in provisional preliminary decisions, as well as in the execution phase of the process. In the cases examined,

62 This represents 68 out of the 82 decisions analyzed.

63 Article 537. The fine is independent of the request of the plaintiff and may be applied at the first phase of the procedure, under provisional preliminary decision or sentencing, or at the stage of execution, provided that it is sufficient and compatible with the obligation and that a reasonable deadline is established for compliance with the precept.

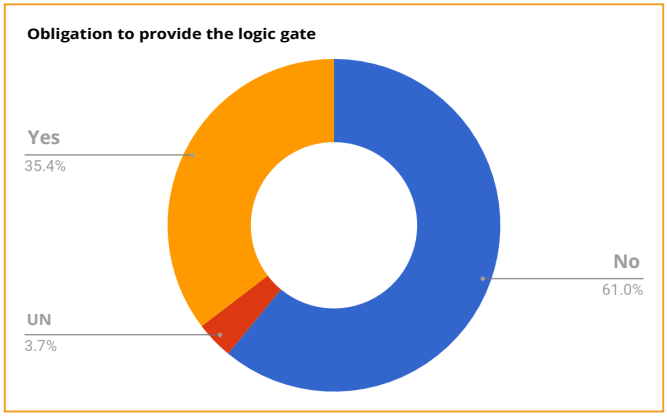
the fines were imposed in order to encourage application providers to supply the original logic gates, if they do not do so by the deadline set.[64] It is observed that the majority of the decisions dealt with fines fixed at a state level (not appeal courts):



In cases where fine arbitration has been identified, it is perceived that the amount established varies. There are daily fines of R $ 100.00[65] and others that reach R $ 10,000.00.[66] Some decisions impose a limit of days, or of an amount to be paid,[67] and others do not set a ceiling/cap.[68] Technically, there is no standard for establishing fines as penalties, therefore in defining them, the **judge** must consider the specificities of the cases, so that the measure is proportional and sufficient. Despite this, the great variation of values and conditions seems to be a symptom of the heterogeneity with which the subject of the obligation to provide logic gates, by the application provider, has been treated in the Brazilian justice system.

Decisions and reasonings

Most of the decisions analyzed, in appeal courts, do not give application providers the obligation to provide logic gates:



64 Interlocutory Appeal n. 2120450-79.2016.8.26.0000/TJSP, for example, regards a fine established in a provisory preliminary decision, in case the provider does not supply the logic gate in 5 days, in which case it will incur in a daily fine of R$ 500.00 until the maximum amount of R$ 50,000.00. TJSP. *Interlocutory Appeal n. 2120450-79.2016.8.26.0000/TJSP.* Rapporteur: Judje Costa Netto, Trial date: 13/12/2016, 9th Chamber of Private Law, published on: 19/12/2016.

65 TJSP. *Interlocutory Appeal n. 2108286-82.2016.8.26.0000*, Rapporteur: Judge Alcides Leopoldo e Silva Júnior, Trial date: 13/09/2016, 1st Chamber of Private Law, published on: 13/09/2016.

66 TJSP. *Interlocutory Appeal n. 2175598-75.2016.8.26.0000.* Rapporteur: Judge Beretta da Silveira, Trial date: 08/12/2016, 3rd Chamber of Private Law, published on: 08/12/2016.

67 Interlocutory Appeal n. 2185053-64.2016.8.26.0000/TJSP, for example, limits the fine to 90 days. However, Interlocutory Appeal n. 2108074-61.2016.8.26.0000/TJSP defines as a ceiling/cap R$ 10,000.00. TJSP. *Interlocutory Appeal n. 2185053-64.2016.8.26.0000.* Rapporteur: Judge J.L. Mônaco da Silva, Trial date: 16/11/2016, 5th Chamber of Private Law, published on: 21/11/2016.

68 C.f.: TJSP. *Interlocutory Appeal n. 2158001-30.2015.8.26.0000/TJSP.* Rapporteur: Judge Rui Cascaldi. Trial date: 03/11/2015, 1st Chamber of Private Law, published on: 04/11/2015.

Having verified the result of the decisions, the research sought to identify its reasonings. In order to do so, it considered as **variables** the presence of **references** to **Brazil's Internet Bill of Rights**, which is the law that establishes the obligation of data storage, by providers, precedents and technical opinions. In general, the matter involves aspects of the **ability of application providers** to store and deliver the logic gateway when requested in court. The numbers that relate the presence of these reasonings to the result about the obligation researched, however, are not enough to establish a pattern of decisions, since they very significantly.

Law n. 12.965/2014, Brazil's Internet Bill of Rights

Regarding the foundations of the decisions analyzed, the research identified that not all[69] are based on Brazil's Internet Bill of Rights. Although the Law does not deal specifically with logic gates, as already mentioned, it disciplines the use of the Internet in Brazil. It is possible to point out, as one of the reasons for that, the lack of knowledge of the law by the judiciary branch itself, because it has been shown that, over time and with the consolidation of Brazil's Internet Bill of Rights, its application has increased. Thus, while in 2014 and 2015 the number of decisions that did not mention the law was greater than those that cited, this behavior is reversed in 2016, and also in the period of 2017 analyzed. It is therefore perceived that the law has been more applied in cases involving logic gates.

The provisions of Brazil's Internet Bill of Rights do not vary significantly when they are included in the decisions.[70] In general, the following devices often appear: article 5, VIII, which defines, for the purposes of the law, "access records";[71] article 10, which deals with the protection of records;[72] and article 15, which defines record keeping relative to application providers.[73] More frequently, other sections of article 5, such as subsection VII,[74] in which Internet applications are defined, article 19, regarding the responsibility of the providers[75] and article 22, on the judicial requisition of the records.[76]

Some decisions, despite quoting Brazil's Internet Bill of Rights, do not focus on interpreting it. From the total of decisions analyzed,[77] the survey on teleological or literal

69 Of the 82 decisions analyzed, in 27 no reference to the Brazil's Internet Bill of Right is identified. It is criticized here that the principles, as well as the legal definitions and responsibilities defined by law, due to the context in which demand is developed, should at least be considered. For more information on the applicability of the law, cf. the section 2 above.

