What is at stake in the Regulation of the **Marco Civil da Internet**?

Final Report on the Public Debate Sponsored by Ministry of Justice on Regulation of Law 12.965/2014

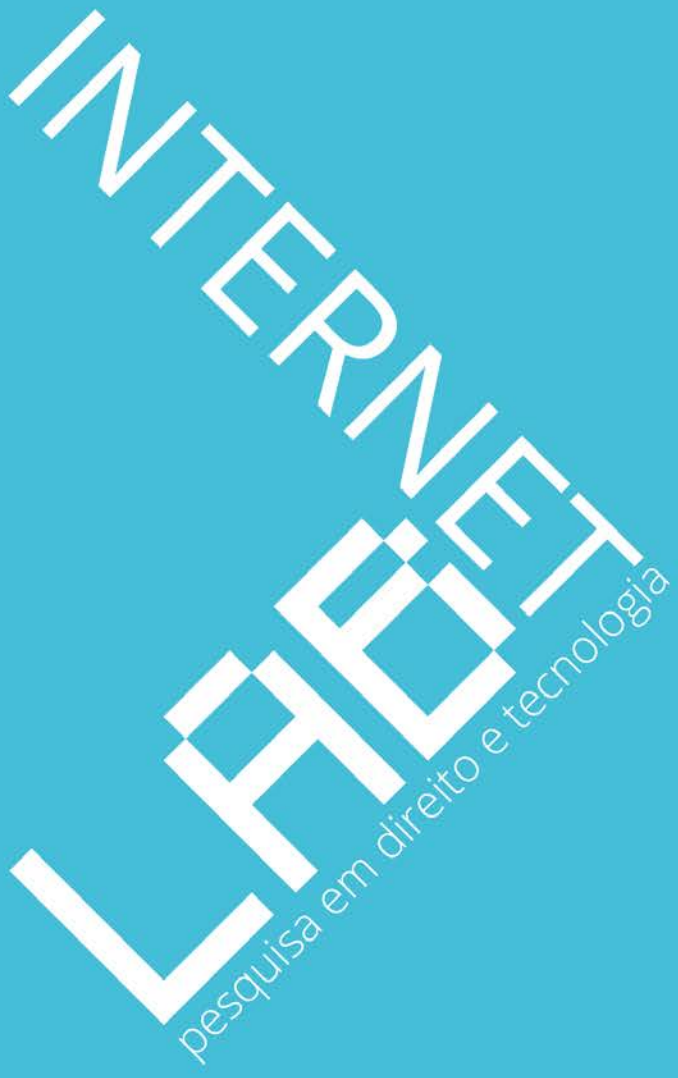
Authors

Francisco Carvalho de Brito Cruz
Jonas Coelho Marchezan
Maike Wile dos Santos

Collaborators

Dennys Marcelo Antonialli
Jacqueline de Souza Abreu
Mariana Giorgetti Valente
Pedro Henrique S. Ramos

www.internetlab.org.br



WHAT IS AT STAKE IN THE REGULATION OF THE **MARCO CIVIL DA INTERNET**?

FINAL REPORT ON THE PUBLIC DEBATE SPONSORED BY MINISTRY OF JUSTICE ON REGULATION OF LAW 12.965/2014

***

INSTITUTIONAL TEAM **Executive Director** Dennys Antonialli **Acting Director** Francisco Brito Cruz **Research Coordinator** Mariana Giorgetti Valente / PROJECT TEAM **Project Leader** Francisco Brito Cruz **Research Intern** Jonas Coelho Marchezan **Research Intern** Maike Wile dos Santos

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA, 2015.

INTERNETLAB / Rua Augusta, 2690, Galeria Ouro Fino, Loja 326 / www.internetlab.org.br

