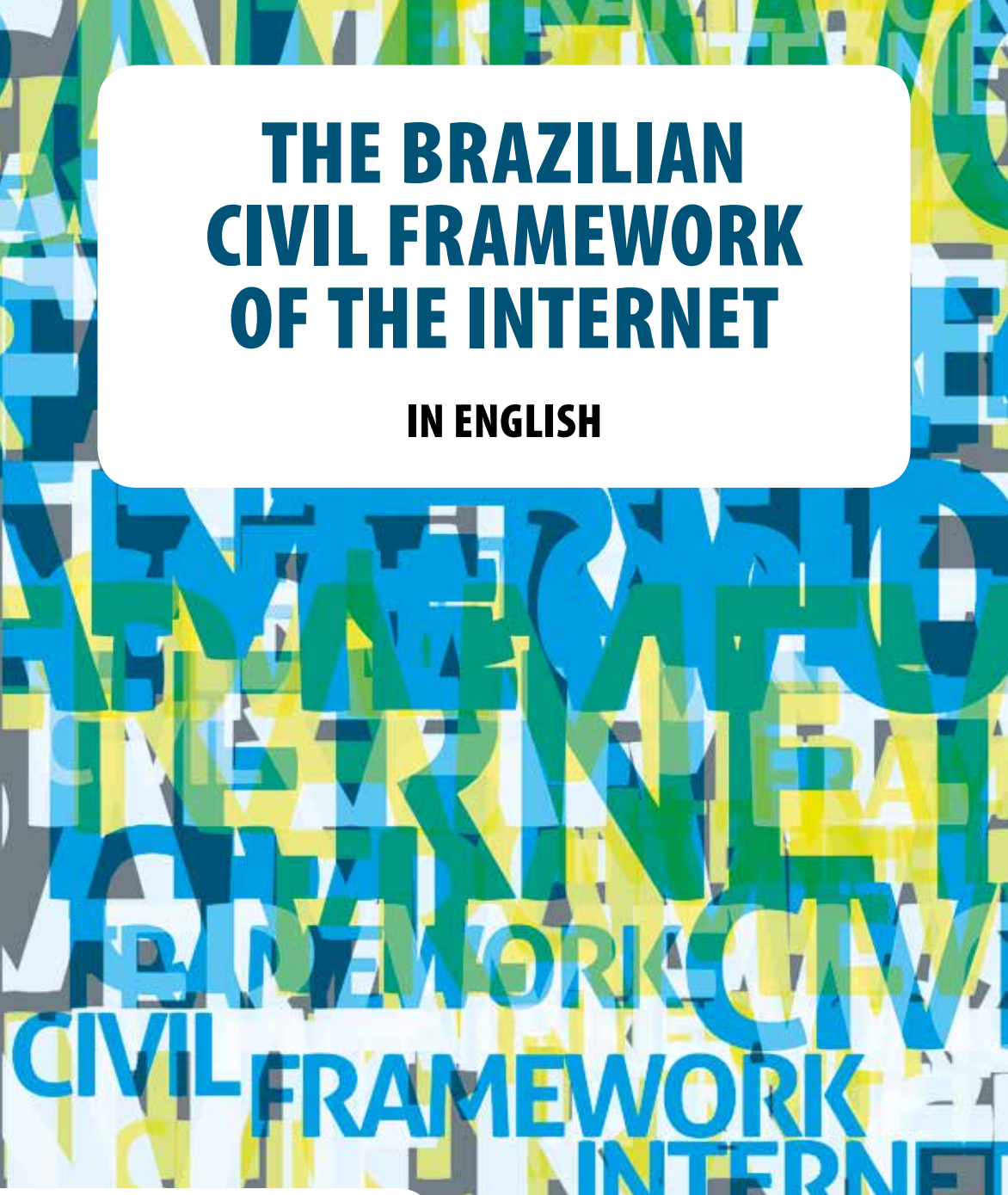
THE BRAZILIAN CIVIL FRAMEWORK OF THE INTERNET

IN ENGLISH



Chamber of Deputies

Série
Legislação

Brasília 2016

THE BRAZILIAN CIVIL FRAMEWORK OF THE INTERNET
IN ENGLISH

Chamber of Deputies
Directing Board
55th Legislature – 2015-2019

President
Eduardo Cunha

1st Vice President
Waldir Maranhão

2nd Vice President
Giacobo

1st Secretary
Beto Mansur

2nd Secretary
Felipe Bornier

3rd Secretary
Mara Gabrilli

4th Secretary
Alex Canziani

Secretaries Substitutes

1st Substitute
Mandetta

2nd Substitute
Gilberto Nascimento

3rd Substitute
Luiza Erundina

4th Substitute
Ricardo Izar

Director General
Rômulo de Sousa Mesquita

Secretary General of the Directing Board
Silvio Avelino da Silva

Chamber of
Deputies

THE BRAZILIAN CIVIL FRAMEWORK OF THE INTERNET

IN ENGLISH

Law No. 12,965, of April 23, 2014, which establishes the principles, guarantees, rights and duties for the use of the Internet in Brazil.

Documentation and Information Center
Edições Câmara
Brasília | 2016

CHAMBER OF DEPUTIES

Legislative Division
Head: *Afrísio Vieira Lima Filho*

Legislative Consultancy Office
Head: *Eduardo Fernandez Silva*

Documentation and Information Center
Head: *André Freire da Silva*

Edições Câmara Coordination
Head: *Heloísa Helena S. C. Antunes*

Coordination of Organization of Legislative Information
Head: *Frederico Silveira dos Santos*

Cover graphic project: Janaina Coe
Inside graphic project: Patrícia Weiss
Desktop publishing: Janaina Coe
Translation: Fernanda Belotti Alice
Translation review: Laerte Ferreira Morgado (Federal Senate), Felipe Sampaio Wense and Pedro Tásio Viana Sobreira Bezerra

Translated from the original in portuguese titled *Marco Civil da Internet* – 2nd edition
(ISBN: 978-85-402-0362-4)

This edition includes the rules in force until their closure, on October 27, 2015.

Câmara dos Deputados
Centro de Documentação e Informação – Cedi
Coordenação Edições Câmara – Coedi
Anexo II – Praça dos Três Poderes
Brasília (DF) – CEP 70160-900
Phone: +55 61 3216-5809
editora@camara.leg.br

SERIES
Legislação
n. 204

International Cataloging-in-Publication Data (CIP)
Library Coordination. Cataloging Section.