70 C.f. Database 01, attached.

71 Art. 5º For the purposes of this Law, the following terms have the meaning ascribed to them below: [...] VI - connection log: a record of information regarding the date and time that the Internet connection begins and ends, its duration, and the IP address used by the terminal to send and receive data packets;

72 Art. 10. Maintenance and disclosure of Internet connection logs and Internet application access logs contemplated in this Law, of personal data, and of the content of private communications must respect the privacy, private life, honor, and image of the parties directly or indirectly involved.

73 Art. 15. Internet applications providers that are legal entities providing applications in an organized, professional manner, for profit, must keep access logs to Internet applications for a period of six months, under strict confidentiality and in a controlled and secure environment, in the manner provided for by regulation.

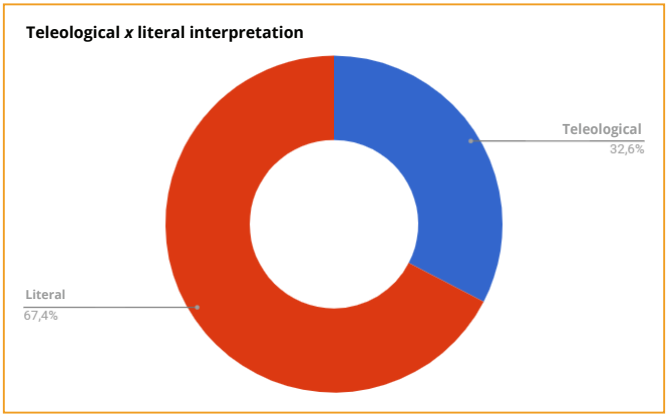
74 Art. 5. [...] VII - Internet applications: the set of functionalities that can be accessed by a terminal connected to the Internet;

75 Art. 19. In order to ensure freedom of expression and prevent censorship, Internet applications providers may only be held civilly liable for damages resulting from content generated by third parties if, after specific judicial order, the provider fails to take action to make the content identified as offensive unavailable on its service by the stipulated deadline, subject to the technical limitations of its service and any legal provisions to the contrary.

76 Art. 22. In order to obtain evidence for use in civil or criminal proceedings, the interested party may apply to the court, as an incident to a main proceeding or in a separate proceeding, for an order compelling the party responsible for keeping Internet connection logs or Internet applications access logs to produce them.

77 These two forms of interpretation were chosen due to the frequency in which they appear on decisions regarding logic gates. On one hand, teleological interpretation is connected to the idea of interpreting the norm under the legislator's purpose while drafting the bill, and seeks to extend the norm beyond its literal meaning. On the other hand, literal interpretation resorts to what is predicted in the text of the law, restrictively, based on legal security. This study does not aim to value the application of one perspective over another, but limits to identifying them.

interpretation of the law was carried out only in 46 decisions, in which it was possible to identify the hermeneutic effort of judges. In this group of decisions, it is observed that literal interpretation has prevailed:



In general, **literal interpretation** is based on the fact that the Brazil's Internet Bill of Rights does not deal with logical gates when defining which access records (article 5) application providers must keep or provide when demanded by a court order (article 15). According to this perspective, since there is no other legal statute to regulate the matter discussed, the absence of provisions on the Brazil's Internet Bill of Rights regarding logic gates frees application providers from their storage and delivery.[78] In a different way, the **teleological interpretation** chooses as purpose of the provisions on the guarding of access records in the Brazil's Internet Bill of Rights the identification of application users, when this is necessary judicially or administratively, or to the police or to public prosecutors (art. 15 and paragraphs). Although the law does not literally mention this obligation, the decisions that adopt a teleological interpretation consider that, in order to enable the identification of the user, logic gates can be included in **access records** referred to in article 5 of the law, whose custody is mandatory by the application providers.[79]

Jurisprudence

Jurisprudence is often used to justify both favorable decisions and those against the **obligation to provide logic gates**. The majority of the decisions counts on other previous judgments and that deal with the same subject. Because previous judgments are cited in both directions, it cannot be concluded that the existence of jurisprudence in the decisions database reveals a tendency of judgement, particularly due to the inconsistency of established guidelines.

Technical Opinions

Considering the nature of the controversy, which involves the infrastructure necessary for application providers to register and deliver - or not - the logic gate, our team sought to analyze whether the decisions of the Courts of Justice also considered technical

78 This perspective can be found, for example, in the following decisions: TJSP. *Interlocutory Appeal n. 2087441-29.2016.8.26.0000*. Rapporteur: Judge Moreira Viegas, Trial date: 23/11/2016, 5th Chamber of Private Law, published on: 24/11/2016; TJSP. *Interlocutory Appeal n. 2083730-16.2016.8.26.0000*. Rapporteur: Judge Vito Guglielmi, Trial date: 14/07/2016, 6th Chamber of Private Law, published on: 15/07/2016; and TJSP. *Interlocutory Appeal n. 2251294-54.2015.8.26.0000*. Rapporteur: Judge Miguel Brandi, Trial date: 21/09/2016, 7th Chamber of Private Law, published on: 21/09/2016.

79 This approach can be observed in the following Interlocutory Appeals: TJSP. *Interlocutory Appeal n. 2149601-90.2016.8.26.0000*, Rapporteur: Judge Ricardo Pessoa de Mello Belli, Trial date: 05/12/2016, 19th Chamber of Private Law, published on: 11/01/2017; TJSP. *Interlocutory Appeal n. 2120450-79.2016.8.26.0000*. Rapporteur: Judge Costa Netto, Trial date: 13/12/2016, 9th Chamber of Private Law, published on: 19/12/2016; e TJAM. *Interlocutory Appeal n. 4004023-74.2016.8.04.0000*. Rapporteur: Judge Maria do Rosário Perpétuo Socorro Guedes Moura, published on: 05/06/2017, 2th Chamber of Private Law.

arguments, not only those contained in reports, but also those included in bibliographic references referring to the subject. It was noted that only 17 of the 82 decisions[80] considered such arguments. Among them, 11 decisions cited technical opinions that defined the obligation to provide logical gates, and 6 denied it.