WHAT IS AT STAKE IN THE REGULATION OF THE **MARCO CIVIL DA INTERNET?**

FINAL REPORT ON THE PUBLIC DEBATE SPONSORED BY MINISTRY OF JUSTICE ON REGULATION OF LAW 12.965/2014

/Summary

TEAM MEMBERS INVOLVED IN THIS PROJECT

AUTHORS

FRANCISCO CARVALHO DE BRITO CRUZ / Master in Philosophy and Jurisprudence by the School of Law of *Universidade de São Paulo* (FDUSP). Graduated in Law by School of Law of *Universidade de São Paulo* (FDUSP) and, in the course of that program, received a scholarship from *Programa de Educação Tutorial* (PET) –Sociology of Law. Visiting Researcher (2013) at the Center for Study of Law and Society of the University of California – Berkeley, through Rede de Pesquisa Empírica em Direito (REED) exchange program. Mr. Brito Cruz received the *Marco Civil da Internet e Desenvolvimento* Award of the School of Law of *Fundação Getúlio Vargas* (SP). Attorney-at-law, practices in areas such as CyberLaw, Intellectual Property, Consummer Law and Press. He was founder and coordinator of FDUSP Group of Law, Internet and Society (NDIS) between 2012 and 2014 and is currently a director of InternetLab.

JONAS COELHO MARCHEZAN /Presently attending Law School at Universidade de São Paulo (FDUSP). Volunteer at the Corporate Team of the Legal Department with NGO "*Un Techo para Mi Pais* – Teto Brasil".

MAIKE WILE DOS SANTOS / Presently attending Law School at Universidade de São Paulo (FDUSP). He participated of *Escola de Formação na Sociedade Brasileira de Direito Público* – SBDP (2014). Mr. Santos received a scholarship from and was a monitor at Programa de *Estímulo ao Ensino de Graduação – PEEG* for topic Legal Doctrines directed to Economists at FEA (2013); he also received a scholarship from and was a monitor at Programa *Ensinar com Pesquisa no Núcleo de Direito, Internet e Sociedade* – NDIS (2014), both associated to USP. Mr. Santos is currently a member of *Centro de Análise e Pesquisa em Educação Jurídica* – CAPEJur, associated to the FDUSP Department of Philosophy and Jurisprudence, as well as research intern with InternetLab.

COLLABORATORS

DENNYS MARCELO ANTONIALLI / Presently taking his PhD in Constitutional Law by *Universidade de São Paulo*, having graduated in Law by that same University (2008), Mater in Law by the University of Stanford (JSM, 2011) and Master in Business in "Law and Business", jointly sponsored by Bucerius Law School and by WHU *Otto Beisheim* School of Management (MLB, 2010). Mr. Antonialli acted with the team engaged in public policies involved in technology and civil rights in the American Civil Liberties Union of Northern California (ACLU/NC) and as legal consultant of the "Timor Leste Legal Education Project", of the Stanford Law School/Asia Foundation. Mr. Antonialli was awarded the Steven M. Block Civil Liberties Award of the Stanford Law School (2011) and the *Marco Civil da Internet e Desenvolvimento* Award of the School of Law of Fundação Getúlio Vargas (SP). Researcher of Alexander von Humboldt Institute for Internet and Society (Berlin), participated in the Summer Doctoral Program do Oxford Internet Institute. Attorney-at-law, he is currently coordinator of FDUSP Group of Law, Internet and Society (NDIS) and director of InternetLab.

JACQUELINE DE SOUZA ABREU / Presently taking her Masters in Law at the *Ludwig-Maximilians-Universität* in Munick (LMU). Graduated in Law by the School of Law of *Universidade de São Paulo* (2014). During her graduation, Ms. Abreu received a scholarship in scientific initiation from *Fundação de Amparo à Pesquisa do Estado de São Paulo* (FAPESP) and *Programa de Estímulo ao Ensino de Graduação* (PEEG) in the areas of Philosophy and Jurisprudence, and is a member of FDUSP's Group of Law, Internet and Society. Ms. Abreu participated of academic exchange with LMU, at which time she received a scholarship from the German Service of Academic Research (DAAD). She was also junior-researcher with FGV DIREITO SP.

MARIANA GIORGETTI VALENTE / Master, and presently taking her PhD in Legal Sociology at USP. Researcher in project Digital Collections with FGV's *Centro de Tecnologia e Sociedade*, where she also coordinated the Open Business Models on copyright and music in the digital age (2012-2014). Under FGV, she was also a legal coordinator of project Creative Commons *Brasil*. Ms. Valente is a member *of Núcleo Direito e Democracia do Centro Brasileiro de Análise e Planejamento* (Cebrap), where she coauthored research for program *Pensando o Direito* (SAL/MJ). Graduated in Law by *Universidade de São Paulo* in 2009, specialized in intellectual property by the World Intellectual Property Organization (WIPO) (Summer School, 2011). Ms. Valente was legal coordinator of *Museu de Arte Moderna de São Paulo* and coordinates Copyright Groups at *GT Arquivos de Museus e Pesquisa* (Capes). Coordinates FDUSP's group of Law, Internet and Society (NDIS). With InternetLab, she is coordinating researcher and project leader for gender and technology.