Brasil. [Lei n. 12.965, de 23 de abril de 2014].
Civil framework of the Internet [recurso eletrônico] : Law nº. 12.965, of April 23, 2014, which establishes the principles, guarantees, rights and duties for use of the Internet in Brazil. – Brasília : Chamber of Deputies, Edições Câmara, 2016. – (Série legislação ; n. 204)

Versão PDF.
Modo de acesso: http//www.camara.leg.br/editora
ISBN 978-85-402-0429-4

1. Internet, legislação, Brasil. I. Título. II. Série.

CDU 004.738.5(81)(094)

ISBN 978-85-402-0429-4 (PDF)

TABLE OF CONTENTS

INTRODUCTION 6

UNDERSTANDING THE CONTROVERSIES AND CHANGES BROUGHT BY THE BRAZILIAN CIVIL FRAMEWORK OF THE INTERNET 7

LAW No. 12,965 OF APRIL 23, 2014
(The Brazilian Civil Framework of the Internet)
Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil. 24

Chapter I – Preliminary Provisions 24

Chapter II – Rights and Guarantees of Users 26

Chapter III – Provision of Connection and Internet Applications 27

Section I – Network Neutrality 27

Section II – Protection of Logs, Personal Data and Private Communications 28

Subsection I – Keeping Connection Logs 30

Subsection II – Keeping Connection Logs of Internet Applications in the Provision of Connection 30

Subsection III – Keeping Connection Logs of Internet Applications in the Provision of Applications 31

Section III – Responsibility for Damages Arising from Content Generated by Third Parties 32

Section IV – Judicial Request for Records 33

Chapter IV – The role of public power 33

Chapter V – Final Provisions 35

INTRODUCTION

This book in the Série Legislação of Edições Câmara brings the updated text of the Brazilian Civil Framework of the Internet, Law No. 12,965, of April 23, 2014.

The Chamber of Deputies goes beyond creating rules with the publication of the Brazilian federal legislation: it works also for their effective compliance by making them known and accessible to the entire population.

The legal text presented in this issue is the result of the work of parliamentarians, who represent the diversity of the Brazilian people. From the presentation to the approval of a law project, there is an extensive road of consultations, studies and discussions with the various social sectors. After they are created, the laws provide a legal framework that makes it possible for people to live together well in society.

The content published by Edições Câmara is also available at the Chamber's Digital Library (bd.camara.leg.br/bd/) and its publisher's website (camara.leg.br/editora). Some publications are also produced in audiobook, epub and Braille formats. The goal is to democratize the access to information and encourage the full exercise of citizenship.

Thus, the Chamber of Deputies contributes to disseminate information about rights and duties to those mainly interested on the subject: the citizens.

Deputy Eduardo Cunha
President of the Chamber of Deputies

UNDERSTANDING THE CONTROVERSIES AND CHANGES BROUGHT BY THE BRAZILIAN CIVIL FRAMEWORK OF THE INTERNET

1. Introduction

The proceedings of the so-called *Civil Framework of the Internet,* sanctioned on April 23, 2014, and converted into the Law 12,965, raised heated debates in society and the Parliament. Several times the discussion caused the segments of different opinions to be on diametrically opposite sides. Since internet is a tool used by the majority of the population, as well as by small, medium and large companies,[1] the Bill 2,126/2011, which was presented in the Chamber of Deputies by the Executive Branch, would have been a cause for conflict whatever the result of the legislative solution to its proceedings.

The initiative, named with the epithet *Constitution of the Internet,* as stated on its summary "establishes principles, guarantees, rights and duties for the use of the Internet in Brazil." In addition to being a statement of principles for use, and to ensure the privacy, human rights and citizenship in digital media, the proposal also seeks to regulate various aspects related to the commercial and governmental exploitation of this large network. Many controversies arouse as a result of the discussion of these subjects. The storage of users data by the Internet providers and by the companies responsible for the content on the Internet, the neutrality of the network and the general storage of data of Internet users in the country were among the issues that generated more debate among telecommunications companies, Internet content providers, copyright holders, the government, user pressure groups and many other actors.

This text, an update of the *Fique Por Dentro* newsletter, made available by the Chamber of Deputies in January 2014[2], aims to clarify the main ideas of the new law and the implications for the various sectors of its entry into force.

1. Data from the Brazilian Internet Steering committee indicate that 69% of the Brazilian population connects to the internet daily, and 97% of companies use the tool. Available at: <http://cgi.br/media/docs/publicacoes/2/tic-domicilios-e-empresas-2012.pdf>, p. 32. Access on 5/27/14.
2. Available at: <http://www2.camara.leg.br/documentos-e-pesquisa/fiquePorDentro/temas/marco-civil/texto-base-da-consultoria-legislativa>. Access on 5/28/14.

2. Brief history of the initiatives of Internet regulation in the Chamber of Deputies

The theme of Internet regulation is certainly controversial. In Brazil, the first proposal for a regulation to be approved in the Chamber was probably the Bill 84/1999, authored by Deputy Luiz Piauhylino, which became known as the Digital Crimes Bill. In the following year, Senator Luiz Estevão proposed the Senate Bill 151/2000 (in the Chamber, Bill 5,403/2001), which determined the storage of connection logs of Internet users.

The Digital Crimes Project – which considered as crime the invasion and change of contents of websites, the theft of passwords and the creation and dissemination of viruses – was approved in the Chamber in 2003, modified by the Senate in 2008, and returned to its chamber of origin for the consideration of modifications. During the second initiative of the bill in the Chamber, there was the episode of the invasion of privacy of the actress Carolina Dieckmann by means of the disclosure of material of her ownership. In reaction to the event, the Bill 2,793/2011, authored by Deputy Paulo Teixeira, was proposed. The case received great attention from de media, causing both projects to be approved in 2012. However, the Digital Crimes Law (12,735/2012) was drastically simplified and new criminal offenses were included in the Carolina Dieckmann Law (12,737/2012).

In contrast to the debates focused on the criminalization of improper Internet use, the Bill 2,126/2011, authored by the Executive Branch, was proposed. Conceived in the Ministry of Justice and the result of several public inquiries, the project countered the earlier initiatives of Internet regulation. Therefore, rather than focusing on the treatment of crimes and prohibitions, it guarantees freedom and rights to Internet users. Hence, the name by which it became known, the *Civil Framework of the Internet.*

During the final stage of the approval of the Civil Framework and possibly due to the political reverberation caused by the discussion of the matter, another proposal for an Internet regulation gained momentum during its legislative process: the Proposal of Amendment to the Constitution 479/2010. An initiative of Deputy Sebastião Bala Rocha, the amendment proposes the inclusion of Internet access among the fundamental rights of the citizen. In December 2013, the proposal's rapporteur, Deputy Amauri Teixeira, echoing the discussions of the Civil Framework, which still faced

difficulties in its approval, included the issue of neutrality in the report and established as a fundamental right of citizens the access not only to the Internet but also to a neutral Internet.[3]

3. The project and its progress in the Chamber

The main proposal sent by the Executive Branch attracted the attachment of 36 other projects, including the Bill 5,403/2001 mentioned above. The main ideas of the project, as originally proposed, were:

- Networks Neutrality

  The concept of neutrality means that telecom operators (those that supply broadband access) cannot interfere with the speed of bundles transmitted over the internet, giving priority to certain types of content over others. The original project guarantees some neutrality, that is to say, it allows the control of transfers by the providers under certain conditions that should be defined in regulation.

- Storage of connection logs

  The data of Internet connection (IP address used, time of connection, etc.) allow the identification of the users, which not only enables their monitoring, but also facilitates the investigation of illegal actions (for example, provision of illegal content). The project stated that the connection providers[4] should store connection logs during one year and, in case of a judicial request, transfer them to the competent authorities.

- The storage of connection logs of internet applications

  This connection log refers to the user's browsing history. In the original proposal, connection providers could not store data; only content providers were allowed to store them.[5] However, if requested by a judicial authority, content providers should store the data for investigations.