The most frequent **technical reference** in the judgments is the final report of activities of the Working Group for the Implementation of the IP-Version 6 Protocol in the Networks of the Telecommunications Service Providers, published by Anatel in 2014. The group brought together not only representatives of Anatel, but also of telecommunication service providers with the objective of discussing the implementation of IPv6 in the country, its transitional period and the techniques to be used in order to do so.[81] In Brazil, the report represents the most significant discussion, under a technical perspective, about NAT techniques, IP sharing and logic gates. Therefore, the document is used in most of the decisions as a technical reference. Curiously, judicial references to the Report are found both to support favorable[82] and contrary[83] decisions as to the obligation of the application provider to provide logic gates.

Anatel's working group Report is not the only publicly available opinion on the subject. TIM Brasil connection provider, for example, indicates in the public consultation of the Ministry of Justice for the decree regulating the Brazil's Internet Bill of Rights that: "[...] the logic gate is not characterized as a registry of access to internet applications, according to Law. On the contrary, logic gates are related to the concept of connection records, since it is an information that complements the IP address."[84] It therefore observed the inertia of the Judiciary branch to seek other technical sources regarding the matter.

Requests for Clarificatinon

Some of the decisions of the courts were questioned by Requests for Clarification. Database 2 sought to gather the profile of these proceedings as well and to verify if the decisions were somehow reviewed. The Requests were only found in the Court of Justice of the state of São Paulo. Just as in Database 1, application providers were the major category of parties, both as defendant and plaintiff. It has been found that most of the Requests for Clarification do not deal with the material object of the claims[85], the logic gates, insisted focusing on strictly procedural arguments, such as the requirements for Requests for Clarification, their nature, their purpose. Some decisions identify a delaying purpose in the filing of Requests for Clarification. For this reason, another important fact regarding Requests for Clarification is that most do not change the aggravated decisions:

80 That entails 20.7% of the decisions analyzed by this study. In 79.3% of the decisions, at least in the Courts of Appeal, technical or especialized arguments were not taken into consideration.

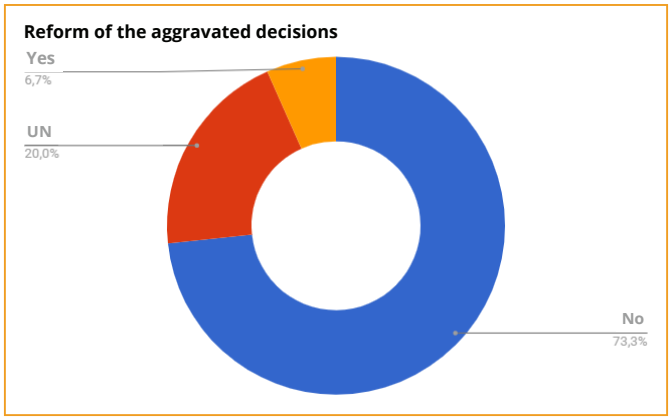
81 Free translation into English: "Article 1. Constitute the Working Group for the Implementation of the IP-Version 6 Protocol in the Networks of the Telecommunications Service Providers – GT-IPv6, with the participation of telecommunication service providers and of Anatel's Especialized Coordinators involved, with the aim of coordenating the actions necessary to adopt the IP-Version 6 Protocol in the networks of Brazilian telecommunication service providers. Anatel. *GT-IPv6: Grupo de Trabalho para implantação do protocolo IP-Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações -Relatório Final de Atividades.* Brasília. 12/2014. Available at: <http://bit.ly/2vy4e9U>. Acessed on: 01/09/2017.

82 One of the decisions that defined the obligation of application providers to supply logic gates and that referenced the GT-IPv6 Report was the Interlocutory Appeal n. 2257879-25.2015.8.26.0000. TJSP. *Interlocutory Appeal n. 2257879-25.2015.8.26.0000.* Rapporteur: Judge J.L. Mônaco da Silva, Trial date: 14/03/2016, 5th Chamber of Private Law, published on: 14/03/2016.

83 As an example of decision that does not define the obligation to provide logic gates and references the Report, see TJSP. *Interlocutory Appeal n. 2189710-83.2015.8.26.0000.* Rapporteur: Judge Ana Lucia Romanhole Martucci, Trial date: 27/11/2015, 6th Chamber of Private Law, published on: 28/11/2015.

84 TIM BRASIL. *"Armazenamento da porta lógica de origem pelos provedores de aplicação".* Available at: <https://goo.gl/LDp7py>. Acessed on: 10/10/2016.

85 80% of the decisions were based on strictly procedural matters. See Database 2, in the annex.



7. Final considerations

It is possible to identify that the problematic regarding logic gates is controversial not only in Brazil, due to the worldwide exhaustion of the IP version 4. At the same time, the implementation of IPv6 will reestablish direct connection of users with the internet, making it feasible the identification of every user. It is also admitted that such transition has been constantly delayed and that the NAT technique continues to be used, even with the new IP version. The discussion about whether (and who) should store and provide data needed for unambiguous identification ought to persist.

The analysis of the decisions collected in Brazilian courts reflects the uncertainties on the subject, since diametrically different understandings are found, without standardization in this phase of our analysis. The interpretation of mandatory access records by application providers is not peaceful, nor is there a uniform solution to the provisions of the Brazil's Internet Bill of Rights.

It is still necessary to consider that many of the decisions analyzed are not the final solution to the proceedings, and were resorted to without the entire framework of procedural evidences being exhausted. In any case, they should be monitored in order to analyze the evidence presented by parties involved and how they will be considered in the solution of the controversy. The results found in the research are, therefore, quite heterogeneous and unbounded jurisprudential perspectives, although it has prevailed the understanding that the application providers do not have the legal obligation to provide the logic gate of origin to the authorities.

Finally, in the absence of public and legislative policies on the use of the NAT technique and on the use of logic gates, it should be noted that the Judiciary branch has been asked to define its position on the issue. In this context, besides the technical aspects, the economic, innovative and viability impacts of small companies should be considered, considering the need to identify users who may have committed illicit acts, considering the principles defined by the Brazil's Internet Bill of Rights for internet governance in Brazil.