PEDRO HENRIQUE S. RAMOS / Master of Laws at FGV/SP. Law degree from University of São Paulo, with post-grad courses from University of Southern California and the International Center of Social Sciences of São Paulo. Former visiting researcher at the Center of Internet and Society at Stanford Law School, under supervision of prof. Barbara van Schewick, working together with the Architecture & Public Policy team on researches focused on net neutrality in developing countries. Pedro was also a speaker at the Telecommunication Policy Research Conference (TPRC) in 2014, where he presented his work on zero-rating and its impact on developing economies.

1. INTRODUCTION

1.1. Public debate on Regulation of the *Marco Civil da Internet*[1]

The public inquiry conducted on the regulation of federal law n. 12.965/14 (internationally known as the **Brazil's Internet Bill of Rights**) was conceived within the project *Pensando o Direito [Thinking of Law]* developed by Office of Legislative Affairs of the Ministry of Justice (SAL/MJ). The project was created in 2007 and intended at stimulating society's participation in developing laws and regulations in Brazil, as means to have more effective laws, more engaged with reality and with communities' demands.

Participation in public debate platform, which began on January 28, 2015, was split into four topic quadrants which, in turn, referred to matters of great significance for discussion of the law: "**Net neutrality**", "**Internet privacy**" (restrictions to collection of personal data and ways to enforce such restrictions), "**Retention of access logs**" (definitions on how tracks of Internet users may be stored and delivered to investigating authorities or third parties) and "**Other matters and considerations**" (such as the State' position in development of Internet policies or technological innovation). Within each such quadrant, user was freely able to create topics with suggestions and recommendations for debate.

As the debate ended on April 30, Ministry of Justice extended a new term for **systematization of findings** of the inquiry. Participants were invited to propose solutions for systematization of contributions and even to submit drafts of the decree, as subsidiary for wording of the official text.

1.2. InternetLab's position: information and academic diversity

Aware of the Academia's role in public policies' debate, InternetLab developed, during the inquiry, project ***InternetLab Reporta: Consultas Públicas*** [InternetLab Reports: Public Consultation].

While inquiry was ongoing, we published, each Friday, a weekly news bulletin with the main contributions or discussions on the platform. We sought to unravel complex matters that came up during proceedings and consulted specialized researchers. **The purpose was to enhance visibility to such an important opportunity for determination of the future of Brazilian Internet**, by fostering participation and enabling contribution by third parties interest in the discussion and disclosing of quality information on the main issues debated on the platform in a concise and organized manner.

This report reflects our follow-up and final findings, organizes recommendations and designs a scenario with the most relevant arguments.

[1] The *Marco Civil da Internet*, also known as the "Brazil's Internet Bill of Rights", "Brazilian Civil Rights Framework for the Internet" or the "Internet Constitution" was approved in Brazil in April 2014 after more than 5 years of intense national and international debate and a series of postponed votes in the Brazilian Congress.

2. OVERVIEW OF THE PUBLIC DEBATE: PARTICIPATION NUMBERS AND PROFILE

The platform had a total of **1843** registered participants and **1200** comments, divided into **339** topics created by users. The most accessed quadrant was "**Other matters and considerations**" with 124 topics, followed by "**Net neutrality**", with 98 topics; "**Retention of access logs"**, with 70 topics; and "**Internet privacy**", with 68 topics.

A large portion of participants chose to contribute in the days that preceded closing of the deadline. There was actually a large number of contributions (total number of participants doubled) in the final days of March since, at first, online debate was scheduled to end on March 31. As deadline was extended to April 30, a last-minute peak was once again verified: comments jumped from 780 to 1131. Please refer to the enclosed charts prepared by InternetLab showing some of these figures.

3. METHODOLOGY: HOW DID WE ORGANIZE HUNDREDS OF OPINIONS AND ARGUMENTS?

We have reviewed all contributions to public inquiry on regulation of the Brazil's Internet Bill of Rights submitted to the Ministry of Justice over platform "Pensando o Direito" in the course of the inquiry, which took place between January 28 and April 30, 2015.