---

3. The amendment was still in progress at the time this text was written, in May 2014.
4. Connection providers are telecommunications companies that provide broadband to users (for example, telephone operators or cable).
5. Content providers are companies or individuals that provide the content of the Internet, which means, who feeds the web pages or posts any material on the network (text, audiovisual, etc.). In this group, are both global companies such as Google and Facebook, national companies like UOL and Globo, as well as users when they create personal pages (e.g. meunome.com.br). When users make use of companies' pages to post content (for example, comments on social networks or blogging in companies that host these applications), it is customary to name this material as content created by third parties.

- Liability for infringing materials

  The project regulates the practice of "notice and take down" for infringing materials such as music and audiovisual content protected by copyright, as well as defamatory or libelous content, among others. Because of this rule, the content provider would be liable if, after judicial notice, the material identified as infringing was not taken down.

In the Chamber, the project was also put into public consultation through the *e-Democracia* portal and, in September 2011, a special committee was established to consider the matter. Despite the widespread debate and the various regional seminars and public hearings, the opinion of the rapporteur, Deputy Alessandro Molon, was not voted. A year later, in 2013, the Executive Branch requested urgency for the matter, which, in Plenary, received 34 amendments. The proposal was also the subject of the general committee in November 2013, with the participation of parliamentarians and various actors in society. At that time, the different positions in relation to the original and substitutive projects were evident. In December, a new substitute was introduced, which incorporated contributions of that debate, especially a new treatment for network neutrality and storage of data in this country.[6] This version reached the necessary percentage of consensus, and with the approval of the Federal Government, it was quickly approved without any changes in the Senate. Possibly, in order to show the world the Brazilian model of Internet regulation, the President of the Republic enacted the law in the World Net event, on the day following its approval by the Congress.[7]

6. The comparative text between the original project and the version published on 12/11/13 can be found on the websites: <http://i.teletime.com.br/arqs/Outro/75182.pdf> and<http://idgnow.uol.com.br/blog/circuito/2013/12/11/molon-torna-publicas-novas-mudancas-no-texto-do-marco-civil/>. Access on 1/9/2014.

7. The World Net event, hosted in São Paulo in April 2014, arose in part due to the commotion caused by the Snowden case, which led to the speech of President Dilma at the UN calling for a new Internet governance. The principles proposed in the event for this new governance cover, among other issues: human rights; cultural and linguistic diversity; unified and defragmented space; security, stability and resiliency of the Internet; open and distributed architecture; innovation and creativity conducive environment; and open standards. Snowden was a consultant hired by the US Agency NSA information who, in a series of interviews with the British newspaper The Guardian, gave detailed information about the gathering of information on the Internet by the American government. An article published in the newspaper O Globo on 7/6/13 claims that the US spy programs and PRISM FAIRVIEW, supposedly maintained by NSA, monitored millions of e-mails, links and transfer of the Brazilian internet.

4. Controversies

Along the process of approval of the law, a number of ideas caused heated debates. The main groups involved in these discussions can be divided into users (including social movements), connection providers (telecommunications companies that provide broadband), national and international content providers (companies responsible for internet sites), copyright holders (labels, studios and such) and the government (including regulatory, judicial and police authorities). The discussions can be summarized in the following points.[8]

- **Networks Neutrality**

  The substitutes presented by the rapporteur throughout the handling of the matter changed the concept of neutrality. Early versions only allowed interference in traffic to solve technical problems and prioritize emergency services. This almost absolute neutrality, which could give greater transparency to the user, would possibly result in increased costs, because in order to maintain the same speed for all services (e.g. e-mail and video), an improved infrastructure would be necessary. For telecom operators, this concept of neutrality would hinder the network optimization and the generation of new businesses (e.g. prioritization of certain partners). Thus, the absolute neutrality would benefit providers of content of lower economic power (who would not have to pay for a possible additional connection to the providers to ensure their good traffic), services competing to those offered by the connection providers (e.g., Skype or Netflix) and intensive users (heavy users, also known as premium subscribers), which generate a lot of traffic.

  The approved wording softened the concept of neutrality, because it indicated that the degradation in traffic could be made to support the emergency services and to meet "technical requirements necessary for the correct provision of services" This version also evolved by providing that the management of neutrality should be done with proportionality, transparency and equality, first informing the management practices and refraining from the practice of anti-competitive conduct. Thus, the law does not allow ISPs to degrade competitive services by means

8. Additional analysis of conflicts can be found in the study of the Legislative Advisory Available at: <http://www2.camara.leg.br/documentos-e-pesquisa/publicacoes/estnottec/tema4/CP13039.pdf>. Access on 5/28/14.

of their business strategy (for example, telephone operators restrict the traffic of companies offering internet telephony). The relativization of the neutrality concept could enable the offer of differentiated bundles by means, for example, of unlimited access plans to social networks or of certain audiovisual content, or yet, for small screens (which generate lower amounts of data). There are controversies, however, as to which types of bundles could be offered according to the text of the law.[9]

- **Storage of connection logs**

  The acceptance by the users of this provision is mixed. The storage of connection logs is considered beneficial by those concerned with the fight against crime on the Internet, but negative by advocates for individual freedoms and the non-monitoring of users. The measure is considered necessary by the copyright holders and the government, because it facilitates the fight against cybercrime and the punishment of those who illegally share protected content. There are those who defend the storage of connection logs for longer than the time established by the project, which is of one year.

- **The storage of connection logs of the Internet applications (the user browsing)**

  Again, receptivity among users is diffuse. Connection companies want to have the power of storing and analyzing transmissions to manage the network, customize services, obtain commercial information about the user and generate new business opportunities. Social movements agents consider the access to the user's data by the connection operators negative, as it allows the monitoring of users by these companies. For content providers, the storage obligation can be beneficial, as it would allow the negotiation of speed maintenance according to the traffic generated by the application. On the other hand, it could favor the concentration of economic power, as some dot-com companies are much larger than the phone companies, and have more resources to pay for differentiated treatment.

  For the government and for rights holders, it is important that providers store this information, in order to facilitate the work of the judicial and

9. Statements of telecommunications companies claim that offering differentiated bundles by contents would not hurt the principle of neutrality as provided in the text. See, for example: <http://www.telesintese.com.br/para-teles-marco-civil-aprovado-assegura-oferta-de-servicos-diferenciados/>. Acess on 5/27/14.

investigative authorities. The approved version and the original proposal prohibit connection providers to store data about the user's browsing, and thereby hinders the mitigation of cybercrimes, because there will be no authority with the responsibility of storing all of the user's navigation data (only the content providers have this data, but in isolation). This is certainly a solution well received by those who advocate for individual freedoms, although it embeds the premise that the monitoring of content providers is acceptable.

- **Liability for infringing materials**

  Once the connection provider cannot monitor user traffic, according to the original proposal, the substitutes and the sanctioned text, it is natural that the resulting law exempts these agents from civil liability for damages arising by contents posted by a third party. The approved substitute determined the application provider's obligation to remove infringing content (notice and take down) in the event of judicial decisions. Note that the connection provider has no obligation to block access to material that has been considered infringing. Although the law applies to application providers established in the country, the systematization will not have effect to remove or block access to infringing content posted in foreign companies not operating here.