8. References

Books, articles and thesis

Anatel . "GT IPv6: Grupo de Trabalho para implementação do protocolo IP-Versão 6 nas redes das Prestadoras de Serviços de Telecomunicações, *Relatório Final de Atividades*." Dezembro de 2014. Available at: <http://bit.ly/2zk0tTF>. Access on: 20/09/2017.

AUSTRALIA. "Telecommunications (Interception and Access) Act" Nº 114, 1979, Compilation Nº. 96. Available at: <http://bit.ly/2yTtp97>. Access on: 05/10/2017.

AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Data retention - Frequently Asked Questions for Industry*. Julho de 2015. Available at: <http://bit.ly/2gOWCJG>. Access on: 06/10/2017.

AUSTRALIAN GOVERNMENT - Attorney-General's Department. *Guidelines for Service Providers* . Julho de 2015. Available at: <http://bit.ly/2gOWCJG>. Access on: 06/10/2017

BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATION *Report on OTT services*. 2016. p. 14. Available at:<http://bit.ly/2yRFc3s>. Access on: 08/10/2017.

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY. "Internet Protocol: DARPA Internet Program Protocol Specification". *IETF*, RFC791. Setembro de 1981. Available at: <http://bit.ly/2jy2SCa>. Access on: 20/09/2017.

DURAN, Alan et al. "Logging Recommendations for Internet-Facing Servers". *IETF*, RFC6302. Junho de 2011. Available at: <http://bit.ly/2kgwjye>. Access on: 02/10/2017.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA). *Data retention across the EU*. Available at: <http://bit.ly/2zhJIZu>. Access on: 18/10/2017.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA). *Fundamental Rights Report 2017*. 2017. p.162-165. Available at: <http://bit.ly/2yvAxoY>. Access on: 18/10/2017.

EUROPOL. *About Europol.* Available at:<http://bit.ly/2jWsUV8>. Access on: 29/09/2017.

EUROPOL/EC3 - 5127/17. "Carrier-Grade Network Address Translation (CGN) And the Going Dark Problem". 16 de Janeiro de 2017. p. 7. Available at: <http://bit.ly/2hw37OX> e <http://bit.ly/2yDviCI>. Access on: 29/09/2017.

EUROPOL. "*IOCTA 2016 - Internet Organised Crime Threat Assessment*". Available at: <http://bit.ly/2fCum7o>. p. 57 e 58. Access on: 25/09/2017.

HINDEN, Robert M. e DEERING, Stephen E. "Internet Protocol, Version 6 (IPv6)". *IETF.* RFC2460. Dezembro de 1998. Available at: <http://bit.ly/2ilJ4Xz>. Access on: 20/09/2017.

HURST, Daniel. *Telcos question data retention plans that exempt Facebook, Gmail and Skype*. The Guardian. 2015. Available at: <http://bit.ly/2xqggnn>. Access on: 08/10/2017.

JIANG, Sheng, GUO, Dayong & CARPENTER, Brian. "An incremental Carrier-Grade NAT (CGN) for IPv6 Transition". *IETF*, RFC6264. Junho de 2011. Available at: <http://bit.ly/2gOo5ZQ> Access on: 20/09/2017.

SRISURESH, Pyda & HOLDREGE, Matt. "IP Network Addres Translator (NAT) Technology and Considerations. *IETF*, RFC2663. Agosto de 1999. Available at: <http://bit.ly/1FFjvRC> Access on: 20/09/2017.

SUZOR, Nicolas; PAPPALARDO, Kylie; McINTOSH, Natalie. *The passage of Australia's data retention regime: national security, human rights, and media scrutiny*. Internet Policy Review- Journal on Internet Regulation.Volume 6, Edição 1. Março de 2017. Available at: <http://bit.ly/2y4aUeB>. Access on: 08/10/2017.

TIM BRASIL. *"Armazenamento da porta lógica de origem pelos provedores de aplicação".* Available at: <https://goo.gl/LDp7py>. Access on: 10/10/2016.

EU - *Directive 2006/24/EC* of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. Available at: <http://bit.ly/2fPZOWg>. Access: 04/10/2017

WEBER, Rolf H. *Shaping internet governance: Regulatory challenges.* Springer Science & Business Media, 2010.

Cases

CJEU. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources Ireland and others and Kärntner Landesregierung*. Joined cases C-293/12 and C-594/12, Grand Chamber, 8 de abril de 2014. Available at: <https://goo.gl/fjqymW>. Access on: 04/10/2017.

CJEU. *Patrick Breyer v. Bundesrepublik Deutschland*. Case C-582/14. 19 Outubro de 2016. Available at: <http://bit.ly/2gsdqaf>. Access on: 18/10/2017.

CJEU. T*ele2 Sverige AB contra Post- och telestyrelsen e Secretary of State for the Home Department contra Tom Watson*. Case C-203/15.2016. Available at: <http://bit.ly/2yxxiNR>. Access on: 18/10/2017.

CJEU. The Court of Justice of the European Union. *Press Release Nº 54 /14*. Luxemburgo, 8 de Abril de 2014. Available at: <http://bit.ly/2tBS4lV>. Access on: 04/10/2017.

Brazilian Superior Court of Justice - STJ, *Special Appeal nº 1403749/GO,* Justice Nancy Andrighi, 3rd Chamber, Trial date: 22/10/2013.

Brazilian Superior Court of Justice - STJ, *Special Appeal nº 897.089 - SP (2016/0087515-0)*, Monocratic Decision, Justice Moura Ribeiro, Trial date: 16/09/2016.

Brazilian Superior Court of Justice - STJ, *Special Appeal nº 1011826 - SP (2016/0293419-7)*, Monocratic Decision, Justice Nancy Andrighi, Trial date: 28/06/2017.

TJAM. *Interlocutory Appeal n. 4004023-74.2016.8.04.0000.* Rapporteur: Maria do Rosário Perpétuo Socorro Guedes Moura, Trial date: 05/06/2017, 2th Chamber of Private Law.