The inquiry platform organized contributions in four subject quadrants: (i) **Net neutrality**; (ii) **Internet privacy**; (iii) **Retention of access logs;** and (iv) **Other matters and considerations**. Choice of topics was free, meaning that citizens were free to navigate among quadrants and recommend any debate and make suggestions as they saw fit.

3.1. How was the review carried out?

Of all contributions, selection for review fell **only on those that pertained to some matter addressed by federal law n. 12.965/14 and were not intended to change anything in the law**. In other words, **our assessment excluded contributions not strictly referring to a matter addressed by the law or seeking to amend it through the decree**.

Starting from such cut-off, we have attempted to identify, in each contribution, the theories and arguments advocated, as well as to link them to the agents involved in the platform. Such first triage enabled us to devise two large categories for organization of contributions:

- **Controversial issues**: such category refers to contributions that were brought to the debates and faced with conflicting positions. It is important to point out that, most times, confrontation was not within a same topic of discussion but rather across several topics.
- **Individual recommendations**: such category refers to those contributions that were not confronted on the platform. It should be noted that not all individual recommendations reviewed are reflected here and some have been summarized for the purposes of this report.

3.2. Comments by InternetLab's team

This report also includes comments by InterneLab's team that seeks to deepen discussions initiated on the platform.

3.3. What to expect from this report?

This report seeks to **describe the public consultation process by mapping the debate issues, main arguments raised and agents engaged**, such that, upon completion of this review, **we submit recommendations that may be viewed as the most relevant**. As a result, we expect to provide subsidies to development of a decree for regulation of the *Brazil's Internet Bill of Rights* and information on the outcome of public inquiry to all those interested in the matter.

3.4. Content usage license

All content published on the platform of Ministry of Justice is subject to license *Creative Commons* – Attribution 4.0 International (CC BY 4.0), as set forth in the platform *Terms of Use*. This report per se is licensed under a *Creative Commons* CC BY 3.0 BR license. Such license allows others to remix, adapt and create derivative work on the original work, including for commercial purposes as long as appropriate credit is granted to its author.

4. ARGUMENTS AND POSITIONS

4.1. Net neutrality

4.1.1. How should the specific regulation address the offering of mobile data plans with free access to specific applications (*zero-rating*)?

The expression *zero-rating* has been used to refer to a practice adopted by mobile network operators under which these operators exempt data charges from certain applications or specific services. It allows customer to use a given application even if its contracted data cap has been reached. Such strategy has been somewhat trendy for a number of years in developing countries. Since 2014, *zero-rating* strategies have also spread all over Europe and in the US. In Brazil, *zero-rating* strategies are adopted since at least 2009, and have become increasingly common in the last few years due to commercial offers that provides free data charges for popular applications such as *Facebook*, *Twitter*, *Waze and WhatsApp*.

Our study has identified that *zero-rating* was the most discussed topic on the public consultation platform. Although each and every contribution has its specificities, we have been able to categorize them into three major trends:

Controversial positions on the subject:
(A) The evaluation of wheter *zero-rating* practices are legal or not (under Marco Civil general rule) should be made in a case-by-case and *ex post* approach. Thus, *zero-rating* practices should not be *ex ante* prevented by the specific regulation.
(B) *Zero-rating* practices *per se* are an exception to net neutrality. Therefore, such practices should not be prohibited under the specific regulation.
(C) *Zero-rating* represents a violation to net neutrality and to the general rule set forth by Marco Civil. Therefore, it should be expressly banned by the specific regulation.

Summary of the positions and its supporters:

(A) *The evaluation of wheter* zero-rating *practices are legal or not (under Marco Civil general rule) should be made in acase-by-case and ex post approach. Thus, zero-rating practices should not be ex ante prevented by the specific regulation..*

This position is based on the argument that the obligation to refrain from discriminating data packets, as provided for in article 9 of *Marco Civil,* comprehends only activities related to the traffic of data packets (the "logical layer", as provided by the simplified ISO model) and, therefore, does not comprehends discrimination among data packets that may take place on a commercial level (the "content

layer"), as long as the practice is in compliance with other rules provided for in the regulation such as consumer protection guarantees and antitrust safeguards.