  The approved substitute included explicit reference to copyright and related rights. In law, these issues will continue to be governed by specific legislation, which met the demand of rights holders. For those users who prioritize individual freedom and the end of the absolute monitoring, the best solution would have been no monitoring of the network and the non-identification of transferred bundles, in order to allow complete freedom in communications. However, there are those groups of users and rights holders who believe in the necessity of monitoring and, that copyright infringements are to be audited, monitored and punished. Other agents advocate that the copyright law is too complex to include the Internet and that a specific law would be of a better effect. From the point of view of the lawsuit, since the infringing content can still be accessed in foreign companies without operations in the country, as previously mentioned, the new law hinders the removal of content and compliance of court decisions.

- **Data storage in the country and compliance to the Brazilian legislation**

  This is a theme introduced at the end of the legislative debates on the civil framework, which came up with revelations of the Snowden case. Through the proposal presented in one of the substitute versions, if it were the case to have the participation of Brazilian users and storage of information by application providers established in the country, they shall obey the Brazilian legislation and could be required to store the data here.

  The proposal provided that the Federal Government could issue a decree obliging the connection and content companies to store, in the country, information on Brazilian users. From the perspective of users, the storage of data in domestic territory could result in loss of service quality due to poor infrastructure. On the other hand, this would more easily allow triggering content providers and the Judiciary Branch to request the removal of material that may be deemed offensive. Telecommunications companies, especially telephony operators, would be the main beneficiaries of the measure, as they have greater investment capacity and business affinity with the obligation. The content companies had more to oppose to, because the obligation could imply increased costs, since the supply and competitiveness of the country's data centers are limited. However, for national providers, the rule could prove to be advantageous because the measure could inhibit the performance of global providers in this country.

  Although at first the government considered this measure important, in order to facilitate the application of the Brazilian law in companies operating in this country, it would be of dubious effectiveness in terms of information security. The data could always be duplicated and stored outside the country. Consequently, the "copies" could be accessed by foreign intelligence services. Thus, the Brazilian subsidiary would be complying with the local law and its main office, outside the country, could continue to collaborate with the intelligence services and complying with the legislation of its country of origin, with absolutely no knowledge on the part of its subsidiary.[10] From the perspective of the copyright holders, the storage in the country would also be beneficial, facilitating the compliance with the Brazilian law.

  In the conclusion of the conduct of the project, the proposal was abandoned at the government's request, according to the press, what

10. For more details about the reach of US law, for example, see item 6, where the Calea Act is commented.

was left in the law were only the provisions determining that Internet transactions involving Brazilians or held in Brazil should follow the Brazilian legislation.

In simple terms, the leading positions of each group of interest can be summarized in the table below.

Table 1 – Positions / interests of the main groups involved with the issue of regulation of the Internet.

	Representing users and groups	Connection Companies (Oi, Net, etc.)	National content providers (Globo, UOL, etc.)	Foreign content providers (Google, Facebook, etc.)	Rights holders (record companies, broadcasters and authors)	Government / judicial and police authorities
Absolute neutrality	Yes / No	No	Yes	Yes	Indifferent	No
Connection logs	Yes / No	Yes	Indifferent	Indifferent	Yes	Yes
Connection Logs of applications by connection companies	Yes / No	Yes	No	No	Yes	Indifferent
Connection Logs of applications by content companies	Yes / No	Yes	Yes	Yes	Yes	Yes/ Indifferent
Storage of data in this country	Yes / No	Yes	Yes / No	No	Yes	Yes
Notice and take down	Yes / No	No	Yes	Yes	Yes / No	Indifferent

5. In practice, what has changed with the new law?

To assess what has changed with the entry of the new law into force, it is necessary to understand the main pillars of the project, and how they alter the standards and the relationship among users, and between users and companies in the sector.

1st point – Ensuring freedom of expression, privacy, privacy of users and inviolability of communications

Until the approval of the civil framework, there were great legal uncertainties as to how to adapt the constitutional guarantees to the virtual world. There were doubts, for example, if comments on social networks or blogs could be censored when they were contrary to the internal policy of the companies, if pages could be blocked and if personal privacy could be violated by applications that collect personal information without the consent or knowledge of the user.

The new law clarifies and consolidates the constitutional rights such as the one of inviolability of communications and the right to information, applicable to the virtual world as well. Comments or criticisms cannot be previously censored, albeit not in compliance with the internal policies, and these must be explicit. In addition, access to Internet pages cannot be blocked without a court order, and intimacy and privacy have greater protection because data collection is regulated.

2nd point – Gathering Personal Data

Earlier, there were doubts as to how to pierce into the virtual world the constant prohibition in the Consumer Protection Code, which prevented the transfer of any personal data to third parties without notification or express user authorization. Moreover, there was no guarantee of the removal of such network data, if requested. On the Internet, user habits (such as accessed websites or purchases) and the contents in e-mails or posts could be passed on to other organizations for commercial purposes.

Under the approved law, data can only be gathered with the prior consent of the users and only those who are not excessive in relation to the purpose of the gathering. The users will have to give express consent to the gathering of their browsing habits, though, in some situations, they may not have the option to continue to use the service if they choose not to accept the terms

imposed by the site. Abusive collections (e.g., purchases made collected by news websites) are prohibited.

3rd point – Internet Connection logs

Until the approval of the law, the providers of broadband internet connection could gather the connection and navigation logs for an indefinite period, but there was no obligation. The connection provider could gather not only when and for how long the user was connected (connection record), but also the sites that had been accessed.

In the new law, Internet connection providers must store the connection logs for one year and cannot store the user's browsing records. It should be noted, however, that the law allows the connection provider to continue gathering the connection log of users for an indefinite period.

4th point – User navigation logs

Previously, there was no obligation to store internet navigation logs of users, and applications (sites) were allowed to store them for an indefinite period. Any site or internet application could gather, indefinitely, any type of data about the users' browsing (for this, the installation of cookies on the users' device was sufficient), which could occur without their consent or knowledge.

By means of the new regulation, the internet application providers must store the navigation logs for 6 months, but there is no obstacle preventing them from continuing the storage of the data for an indefinite amount of time. The sites or applications shall inform their users in case they gather and store navigation logs on other sites. However, the data collected may not be excessive or unusual for the purpose of the application. In all cases, users will have to consent explicitly to the gathering and storage of the data. In all cases, users will have to consent explicitly to the gathering and storage of the data.

5th point – Withdrawal of infringing content (notice and take down)

Previously, those in concern requested that the application (site) removed the Internet content they considered infringing, and if the Internet company did not meet the request, they could file a lawsuit for this purpose. Sometimes, the legal representatives of the companies did not answer the lawsuits alleging that they did not hold access to the data stored outside of Brazil.

In addition to the notice and take down, the new law provides that, if the infringing content is of sexual character, the Internet application (site) subsidiarily begins to respond for violation of privacy and may be liable, along with the author of the offense, for crimes such as violation to the honor or disclosure of secret, in case it does not remove the content when directly notified by the victim. Following the example of the previous situation, the new law does not explicitly state that the sites automatically extend the removal and blocking of content when the material is replicated elsewhere on the same site (for example, an infringing video posted by different users on YouTube). Legal representatives of sites or applications have to meet the legal demands under penalty of fine.