TJSP. *Interlocutory Appeal nº 2120450-79.2016.8.26.0000/TJS*P. Rapporteur: Costa Netto, Trial date: 13/12/2016, 9th Chamber of Private Law, published on: 19/12/2016.

TJSP. *Interlocutory Appeal nº 2108286-82.2016.8.26.0000*, Rapporteur: Alcides Leopoldo e Silva Júnior, Trial date: 13/09/2016, 1th Chamber of Private Law, published on: 13/09/2016.

TJSP. *Interlocutory Appeal nº 2185053-64.2016.8.26.0000.* Rapporteur: J.L. Mônaco da Silva, Trial date: 16/11/2016, 5th Chamber of Private Law, published on: 21/11/2016.

TJSP. *Interlocutory Appeal nº 2158001-30.2015.8.26.0000/TJSP.* Rapporteur: Rui Cascaldi. Trial date: 03/11/2015, 1th Chamber of Private Law, published on: 04/11/2016.

TJSP. *Interlocutory Appeal n. 2087441-29.2016.8.26.0000*. Rapporteur: Moreira Viegas, Trial date: 23/11/2016, 5th Chamber of Private Law, published on: 24/11/2016.

TJSP. *Interlocutory Appeal n. 2083730-16.2016.8.26.0000.* Rapporteur: Vito Guglielmi, Trial date: 14/07/2016, 6th Chamber of Private Law, published on: 15/07/2016.

TJSP. *Interlocutory Appeal n. 2251294-54.2015.8.26.0000*. Rapporteur: Miguel Brandi, Trial date: 21/09/2016, 7th Chamber of Private Law, published on: 21/09/2016.

TJSP. *Interlocutory Appeal n. 2257879-25.2015.8.26.0000.* Rapporteur: J.L. Mônaco da Silva, Trial date: 14/03/2016, 5th Chamber of Private Law, published on: 14/03/2016.

TJSP. *Interlocutory Appeal n. 2189710-83.2015.8.26.0000*. Rapporteur: Ana Lucia Romanhole Martucci, Trial date: 27/11/2015, 6th Chamber of Private Law, published on: 28/11/2015.