Besides, advocates of this position argue that it is not possible to assess that *zero-rating* strategies will have a negative impact on competition *per se*. In fact, advocates argue that the flourish of alternative princing schemes will not only benefit consumers but also foster competition **(Tim Brasil).** From a consumer perspective, arguments on such position also point to the fact that *zero-rating* strategies may enable wider access to the internet, mostly among the poor. Hence, *zero-rating* would allow less privileged communities to have access to services related to education, health, communications and basic information. Supporters of this position also stress that the protection of consumers and of the principles of *Marco Civil* greatly rely on the assurance of transparency of information, and these guidelines should be the foremost compass to assess the legality of mobile data plans contained in plants and the ability to determine whether plans are being fulfilled. **(CISCO Brasil)**

Who stands for that? *FEBRATEL, SINDITEBRASIL, SINDISAT, TELCOMP, TELEBRASIL, ABRAFIX, ACEL, ABINEE, Tim Brasil, Cisco Brasil, Brasscom.*

(B) Zero-rating *practices* per se *are an exception to net neutrality. Therefore, such practices should not be prohibited under the specific regulation.*

Some have argued that, although *zero-rating* practices might infringe the principle of net neutrality, those practices should be treated as a reasonable exception due to its beneficial social and economic effects. Moreover, one of the key principles of *Marco Civil* is competition; therefore, the application of the rule should balance these key principles in favor of *zero-rating* practices.

Who stands for that? *Claro S/A.*

(C) Zero-rating *represents a violation to net neutrality and to the general rule set forth by Marco Civil. Therefore, it should be expresslybanned by the specific regulation.*

Supporters of this position understand the legal rationale behind article 9 of *Marco Civil* with a different approach. they understand that *Marco Civil* assigns to ISPs the obligation of treating all data packets equally, not discriminating or charging differentially by user, content, site, platform, application, or mode of communication. According to this broad understanding of the rule, *zero-rating* practices would violate an *ex ante* obligation already addressed by *Marco Civil*'s general rule.

From a a social and economic perspective, supporters of this position ground their arguments in studies and researches that point *zero-rating* strategies as adverse to competition, as these strategies might create access barriers on the application level. Other adverse consequences have also been indicated. From a user perspective, this position argues that, by limiting the number of platforms through which users may communicate and exchange information, *zero-rating* strategies may facilitate surveillance and censorship, as well as empower the replication of the inequality gap between full access

to the Internet by those who can afford to pay the "unilimited experience" and those who have only limited access to some applications.

Who stands for that? *COGPC/SEAE/MF, AccessNow, Artur, Sergio Deliconi, ABSTARTUPS, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores, ABRINT and CTS-FGV.*

4.1.2. Which executive bureau should enforce net neutrality rules?

Another subject widely discussed on the public consultation refers to the enforcement and oversight of net neutrality rules. In Brazil, specific regulations enacted by the Presidency commonly address how the Executive bureau and its agencies will deal with the enforcement of a given statute, so as to establish procedures for the enforcement and rules for applying sanctions. In this sense, three different positions have been identified:

Controversial positions on the subject:
(A) The National Telecommunications Agency (ANATEL) should be in charge of overseeing and enforcing net neutrality
(B) ANATEL should be in charge of oversight and enforcement, with the testimony of CGI.br
(C) A multistakeholder monitoring and oversight model, composed by ANATEL, CADE, SENACOM and CGI.br

Summary of the positions and its supporters:

(A) *The National Telecommunications Agency (ANATEL) should be in charge of overseeing and enforcing net neutrality.*

Supporters of this argument argue that Internet is a value-added service, pursuant to the General Communications Act] ("LGT"). As a result, according to article 61 of LGT, ANATEL has jurisdiction to oversee the interaction between value-added services and telecommunications services and, therefore, ANATEL should be in charge of overseeing and enforcing net neutrality rules.