6th point – Internet Neutrality

Previously there were no rules that explicitly guaranteed the neutrality or prohibited the differentiated treatment to bundles on the network. Companies could slow down or deteriorate certain types of traffic over others, despite contradicting the competitive and consumer legislation, if the application of these rules to the virtual world were accepted. Furthermore, Internet connection companies could degrade the quality of VoIP services (Skype) or of videos (Netflix) and favor applications with which they held business interests. They could also offer bundles with data allowance (e.g. 10 Gb/month for mobile phones) or gratuity to specific services (e.g., Facebook or Twitter free on prepaid cell phones).

With the new law, Internet traffic can be managed as long as the user is informed of the policies and conditions of the contract. The connection companies and other telecommunications companies shall act with transparency, equality, non-discriminatory conditions and ensure competition. Consumer protection and competition are explicitly strengthened so that companies do not degrade applications and competing services (Skype, Netflix, etc.) in attitudes that affect users. The new law states that the traffic can be broken down (managed) to the adequate provision of services and contracted applications. Deductible plans are still allowed.

6. An international parallel

In the discussion of the civil framework, the arguments that "the world is watching Brazil" and that the Brazilian proposal "did not find a parallel in other countries" were raised a couple of times. In fact, in the US, the regulation of various aspects of the Internet has already been a source of contention for some time. With regard to neutrality, in 2008, the Federal Communications Commission (FCC) commanded that Comcast (broadcasting and Cable Company) should not interfere with the traffic of subscribers.[11] The dispute is still in court. According to the FCC's rules still valid in 2014, operators must comply with three basic rules: 1) be transparent in their management practices; 2) do not block legal content; and 3) do not unreasonably discriminate traffic, including that of competitors.[12]

In February 2014, according to press reports, possibly in response to the announcement of the trade agreement between Comcast and Netflix[13], the FCC was preparing changes to the rules of neutrality. According to the news, the new rules determine that preferential rate agreements for certain content would be allowed provided that they would not undermine competition or restrict the freedom of expression.[14]

In the European Union, there are no specific rules on network neutrality, although a public inquiry on the subject was launched in 2010. In September 2013, the European Commission presented a proposal for revision of the EU Directives, aimed at creating a single market for electronic communications. In the proposal, the net neutrality referred to in article 23 under the suggestive name of "freedom to provide and avail of open Internet access, and reasonable traffic management", would allow the contract for franchises and the sale of packages with different qualities of service. The proposal, which should enter into force in July 2014 and is still under review by the European Parliament, determines that management is

11. In this case, Comcast was slowing down the speed of users who used peer-to-peer applications, often used to download protected content such as movies, etc. See, for example: <http://news.idg.no/cw/art.cfm?id=7F0DF512-17A4-0F78-317789B4C24713C4>. Accessed on 7/1/2014.
12. Final Rule FCC 47 CFR Parts 0 and 8, of 9/23/11, "Preserving the Open Internet". Available at: <http://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf>. Accessed on 11/7/13.
13. Available in: <http://www.nytimes.com/2014/02/24/business/media/comcast-and-netflix-reach-a-streaming-agreement.html?_r=0>. Access on 5/27/14.
14. See for example: <http://www.estadao.com.br/noticias/internacional,fcc-deve-propor-fim-de-neutralidade-na-rede-nos-eua,1158124,0.htm> e <https://www.yahoo.com/tech/fcc-chairman-to-propose-new-net-neutrality-rules-after-85527727044.html>. Access on 5/27/14.

allowed under certain circumstances and, within the contracted limits, it should be transparent, non-discriminatory and proportionate.[15]

Data collection and privacy of Internet users is another issue that has been the concern of many countries. In Europe and the US, the issue of data collection and privacy has been seriously affected by the terrorist attacks of September 11, 2001. Also in 2001, the US launched the *Patriot Act,* which allows spying and gathering of information of any American citizen by the government. Additionally, the law known as *Calea*, of 1994, which requires US telecommunications companies to cooperate with the government, was altered in 2005 to include the cooperation of Internet companies. These laws allow the programs of the American security agencies Prism and Echelon, well known in the press and brought to the surface by the Snowden case, to collect information about any citizen who makes use of equipment, networks, programs or Internet sites maintained by American companies.

Although some European countries have renewed their anti-terror laws, the European Data Protection law protects citizens of the European Community. The law, under review during 2013 and 2014 because of the Snowden problem, guarantees, among other principles, transparency in the use of the collected information and access to the information that companies hold of their users.[16] An emblematical case of this matter was of the Austrian Max Schrems, who after invoking the European law, received from Facebook a dossier with over 1,200 pages about data that the social network had stored about him.

All this discussion about possible regulations for the Internet limiting not only the powers of the companies but also of governments over users, rekindled the debate on the implementation of a new management model for the large network. In this case, the Brazilian movements arising from the conduct of the Civil Framework can be considered influential

15. Proposal for a new regulation and changes in existing policies, of 9/11/13, "Proposal for a Regulation of the European Parliament and of the Council – laying down Measures Concerning the European single market for electronic communications and to Achieve the Connected Continent, and Amending Directives 2002/20/EC, 2002/21/EC and 2002/22/EC and Regulations (EC) No 1211/2009 and (EU) No 531/2012." Available at: <http://www.ipex.eu/IPEXL-WEB/dossier/document.do?code=COM&year=2013&number=627&extension=null>. Accessed on 11/7/13.

16. More information about the review of the policy can be found in "Commission proposes a comprehensive reform of the data protection rules", available at <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>. Accessed on 11/12/13.

in the process. At first, the speech of President Dilma Rousseff at the UN in response to the Snowden case – in which revelations that the US government would have spied on the president's personal e-mail – called for the implementation of a new governance model of the global network. The second point of influence is embodied in the presentation of the Brazilian regulatory model, the Civil Framework, already approved, with government support. These two benchmarks accredited Brazil to host the World Net event, mentioned above, and may have an influence in shaping the new model.

The government's imposition of changes, however, is not so simple. National governments have, in fact, little decision-making power over the Internet, because the Internet was born and is largely unregulated. However, on March 14, 2014, the NTIA – National Telecommunications and Information Administration, an agency of the US Department of Commerce, determined that the ICANN[17] must seek along with international institutions a new governance model for the Internet.[18] The NTIA noted in its statement that the ICANN should look for alternatives in the international community to remove the NTIA agency from the coordination of the Internet's domain system. Some speculate on what are the reasons for this decision: it can be a consequence of the Snowden case, it may be international pressure, and it is also possible to imagine that the conduct of the Civil Framework of the Internet has contributed to this decision on the part of the US government.

7. Final Thoughts

The discussion of Bill 2,126/2011 highlighted the important disagreements existing on the subject of regulation of Internet use between user groups, telecommunications companies, content provider companies, national and international copyright holders and public authorities. Certainly, the Internet is no longer a free and ideal environment where users navigate and participate without the interference and monitoring by companies and governments, as well as it ceased to be a harmless environment. With the

17. CANN (Internet Corporation for Assigned Names and Numbers) is an American private organization responsible for assigning domain names and addresses on the network (called IP addresses). Under the current arrangement, the ICANN determines the amount and which IPs addresses are assigned to certain countries, so that this body is, in practice, the holder of the existing IP address reservations.

18. Available at: <http://www.ntia.doc.gov/print/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>. Access on 4/22/14.

proliferation of innovative services, several practices began to demonstrate conflicts of interest in the dispute over access and control of information circulating on the large network.