9. Appendix

Data base 01

-	Estado (UF)	Ano	Polo ativo categorizado	Polo passivo categorizado	Multa	Valor da Multa	Tutela provisória	Argumento est. processual	Cita o MC? *	Se Sim, qual dispositivo?	Obrigação de fornecer porta lógica (prov. apli.)	Cita precedentes sobre porta lógica	Cita parecer técnico	Interpretação teleológica MCI*	Interpretação literal MCI*
AI 2107751-27.2014.8.26.0000	SP	2014	PA	PA	Não	-	Sim	Sim	Não	-	Não	Não	Não	Não	Não
AI 2158001-30.2015.8.26.0000	SP	2015	PA	PN	Sim	Diária - R$5.000,00 sem teto	Sim	Não	Sim	Arts. 5º, VI a VIII, e 15, caput	Não	Sim	Não	Não	Sim
AI 2205211-77.2015.8.26.0000	SP	2015	PA	PJ	NI	-	NI	Não	Não	-	Não	Não	Não	Não	Não
AI 2012094-24.2015.8.26.0000	SP	2015	PA	PC	Não	-	Sim	Não	Não	-	Não	Não	Não	Não	Não
AI 2250400-78.2015.8.26.0000	SP	2015	PA	PJ	Não	-	Sim	Sim	Não	-	Sim	Não	Não	NI	NI
AI 2086530-51.2015.8.26.0000	SP	2015	PA	PA	Sim	-	Sim	Não	Sim	Art. 15	Sim	Não	Não	Sim	Não
AI 2228882-32.2015.8.26.0000	SP	2015	PA	PJ	Não	-	Sim	Sim	Não	-	Sim	Não	Não	NI	NI
AI 2227540-83.2015.8.26.0000	SP	2015	PA	PJ	Não	-	Não	Não	Não	-	Não	Não	Não	NI	NI
AI 2012094-24.2015.8.26.0000	SP	2015	PA	PC	Não	-	Sim	Não	Não	-	Não	Não	Não	NI	NI
AI 2112160-12.2015.8.26.0000	SP	2015	PA	PA	Não	-	Sim	Sim	Não	-	Sim	Não	Não	NI	NI
AI 2028312-30.2015.8.26.0000	SP	2015	PJ	PA	Sim	Diária R$ 5.000 limitada à quantia de R$ 150.000.	Sim	Não	Sim	Art. 22	Sim	Não	Não	NI	NI
AI 2136055-02.2015.8.26.0000	SP	2015	PA	PJ	Sim	Diária - R$1.000,00 a R$50.000,00	Sim	Sim	Não	-	Sim	Sim	Não	NI	NI
AI 2057480-77.2015.8.26.0000	SP	2015	PJ	PA	Sim	-	Sim	Não	Sim	Art. 22	Sim	Sim	Não	NI	NI
AI 2159146-58.2014.8.26.0000	SP	2015	PA	PJ	Não	-	Sim	Sim	Não	-	NI	Não	Não	NI	NI
AI 2092413-76.2015.8.26.0000	SP	2015	PA	PN	Sim	-	Sim	Não	Não	-	Não	Sim	Não	Não	Sim
AI 2203864-09.2015.8.26.0000	SP	2015	PA	PJ	Sim		Sim	Não	Sim	Art. 15	Não	Sim	Não	Não	Sim
AI 2150710-76.2015.8.26.0000	SP	2015	PA	PC	Sim	Diária - R$10.000,00 com valor máximo de R$500.000,00	Sim	Não	Sim	Art. 5º, VIII e 15	Não	Sim	Não	Não	Sim
AI 2255280-16.2015.8.26.0000	SP	2015	PA	PJ	Sim	R$50.000,00/dia	Sim	Não	Sim	Art. 5º, VIII	Não	Sim	Não	Não	Sim
AI 2172692-49.2015.8.26.0000	SP	2015	PA	PJ	Sim	Diária - R$2.000,00 sem teto	Sim	Não	Sim	Arts. 5º, VIII, e 15	Não	Sim	Não	Não	Sim
AI 2189710-83.2015.8.26.0000	SP	2015	PA	PJ	Não	-	Sim	Não	Sim	Arts. 5º, VIII, e 15	Não	Sim	Sim	Não	Sim
AI 2172692-49.2015.8.26.0000	SP	2015	PA	PJ	Sim	Diária - R$ 2.000,00	Sim	Não	Sim	-	Não	Sim	Sim	Não	Sim
AI 2219.128-03.2014.8.26.0000	SP	2015	PA	PJ	Sim	Diária - R$ 2..500,00 sem teto	Sim	Não	Sim	Arts. 10, §2º, e 20	Não	Não	Não	NI	NI
AI 2040293-22.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$5.000,00/dia até R$500.000,00	Sim	Não	Sim	Art. 22	Sim	Sim	Não	Sim	Não
AI 2274058-34.2015.8.26.0000	SP	2016	PN	PA	Não	-	Sim	Não	Sim	Arts. 10, § 1º; 13; 15; e art 22	Não	Sim	Não	Não	Não
AI 2254100-62.2015.8.26.0000	SP	2016	PA	PN	Não	-	Sim	Não	Não	-	Sim	Não	Não	Não	Não
AI 2072406-29.2016.8.26.0000	SP	2016	PA	PA	Sim	Diária - R$5000,00 sem teto	Sim	Não	Sim	Arts. 5º, VII, e 15	Sim	Sim	Não	Não	Não
AI 2061576-04.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$5.000,00 sem teto	Sim	Não	Sim	Art. 5º, VI e VIII, e 15	Sim	Sim	Não	Sim	Não
AI 2061576-04.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$5.000,00 sem teto	Sim	Não	Sim	Arts. 5º, VI e VIII, e 15	Sim	Sim	Não	Sim	Não
AI 2257879-25.2015.8.26.0000	SP	2016	PA	PJ	Não	-	Sim	Não	Sim	Art. 5º, VIII	Sim	Sim	Sim	Sim	Não
AI 2081265-34.2016.8.26.0000	SP	2016	PA	PJ	Não	-	Sim	Não	Sim	Arts 6 e 10.	Sim	Sim	Sim	Sim	Não
AI 2185053-64.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$ 1.000,00 (limite 90 dias)	Sim	Não	Sim	Arts. 5º,VIII; 10, capu, e § 1º; e 15	Sim	Sim	Sim	Sim	Não
AI 2092101-03.2015.8.26.0000	SP	2016	PJ	PJ	Sim	Não especificado	Não	Não	Não	-	Não	Não	Não	NI	NI
AI 2136855-93.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$ 5.000,00	Sim	Não	Não	-	Não	Não	Não	NI	NI
AI 2134739-17.2016.8.26.0000	SP	2016	PC	PN	Sim	Diária R$ 10.000,00.	Sim	Não	Não	-	Não	Não	Não	NI	NI
AI 2108074-61.2016.8.26.0000	SP	2016	PA	PJ	Sim	R$ 1.000,00 limitado à R$ 10.000,00.	Sim	Não	Sim	Art. 5º, VIII, e 15.	Não	Sim	Não	Não	Sim
AI 2004349-56.2016.8.26.0000	SP	2016	PC	PJ	Não	-	Não	Sim	Não	-	Não	Não	Não	NI	NI
AI 2057550-60.2016.8.26.0000	SP	2016	PJ	PA	Não	-	Sim	Sim	Não	-	Não	Não	Não	NI	NI
AI 2139037-52.2016.8.26.0000	SP	2016	PA	PJ	Não	-	Sim	Não	Não	-	Sim	Não	Não	NI	NI
AI 2039490-39.2016.8.26.0000	SP	2016	PJ	PA	Sim	Diária - R$1.000,00 sem teto	Sim	Não	Não	-	Sim	Não	Não	NI	NI
AI 2206954-25.2015.8.26.0000	SP	2016	PA	PJ	Não	-	Não	Não	Sim	Art 5º, 6º, 10º, §1º	Sim	Sim	Sim	Sim	Não
AI 2258906-43.2015.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$ 50.000,00	Sim	Não	Sim	Art 5º, 6º, 10º, §1º	Sim	Sim	Sim	Sim	Não
AI 2175598-75.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária - R$10.000,00 a R$310.000,00	Sim	Sim	Não	-	Sim	Não	Não	NI	NI
AI 2109770-35.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$10.000,00 sem teto	Sim	Sim	Não	-	Sim	Não	Não	NI	NI
AI 2108286-82.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária - R$ 100.00, até no máximo R$ 2.000,00.	Sim	Não	Sim	Arts 5º, V,VI, VII e VIII; e 15	NI	Sim	Não	NI	NI
AI 2250177-28.2015.8.26.0000	SP	2016	PA	PJ	Não	-	Não	Sim	Não	-	Não	Não	Não	NI	NI
AI 2057550-60.2016.8.26.0000	SP	2016	PJ	PA	Não	-	Não	Sim	Não	-	NI	Não	Não	NI	NI
AI 2149601-90.2016.8.26.0000	SP	2016	PJ	PA	Não	-	Sim	Não	Sim	Arts 5º, VII, 15, §§	Sim	Sim	Sim	Sim	Não
AI 2040105-29.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária - R$1.000,00	Sim	Não	Sim	Art. 5º, VIII e 15	Não	Não	Não	Não	Sim
AI 2120450-79.2016.8.26.0000	SP	2016	PA	PJ	Sim	Diária R$500,00 - limite: R$50.000,00	Sim	Não	Sim	Arts. 5º, VIII; 10; 19; 22	Sim	Não	Não	Sim	Não
AI 2072406-29.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária - R$ 5.000,00 sem teto	Sim	Não	Sim	Arts. 5º, VII e VIII, e 15	Não	Não	Não	Não	Sim
AI 2110716-07.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária R$ 1.000,00	Sim	Não	Sim	Art 5º, V e VII	Não	Não	Não	Não	Sim
AI 2251294-54.2015.8.26.0000	SP	2016	PA	PJ	Sim	-	Sim	Não	Sim	Arts 5º, VIII e 15, § 1°	Não	Não	Não	Não	Sim
AP 1088666-63.2014.8.26.0100	SP	2016	PN	PA	Sim	Não	Sim	Sim	Sim	Arts. 10 e 22	Não	Não	Não	Não	Sim
SE 2066773-37.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária - R$10.000,00 (limite 10 dias)	Não	Não	Sim	Arts. 5º, VIII e 15	Não	Sim	Não	Não	Sim
AP 1055250-07.2014.8.26.0100	SP	2016	PN	PA	Sim	-	Não	Não	Sim	Arts. 5º, VIII e 15	Não	Sim	Não	Não	Sim
AP 1108368-58.2015.8.26.0100	SP	2016	PA	PJ	Não	-	Não	Não	Sim	Arts. 5º, VIII e 15	Não	Sim	Não	Não	Sim
AI 2078865-47.2016.8.26.0000	SP	2016	PN	PA	Sim	Diária R$500,00.	Sim	Não	Sim	Arts. 5°, VIII, e 15.	Não	Sim	Não	Não	Sim