Who stands for that? *FEBRATEL, SINDITEBRASIL, SINDISAT, TELCOMP, TELEBRASIL, ABRAFIX, ACEL, ABINEE, CLARO S/A, ABDTIC, Netflix Brasil, Cisco Brasil.*

(B) *ANATEL should be in charge of oversight and enforcement, with the testimony of CGI.br*

This argument acknowledges that ANATEL's jurisdiction to oversee net neutrality has already a solid legal foundation in Brazil (article 19 of LGT), and that the regulatory agency has institutional mechanisms already in place to facilitate oversight and enforcement of *Marco Civil*. However, scholar **Pedro Ramos** proposed that, ameans a way to reduce adverse selection and moral hazard effects i and improve institutional legitimacy, the specific regulation should provide a mandatory "*amicus curiae*" procedure involving CGI.br. As pointed out by the scholar, CGI.br should be solicited to give his opinion on cases involving net neutrality, as many of the particularities of traffic discrimination could be better addressed with the opinion of the steering committee.

Who stands for that? *Pedro Ramos (InternetLab researcher).*

(C) *A multistakeholder monitoring and oversight model, composed by ANATEL, CADE, SENACOM and CGI.br.*

A group of several civil society assocations advocated for a multi-institutional model for the oversight and enforcement of net neutrality. According to these entities, such task will only be accomplished if undertaken as an articulated work of more than one administrative bureau. These multi-institutional model would encompass the following entities: Anatel, *Conselho Administrativo de Defesa Econômica* [Administrative Council for Economic Defense, Brazilain Antitrust Authority] (CADE), *Secretaria Nacional do Consumidor* [Office for Consumer's Defense at the Ministry of Justice] (Senacom) and *Comitê Gestor da Internet no Brasil/ Núcleo de Informação and Coordenação do Ponto BR* [Brazilian Internet Steering Committee] (CGI.br/NIC.br).

Who stands for that? *Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores, CTS-FGV, Cristiana Gonzalez.*

4.1.3. How should the specific regulation address exceptions to the net neutrality rule provided for in the *Marco Civil*?

This topic is directly related with the technical requirements that are necessary to the provision of Internet-access services and would, directly or indirectly, create some sort of discrimination between different datapackets. Some recommendations sent through the public consultation platform sought to determine how such exceptions shoulb be better clarified by the specif regulation.

Controversial positions on the subject:
(A) The decree should contain an exhaustive list of the permitted network management practices.
(B) The decree should contain general rules that would help regulators and courts to determine wheter such network managemet practice is or is not in compliance with the general net neutrality rule.
(C) The decree should not contain an exhaustive list of the permitted network management practices, as the regulation in place already limits ISPs ability to use network management practices.
(D) The decree should expressly address the agnostic status of the internet

Summary of the positions and its supporters:

(A) *The decree should contain an exhaustive list of the permitted network management practices.*

Only a very thorough and complete list of the permitted network management practices would be able to preserve the goals set forth by *Marco Civil*. Supporters of this argument advocate that the establishment of an exhaustive list also contributes to a better institutional control over possible abuses and arbitrary practices by ISPs.

Who stands for that? *Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores, ANER, IASP, ABRANET and ANJ.*

(B) *The decree should contain general rules that would help regulators and courts to determine wheter such network managemet practice is or does not comply with the general net neutrality rule.*

Due to the always-changing nature of Internet, an exhaustive list of permitted network management practices would become quickly obsolete. Therefore, it would not be advisable to prevent new techniques of traffic management from being implemented, as thisoption would ultimately block innovation.

With that in mind, some have argued that the decree should, whether by using principles or standards, focus on defining the difference between a reasonable network management practice and practices that would represent a breach of net neutrality. As a result, ISPs would be able to define the best practices to be used for traffic management in each situation.

In turn, the decree should establish strict and clear protection mechanisms and a regulatory authority with jurisdiction to enforce existing safeguards already in place since the enactecment of *Marco Civil* (argument brought by **Cisco Brasil**).

Who stands for that? *TIM Brasil, Telcomp, FEBRATEL, SINDITEBRASIL, SINDISAT, TELCOMP, TELEBRASIL, ABRAFIX, ACEL, ABINEE, ILCO (*Instituto Liberal do Centro Oeste)*, Cisco Brasil, Sky Brasil.*

***(C)** The decree should not contain an exhaustive list of the permitted network management practices, as the regulation in place already limits ISP`s ability to use networj management practices*.

Some limitations to traffic management are already in place under the rule set forth by *Marco Civil*: "(a) traffic *management shall not cause damages to users, as per article 927 of the Brazilian Civil Code*; (b) *while managing its network, ISPs must act with proportional, transparent and isonomic standards*; (c) traffic management practices *must be disclosed to users in a transparent, clear and exhaustive way, and*; (d) *ISPs must offer its services in non-discriminatory commercial conditions, as well as refrain from engaging in antitrust practices*" (*free translation from the official text)*.