Net neutrality notably represented the core of the dispute for the approval of the proposal and there were several points of view that could tip the balance for both sides. Neutrality can be seen as a dispute between those who believe in freedom in the markets and those who advocate that the market needs to be regulated. Not to embrace neutrality could favor economic concentration and increase the barrier of the entrance of new services. On the other hand, in an environment free of competition, the market develops bundles for each type of consumer and price.

Analyzing neutrality under the aspects of finances and infrastructure management, monitoring of internet traffic allows more efficient use of the network: e-mails can take a few milliseconds longer to get to the recipient, and a slow video service is a bad user experience. On the other hand, the adoption of an absolute neutrality would imply that those users that require little traffic (those who use the internet only to check social networks and news and to send e-mails) subsidize the heavy users, which generate a lot of traffic and subscribe to premium services (such as movie channels on the Internet).

In addition, absolute neutrality and an infinite amount of data per month are of little use to those who access the internet from a cell phone's small screen. From the point of view of the price for users, if all bundles were equal, the absolute neutrality would imply that there could be no plans with cheaper rates: all subscribers of a certain speed would have to pay the same amount, regardless of their need, their means of access or financial resources.

The discussions showed that the absolute neutrality had a strong echo among those who believe that communications should be free and open and therefore favor democracy and the right to freedom. In this view, any monitoring and management limits the free flow of information and increases the power of corporations, in addition to reducing competition and innovation.

For operators, the permission to analyze the bundles is a guarantee of isonomy with the content providers and leads to what actually should be the fundamental debate: "Who has the right to pry into personal

communications?" This question approaches the discussion about neutrality to the discussion about data storage.

The controversy on the storage of logs of internet users is another point where commercial, government and users' interests diverge. Today, monitoring is done by connection and content providers and by governments. The connection companies wished to continue to explore this vast "market" of opportunities.

In short, the debate on the *Civil Framework of the Internet* proved to be clearly multifaceted. A point at which this discussion significantly evolved was the introduction of rules to make neutrality flexible. On the good side, transparency, isonomy and purely competitive non-discriminatory services were guaranteed. These issues are fundamental to users: transparency for the users to know what conditions their connection plan targets; what is and what is not included in that price; what personal information is being shared when a given site is accessed, who is entitled to read them, who is entitled to sell them and to whom they are transferred; as well as who is responsible for the services and for the custody of the information.

There is no doubt that the concept and the imposition of rules and limits on the Internet are problematic in several aspects. However, in a highly commercialized environment where all information is monetized and is of some risk to the user, certainly the Internet user can no longer be at the mercy of adhesion contracts that do not guarantee privacy, protection and freedom. In the virtual world, the imposition of limits on companies and governments to ensure the privacy of citizens and the isonomic access to services is a major challenge.

Currently, the Internet is no longer a free, impartial and non-profit environment. On the other hand, citizens also want to participate in major social networks that, ultimately, seek profit. There are also e-mails in companies that are evidently read by them and that use globalized services that can be monitored by governments abroad. The challenge is how to resolve all this in an Internet that is feasible, accessible and fair for everyone.

CLAUDIO NAZARENO
Legislative Consultant
Area XIV – Science and Technology, Computers and Communication

LAW No. 12,965 OF APRIL 23, 2014[19]

(The Brazilian Civil Framework of the Internet)

Establishes principles, guarantees, rights and duties for the use of the Internet in Brazil.

The president of the Republic

Be it known that the National Congress decrees and I sanction the following law:

CHAPTER I
PRELIMINARY PROVISIONS

Article 1. This law establishes principles, guarantees, rights and duties for the use of the Internet in Brazil and determines the guidelines for the action of the Union, the states, the Federal District and the municipalities in this regard.

Article 2. The discipline of Internet use in Brazil is founded on the respect for freedom of expression as well as:
I – the recognition of the global scale of the network;
II – the human rights, the development of personality and the exercise of citizenship in digital media;
III – plurality and diversity;
IV – openness and collaboration;
V – free enterprise, free competition and consumer protection; and
VI – the social purpose of the network.

Article 3. The discipline of Internet use in Brazil has the following principles:
I – guarantee of freedom of expression, communication and expression of thought, under the terms of the Federal Constitution;

19. Published in *Diário Oficial da União* (Brazil's official gazette), Section 1, of April 24, 2014, p. 1.

II – privacy protection;
III – protection of personal data, as provided by law;
IV – preservation and guarantee of network neutrality;
V – preservation of stability, security and functionality of the network, through technical measures consistent with international standards and by encouraging the use of good practices;
VI – accountability of agents according to their activities, in accordance with law;
VII – preservation of the participatory nature of the network;
VIII – freedom of business models promoted on the Internet, provided as they do not conflict with the other principles established in this law.
Sole paragraph. The principles expressed in this law do not exclude others specified in the Brazilian legal system that are related to the field, or in international treaties to which the Federative Republic of Brazil is a party.

Article 4. The discipline of Internet use in Brazil aims to promote:
I – the right of access to the Internet for all;
II – access to information, knowledge and participation in cultural life and in the conduct of public affairs;
III – innovation and promotion of the ample diffusion of new technologies and models of usage and access; and
IV – adherence to open technology standards that enable communication, accessibility and interoperability between applications and databases.

Article 5. For the purposes of this law it is considered:
I – Internet: the system consisting of the set of logical protocols, structured on a global scale for public and unrestricted use, in order to enable data communication between terminals through different networks;
II – terminal: the computer or any device that connects to the Internet;
III – Internet Protocol address (IP address): the code assigned to a terminal of a network to allow its identification, defined according to international standards;
IV – autonomous system administrator: the person or entity that manages specific IP address blocks, and their autonomous system routing, duly registered in the national entity responsible for the registration and distribution of IP addresses geographically related to the country;
V – internet connection: enabling a terminal to send and receive data bundles over the Internet, by the assignment or authentication of an IP address;

VI – connection log: all information regarding the date and time of start and end of an internet connection, the amount of time it was used, and the IP address used by the terminal to send and receive data bundles;
VII – Internet applications: the set of features that can be accessed through a terminal connected to the Internet; and
VIII –access logs of Internet applications: the set of information regarding the date and time of use of a particular Internet application from a particular IP address.

Article 6. In the interpretation of this law it will be taken into account, beyond the fundamentals, the set of principles and goals, the nature of the Internet, its uses and particular customs and its importance to the promotion of human, economic, social and cultural development.

CHAPTER II
RIGHTS AND GUARANTEES OF USERS

Article 7. Internet access is essential for the exercise of citizenship, and the users have the following rights:
I – inviolability of intimacy and privacy, protection and compensation for property or moral damages resulting from its breach;
II – inviolability and secrecy of the flow of communications over the Internet, except by court order, according to the law;
III – inviolability and confidentiality of stored private communications, except by court order;
IV – no suspension of Internet connection, except for debt resulting directly from its use;
V – maintenance of the quality of the contracted Internet connection;
VI – clear and comprehensive information contained in the contracts of provision of services, with details on the protection scheme for connection logs and access logs of Internet applications, as well as network management practices that may affect its quality;
VII – no supply of personal data to third parties, including connection logs, and data of access to Internet applications, except by free, express and informed consent or in the cases provided by law;
VIII – clear and comprehensive information about gathering, use, storage, processing and protection of their personal data, which can only be used for purposes that:

a) justify the gathering;
b) are not prohibited by law; and
c) are specified in the contracts of provision of services or in terms of internet applications;

IX – Express consent to the collection, use, storage and processing of personal data, which should be highlighted in the contract terms;
X – definitive exclusion of personal data that have been provided to the particular Internet application, on request of the user, at the end of the relationship between the parties, except in the cases of mandatory log keeping provided for in this law;
XI – publicity and clarity of eventual user policies from Internet connection and Internet applications providers;
XII – accessibility, considering the physical-motor, perceptual, sensory, intellectual and mental characteristics of the user, under the law; and
XIII – application of protective standards and consumer protection in consumer relations carried out on the Internet.