-	Estado (UF)	Ano	Polo ativo categorizado	Polo passivo categorizado	Multa	Valor da Multa	Tutela provisória	Argumento est. processual	Cita o MC? *	Se Sim, qual dispositivo?	Obrigação de fornecer porta lógica (prov. apli.)	Cita precedentes sobre porta lógica	Cita parecer técnico	Interpretação teleológica MCI*	Interpretação literal MCI*
AI 2106771-12.2016.8.26.0000	SP	2016	PA	PJ	Sim	R$ 1.000,00.	Sim	Não	Sim	Arts 5º V, VI, VII e VIII, e 15	Não	Sim	Não	Não	Sim
AI 2064240-08.2016.8.26.0000	SP	2016	PC	PA	Sim	Diária R$ 500,00.	Sim	Não	Sim	Arts 5°, inciso VIII, e 15.	Não	Sim	Não	Não	Sim
AI 2027881-59.2016.8.26.0000	SP	2016	PC	PA	Sim	Diária de R$ 500,00, limitada a R$25.000,00	Sim	Não	Sim	Arts 5°, VIII, e 15.	Não	Sim	Não	Não	Sim
AI 2084529-59.2016.8.26.0000	SP	2016	PA	PN	Não	-	Sim	Não	Sim	Arts. 5º, VI e VIII e 22	Não	Sim	Não	Não	Sim
AI 2184364-20.2016.8.26.0000	SP	2016	PA	PN	Sim	Diária R$ 5.000,00	Sim	Não	Sim	Arts 5°, VIII e 15.	Não	Sim	Não	Não	Sim
AI 2256281-36.2015.8.26.0000	SP	2016	PN	PA	Não	-	Sim	Não	Não	-	Não	Sim	Sim	Não	Sim
AI 2252527-86.2015.8.26.0000	SP	2016	PA	PJ	Sim	Diária de R$ 3.000,00	Sim	Não	Sim	Arts 5°, VIII, e 15.	Não	Sim	Sim	Não	Sim
AI 2083730-16.2016.8.26.0000	SP	2016	PA	PJ	Sim		Sim	Não	Sim	Arts 5º e 15	Não	Sim	Sim	Não	Sim
AI 2087084-15.2017.8.26.0000	SP	2017	PA	PA	Sim		Sim	Não	Sim	Art. 5º, VIII	Sim	Sim	Sim	Sim	Não
AI 2168151-36.2016.8.26.0000	SP	2017	PA	PJ	Não	-	Sim	Não	Sim	Art. 5º, III	Sim	Sim	Sim	Sim	Não
AI 2216048-60.2016.8.26.0000,	SP	2017	PA	PN	Sim	Diária - R$ 2.000,00 até R$ 20.000,00.	Sim	Não	Não	-	Não	Sim	Não	Não	Não
AI 2225114-64.2016.8.26.0000	SP	2017	PA	PN	Sim	Diária - R$ 2.000,00 até R$20.000,00	Sim	Não	Não	-	Não	Sim	Não	Não	Não
AI 0620437-78.2017.8.06.0000	CE	2017	PC	PJ	Sim	R$ 4.400,00.	Sim	Não	Sim	-	Não	Sim	Não	Não	Não
AP 0004132-12.2015.8.26.0411	SP	2017	PJ	PA	Não	-	Não	Não	Sim	Arts. 5º, VIII; 6º; 15; e 16, II	Sim	Sim	Sim	Sim	Não
AI 4004023-74.2016.8.04.0000	AM	2017	PA	PN	Sim	Diária - 1.000,00 limite até R$20.000	Sim	Não	Sim	Arts. 5º III, IV, V e VI, e 22	Sim	Sim	Sim	Sim	Não
AI 2034460-86.2017.8.26.0000	SP	2017	PN	PJ	Não	-	Não	Não	Sim	Arts. 7º, I, e 8º	Não	Não	Não	NI	NI
AI 2087441-29.2016.8.26.0000	SP	2017	PA	PN	Não	-	Sim	Não	Sim	Art 5º, VIII	Não	Sim	Não	Não	Sim
AI 2251999-18.2016.8.26.0000	SP	2017	PN	PA	Sim	Diária - R$500,00 a R$20.000,00	Sim	Não	Não	-	Sim	Não	Não	NI	NI
AI 2106758-13.2016.8.26.0000	SP	2017	PA	PJ	Sim	R$ 2.000,00/dia	Sim	Não	Sim	Art. 15	Sim	Não	Sim	NI	NI
AP 1078660-60.2015.8.26.0100	SP	2017	PC	PA	Não	-	Não	Não	Sim	Art. 10, §1º	Não	Sim	Não	Não	Sim
AI 2062855-88.2017.8.26.0000	SP	2017	PC	PA	Não	-	Não	Não	Sim	Arts. 5º, VIII, e 15	Não	Sim	Não	Não	Sim
AI 2062855-88.2017.8.26.0000	SP	2017	PC	PA	Não	-	Sim	Não	Sim	Arts 5º, V, VII e VIII; e 15	Não	Sim	Não	Não	Sim
AI 2225928-76.2016.8.26.0000	SP	2017	PC	PJ	Sim	Diária - R$500,00 a R$100.000,00	Sim	Não	Sim	Arts. 5º, V, VII e VIII; e 15	Não	Sim	Não	Não	Sim
AI 2203488-86.2016.8.26.0000	SP	2017	PA	PJ	Sim	Diária - R$500,00 a R$5.000,00	Sim	Sim	Sim	Arts. 5º, VIII, e 15	Não	Sim	Não	Não	Sim
AI 2072869-68.2016.8.26.0000	SP	2017	PA	PJ	Sim	Diário - R$ 1.000,00	Sim	Não	Sim	Arts. 5º, inc. VIII, 6 e 15	Não	Sim	Sim	Não	Sim