Article 8. The guarantee of the right to privacy and freedom of expression in communications is a prerequisite for the full exercise of the right of access to the Internet.
Sole paragraph. The contract terms that violate the provisions of the heading are automatically void, such as those that:
I – Involve harm to the inviolability and secrecy of private communications over the Internet; or
II – in the adhesion agreement, do not offer as an alternative to the contractor, the adoption of the Brazilian forum for settlement of disputes relating to services provided in Brazil.

CHAPTER III
PROVISION OF CONNECTION AND INTERNET APPLICATIONS

Section I
Network Neutrality

Article 9. Those in charge of the transmission, switching and routing are required to deal in an isonomic way with any data bundles without distinction between content, origin and destination, service, terminal or application.
§ 1. The discrimination or degradation of traffic will be regulated under the exclusive competence of the President of the Republic provided for in

item IV of article 84 of the Federal Constitution, for the faithful execution of this law, after hearing the Internet Steering Committee and the National Telecommunications Agency, and can only result from:
I – technical requirements necessary for the correct delivery of services and applications; and
II – prioritization of emergency services.
§ 2. In the event of discrimination or degradation of traffic described in § 1, the person mentioned in the heading shall:
I – refrain from causing harm to users, according to article 927 of Law 10,406, of January 10th, 2002 (Civil Code);
II – act with proportionality, transparency and isonomy;
III – previously inform in a transparent, clear and sufficiently descriptive manner to its users about the management and traffic mitigation practices adopted, including those related to network security; and
IV – offer services on non-discriminatory commercial conditions and refrain from practicing anti-competitive conduct.
§ 3. In the Internet connection provision, costly or free, as well as in the transmission, switching and routing, it is prohibited to block, monitor, filter or analyze the content of the data bundles, subject to the provisions of this article.

Section II
Protection of Logs, Personal Data and Private Communications

Article 10. The storage and the availability of connection and access logs to Internet applications mentioned in this law, as well as personal data and the content of private communications, must take into account the preservation of intimacy, privacy, honor and image of the parties directly or indirectly involved.
§ 1. The provider responsible for the storage shall only be obliged to release the logs mentioned in the heading, autonomously or associated with personal data or other information that may contribute to the identification of the user or terminal, by court order, as provided in Section IV of this chapter, subject to the provisions of article 7.
§ 2. The contents of private communications shall only be made available by court order, in the cases and in the manner provided by law, subject to the provisions of sections II and III of article 7.

§ 3. The provision of the heading does not prevent access to registration data that inform personal qualification, affiliation and address, as provided by law, by the administrative authorities holding legal power for this request.
§ 4. The measures and the security and confidentiality procedures shall be informed by the party responsible for the provision of services in a clear way and meet the standards set by regulation, respecting the right to confidentiality regarding trade secrets.

Article 11. In any operation of gathering, storage, custody and treatment of records, personal data or communications by connection and internet application providers in which at least one of these acts occurs in national territory, the Brazilian law and the rights to privacy, protection of personal data and the confidentiality of private communications and records must be mandatorily respected.
§ 1. The provision of the heading applies to data collected in the national territory and the contents of communications, provided that at least one of the terminals is located in Brazil.
§ 2. The provision of heading applies even if the activities are carried out by a legal entity located abroad, provided that it offers services to the Brazilian public or at least one member of the same group has an establishment in Brazil.
§ 3. The connection and Internet application providers shall give, according to regulation, information allowing the verification as to compliance with Brazilian legislation relating to the gathering, the retaining, storage or processing of data, as well as regarding privacy and confidentiality of communications.
§ 4. A decree shall regulate the procedure for investigating violations to the provisions of this article.

Article 12. Without prejudice to other civil, criminal or administrative penalties, violations of the standards set forth in articles 10 and 11 are subject, as appropriate, to the following sanctions, applied in isolation or cumulatively:
I – warning, with indication of the deadline for a corrective action to be taken;
II – fine of up to 10% (ten percent) of the revenues of the economic group in Brazil in its last financial year, excluding taxes, considering the economic condition of the offender and the principle of proportionality between the seriousness of the misconduct and the intensity of the penalty;
III – temporary suspension of activities involving the acts referred to in article 11; or

IV – prohibition from carrying out activities involving the acts referred to in article 11.
Sole paragraph. In the case of a foreign company, its subsidiary, branch, office or establishment in the country will be jointly and severally liable to pay the fine referred to in the heading.

Subsection I
Keeping Connection Logs

Article 13. In the provision of Internet connection, it is the duty of the respective autonomous system administrator to maintain the connection logs, under secrecy, in a controlled and secure environment, for a period of one year, according to regulation.
§ 1. The responsibility for the maintenance of the connection logs cannot be transferred to third parties.
§ 2. The police or administrative authority or the Prosecutor's office may request, as precautionary measure, that the connection logs be stored for a period longer than required in the heading.
§ 3. In the event of § 2, the applicant authority shall have a period of sixty days from the request to file the request for judicial authorization for access to logs described in the heading.
§ 4. The provider responsible for keeping the logs shall maintain confidentiality with regard to the request referred to in § 2, which will lose its effectiveness if the judicial authorization request is refused or has not been filed within the period specified in § 3.
§ 5. In any case, the availability to the applicant of the logs referred to in this article shall be preceded by judicial authorization, as provided for in Section IV of this chapter.
§ 6. In the application of penalties for non-compliance to the provisions of this article, it shall be taken into consideration the nature and seriousness of the offense, the damages resulting from it, the possible advantage gained by the offender, aggravating circumstances, the records of the offender and recidivism.

Subsection II
Keeping Connection Logs of Internet Applications in the Provision of Connection

Article 14. In the provision of connection, costly or free, it is forbidden to keep access logs of Internet applications.

Subsection III
Keeping Connection Logs of Internet Applications in the Provision of Applications

Article 15. The internet applications provider established as a legal entity and which performs this activity in an organized, professional manner and for economic purposes, shall keep the access logs of Internet applications under secrecy, in a controlled and secure environment for a period of six months, under the terms of the regulation.
§ 1. Court order may require, for a certain amount of time, that Internet application providers which are not subject to the provisions of the heading store connection logs of Internet applications, provided that such records are related to specific facts in a given period.
§ 2. The police or administrative authority or the Prosecutor's office may request any provider of Internet applications, as a precautionary measure, that access logs of Internet applications be stored, including for longer than described in the heading, subject to the provisions of §§ 3 and 4 of article 13.
§ 3. In any case, the availability to the applicant of the logs referred to in this article shall be preceded by judicial authorization, as determined in Section IV of this chapter.
§ 4. In the application of penalties for non-compliance to the provisions of this article, it shall be taken into consideration the nature and seriousness of the offense, damages resulting from it, possible advantage gained by the offender, aggravating circumstances, the record of the offender and recidivism.

Article 16. In the provision of Internet applications, costly or free, it is forbidden to keep:
I – access logs to other Internet applications, without the previous consent of the owner of the data, subject to the provisions of article 7; or
II – personal data that are excessive in relation to the purpose for which the owner gave their permission.

Article 17. Except for the situations laid down by this law, the option not to keep the access logs to Internet applications does not imply responsibility for damages resulting from the use of these services by third parties.

Section III
Responsibility for Damages Arising from Content Generated by Third Parties

Article 18. The provider of Internet connection shall not be civilly liable for damages arising from content generated by third parties.

Article 19. In order to ensure freedom of expression and prevent censorship, providers of Internet applications can only be civilly liable for damages resulting from content generated by third parties if, after specific court order, they do not make arrangements to, in the scope and technical limits of their service and within the indicated time, make unavailable the content identified as infringing, otherwise subject to the applicable legal provisions.

§ 1. The court order referred to in the heading shall have, under penalty of nullity, clear and specific identification of the content identified as infringing, that enables the unequivocal location of the material.

§ 2. The application of this article to violations of copyright or related rights depends on specific legal provisions, respecting freedom of expression and other guarantees described in article 5 of the Federal Constitution.

§ 3. Lawsuits that deal with compensation for damages arising from content made available on the Internet, related to honor, reputation or personality, as well as the unavailability of such content by Internet application providers, may be brought before special courts.

§ 4. The judge, including in the procedure described in § 3, may anticipate, in whole or in part, the effects of the intended protection in the initial application, as long as there is unequivocal evidence of the fact and considering the interest of the collectivity in the availability of the content on the Internet, and as long as the requirements of verisimilitude are present in the author's claim and there is a fear of damage that is irreparable or difficult to repair.

Article 20. If the provider of Internet application has the information of contact of the user directly responsible for the content referred to in article 19, it will be the responsibility of the provider to communicate to the user the reasons and information related to the unavailability of the content, with information allowing the adversarial and full defense in court, unless there is express legal provision or express judicial determination based on the contrary.

Sole paragraph. When requested by the user who provided the content that became unavailable, the Internet applications provider carrying out this activity in an organized and professional manner, and for economic purposes,

shall replace the content made unavailable with the motivation or the court order that gave grounds to the unavailability.

Article 21. Providers of Internet applications who make available the content generated by third parties shall be held subsidiarily responsible for the breach of privacy resulting from the disclosure, without the participants' permission of images, videos or other materials containing nudity or sexual acts of private character when, upon receipt of notification by the participant or their legal representative, fails to diligently promote, within the technical limits of their service, the unavailability of that content.
Sole paragraph. The notification mentioned in the heading shall include, under penalty of nullity, elements allowing for the specific identification of the material appointed as violator of the participant's intimacy and verification of the legitimacy for the presentation of the request.

Section IV
Judicial Request for Records

Article 22. The interested party may, with the purpose of having evidence in civil or criminal proceedings, in incidental or autonomous character, ask the judge to order the party responsible for keeping the data to provide connection logs or access logs of Internet applications.
Sole paragraph. Without prejudice to other legal requirements, the application shall contain, under penalty of inadmissibility:
I – founded evidence of the illicit occurrence;
II – motivated justification of the usefulness of logs requested for research or conclusive statement; and
III – the period to which the records are related.

Article 23. It is the responsibility of the judge to take the measures necessary to ensure the confidentiality of information received and the preservation of intimacy, private life, honor and image of the user, being allowed to determine secrecy of justice, even for requests of keeping connection logs.

CHAPTER IV
THE ROLE OF PUBLIC POWER

Article 24. Following are directives for the actions of the Union, the states, the Federal District and municipalities in the development of the Internet in Brazil:

I – establishment of multi-stakeholder, transparent, collaborative and democratic governance mechanisms, with the participation of the government, the business sector, civil society and the academic community;
II – promotion of the rationalization of management, expansion and use of the Internet, with the participation of the Internet Steering Committee in Brazil;
III – promotion of the rationalization and technological interoperability of electronic government services among the different public powers and levels of the federation, to allow the exchange of information and the celerity of procedures;
IV – promotion of interoperability between systems and different terminals, including between the different federal levels and various sectors of society;
V – preferential adoption of open and free technologies, standards and formats;
VI – publicity and dissemination of data and public information in an open and structured manner;
VII – network infrastructure optimization and stimulus to the implementation of storage, management and data dissemination centers in the country, promoting the technical quality, innovation and the diffusion of Internet applications, without prejudice to openness, neutrality and participatory nature;
VIII – development of actions and capacity-building programs for use of the Internet;
IX – promotion of culture and citizenship; and
X – provision of public services for citizen care in an integrated, efficient, simplified manner and through multiple access channels, including remote.

Article 25. The internet applications of public power entities shall seek:
I – compatibility of electronic government services with various terminals, operating systems and applications for access;
II – accessibility to all interested parties, regardless of their physical-motor, perceptual, sensory, intellectual, mental, cultural and social capacities, safeguarding the aspects of confidentiality and administrative and legal restrictions;
III – compatibility with both human reading and the automatic processing of information;
IV – ease of use of electronic government services; and
V – strengthening social participation in public policies.

Article 26. The compliance with the constitutional duty of the govermment in the provision of education at all levels of teaching includes capacity building,

integrated with other educational practices for the safe, conscious and responsible use of the Internet as a tool for the exercise of citizenship, the promotion of culture and technological development.

Article 27. The public initiatives promoting digital culture and the Internet as a social tool shall:
I – promote digital inclusion;
II – seek to reduce inequalities, especially among different regions of the country, in the access to information and communication technologies and their use; and
III – promote the production and circulation of national content.

Article 28. The State shall periodically formulate and promote studies, as well as set goals, strategies, plans and schedules, relating to the use and development of the Internet in the country.

CHAPTER V
FINAL PROVISIONS

Article 29. The user shall have the option of free choice in the use of computer program on their terminal for the exercise of parental control of content understood by them as unfit for their underage children, provided the principles of this law are respected, as well as Law no. 8,069 of July 13, 1990 (Statute of the Child and the Adolescent).
Sole paragraph. It is the public power's responsibility, along with the Internet connection and application providers and civil society, to promote education and provide information on the use of computer programs referred to in the heading, as well as to define best practices for digital inclusion of children and adolescents.

Article 30. The defense of the interests and rights set forth in this law may be exercised either individually or collectively, according to the law.

Article 31. Until the coming into effect of specific law predicted in § 2 of article 19, the liability of the provider of Internet applications for damages arising from content generated by third parties, in case of infringement of copyright or related rights, shall continue to be disciplined by the current copyright legislation applicable on the date this law comes into effect.

Article 32. This law shall come into effect sixty days after its official publication.

Brasilia, April 23, 2014; 193rd of the Independence and 126th of the Republic.

DILMA ROUSSEFF
José Eduardo Cardozo
Miriam Belchior
Paulo Bernardo Silva
Clélio Campolina Diniz

edições câmara

CÂMARA DOS DEPUTADOS