Legenda
PA = provedor de aplicação
PC = provedor de conexão
PJ = pessoa jurídica que Não PA e PC
PN = pessoa natural
NI = Não identificável

Data base 02

Embargo	Estado (UF)	Ano	Polo ativo categorizado	Polo passivo categorizado	Reforma da decisão agravada	Argumentação estritamente processual
ED 2168151-36.2016.8.26.0000/50000	SP	2.017	PA	PJ	Não	Sim
ED 2105786-43.2016.8.26.0000/50000	SP	2.016	PJ	PN	NI	Sim
ED 2107751-27.2014.8.26.0000/50000	SP	2.014	PJ	PA	Não	Sim
ED 2216048-60.2016.8.26.0000/50001	SP	2.017	PN	PA	Não	Sim
ED 0620437-78.2017.8.06.0000/50000	CE	2.017	PC	PJ	Não	Sim
ED 2250400-78.2015.8.26.0000/50000	SP	2.015	PA	PJ	Não	Não
ED 2228882-32.2015.8.26.0000/50001	SP	2.016	PA	PA	Não	Sim
ED 2081265-34.2016.8.26.0000/5000	SP	2.016	PJ	PJ	Não	Sim
ED 2108074-61.2016.8.26.0000/50000	SP	2.016	PJ	PA	Não	Sim
ED 2090609-73.2015.8.26.0000/50000	SP	2.015	PA	PA	NI	Sim
ED 2142453-62.2015.8.26.0000/50000	SP	2.016	PJ	PA	NI	Sim
ED 2107751-27. 2014.8.26.0000/50000	SP	2.014	PA	PA	NI	Sim
ED 2087441-29.2016.8.26.0000/50000	SP	2.017	PN	PA	Não	Sim
ED 2139037-52.2016.8.26.0000/50000	SP	2.017	PA	PJ	Sim	Sim
ED 2039490-39.2016.8.26.0000/50000	SP	2.016	PJ	PA	Não	Não
ED 2039490-39.2016.8.26.0000/50001	SP	2.016	PA	PJ	Não	Sim
ED 2039490-39.2016.8.26.0000/50002	SP	2.016	PA	PJ	Não	Sim
ED 2125513-85.2016.8.26.0000/50000	SP	2.016	PJ	PA	NI	Sim
ED 2206954-25.2015.8.26.0000/50000	SP	2.016	PA	PJ	Não	Sim
ED 2258906-43.2015.8.26.0000/50000	SP	2.017	PA	PJ	Não	Sim
ED 2106303-48.2016.8.26.0000/50000	SP	2.016	PJ	PA	NI	Sim
ED 2131118-46.2015.8.26.0000/50000	SP	2.015	PN	PA	NI	Sim
ED 2149601-90.2016.8.26.0000/50000	SP	2.017	PA	PC	NI	Sim
ED 2040105-29.2016.8.26.0000 /50000	SP	2.016	PJ	PA	Não	Sim
ED 2120450-79.2016.8.26.0000/50000	SP	2.017	PA	PJ	Não	Sim
ED 2203864-09.2015.8.26.0000/50000	SP	2.016	PJ	PA	NI	Sim
ED 2150710-76.2015.8.26.0000/50000	SP	2.016	PC	PA	Não	Não
ED 2078865-47.2016.8.26.0000/50001	SP	2.017	PN	PA	Não	Não
ED 2106771-12.2016.8.26.0000/50000	SP	2.016	PJ	PA	Não	Sim
ED 2064240-08.2016.8.26.0000/50000	SP	2.016	PC	PA	Sim	Não
ED 2027881-59.2016.8.26.0000/50000	SP	2.016	PC	PA	Não	Não
ED 2172692-49.2015.8.26.0000/50000	SP	2.015	PJ	PA	Não	Não
ED 2203488-86.2016.8.26.0000/50000	SP	2.017	PA	PJ	Não	Sim
ED 2057480-77.2015.8.26.0000/50000	SP	2.015	PA	PJ	Sim	Não
ED 2158001-30.2015.8.26.0000/50001	SP	2.016	PN	PA	Não	SIm
ED 2227540-83.2015.8.26.0000/50000	SP	2.016	PA	PJ	Não	Sim
ED 2012094-24.2015.8.26.0000/50000	SP	2.015	PC	PA	Não	Sim
ED 2090609-73.2015.8.26.0000/50000	SP	2.016	PJ	PA	Não	Sim
ED 2172692-49.2015.8.26.0000/50000	SP	2.015	PJ	PA	Não	Sim
ED 2189710-83.2015.8.26.0000/50000	SP	2.016	PJ	PA	Não	Sim
ED 2219.128-03.2014.8.26.0000/50000	SP	2015	PJ	PA	Não	Sim
ED 2225114-64.2016.8.26.0000/50000	SP	2017	PN	PA	Não	Sim
ED 2083730-16.2016.8.26.0000/50000	SP	2016	PJ	PA	Não	Sim
ED 2252527-86.2015.8.26.0000/50000	SP	2016	PJ	PA	Não	Não
ED 1055250-07.2014.8.26.0100/50000	SP	2016	PN	PA	Não	Sim

Legenda
PA = provedor de aplicação PC = provedor de conexão PJ = pessoa jurídica que Não PA e PC PN = pessoa natural NI = Não identificável