Supporters of this perspective stress that specific regulation enacted by the Executive branch should be intended to detail the set forth by the general statute, as to give clear guidance of what is and what is not a reasonable network management. Thus, it should also avoid restrictions that might lead to the discourage network management techniques, as long as its practices are used for strictly technical concerns rather than commercial motivations.

Who stands for that? *ABDTIC and CTS-FGV (although CTS recommended greater restrictions).*

***(D)** The decree should expressly address the agnostic status of the internet*

Scholar Ademir Antonio Pereira Júnior proposed that the internet should be application-agnostic, thus impeding any kind of discrimination among different applications and classes of application. In the opinion of Pereira Júnior, ISPs should adopt agnostic network management practices, suggesting that the specific regulation should expressly ban "*any kind of discrimination among applications or classes of applications or traffic deterioration. In this sense, practices that involve contracting prioritized traffic for an specific application or class of application or that involve favoring applications from the same economic group should be banned*". Practices that are not agnostic could be authorized, provided that these practices are treated as exceptions only admitted so as to solve security and congestion issues, subject to the limites set forth in Marco Civil.

Who stands for that? *Ademir Antonio Pereira Júnior.*

4.1.4. Should the decree authorize ISPs to exam and monitor data packets headers?

INTERNETLAB comment – Author: Pedro Ramos (associate researcher)

The technical specifications that based the first packet switching networks generally did not provided guarantees that data is delivered or that a user is given a guaranteed quality of service level or a certain priority. Such standard became known as *best efforts delivery*: data packets delivery followed a "*best efforts*" standard and, in case of network congestion, packets were placed on hold following a *first come, first served* criteria.

However, *best-efforts* was never regarded as an absolute paradigm for the Internet. The basic structure of TCP/IP protocol establishes that data packets transmitted through the web are individually packaged and identified by a prefix (*IP header*), containing the necessary information for ISPs to identify where that packet came from, where it is to be delivered and how it should be treated on their networks.

Among the information included in the IP header, there is a field called *traffic class* that performs two basic functions: (i) it signals the existence of network congestion, by means of a *Explicit Congestion Notification* (ECN), thus allowing network operators to identify an overload and reorganize data packets so as to reduce latency and *jitter*; and (ii) it allows the use of a function named *Differentiate Services* (DiffServ), which permits the classification of the type of data contained in a given package, giving higher or lower traffic priority to packets transmitting data that might be more sensitive to latency. Both functions were discussed and incorporated to technical standards used by the Internet following years of debate and consolidation under the the *Internet Engineering Task Force*.

Such structural model of the TCP/IP protocol, together with many traffic management hardware and software currently used by ISPs, seeks to address answers to a crucial issue for Quality of Service: not all data packets are equal, and some packets are more sensitive to latency than others (videos are more sensitive than e-mails, for instance). In turn, the boundary between a lawful traffic-prioritization practice and a content-discrimination practice is not always easy to assess and might be used as a loophole by ISPs to discriminate traffic that might not be aligned with its corporate interests.

Controversial positions on the subject:

(A) Packet monitoring prohibitions set forth in §3 ofarticle 9 should not be applied to metadata contained in IP headers.

(B) According to article 9, § 3, Internet Service Providers (ISPs) are prevented from monitoring even IP headers.

Summary of the positions and its supporters:

(A) *Packet monitoring prohibitions set forth in §3 ofarticle 9 should not be applied to metadata contained in IP headers.*

Supporters of this position (all of them representatives of ISPs) argue that monitoring IP headers is crucial because it is what enables network management.

Who stands for that? *FEBRATEL, SINDITEBRASIL, SINDISAT, TELCOMP, TELEBRASIL, ABRAFIX, ACEL and ABINEE.*

***(B)** According to article 9, § 3, Internet Service Providers (ISPs) are prevented from monitoring even IP headers.*

According to the supporters of this argument, such express ban would prevent ISPs from discrimination any kind of data that might not be beneficial to its corporate goals.

Who stands for that? *Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega and PROTESTE – Associação de Consumidores.*

4.1.5. Do Content Delivery Networks (CDNs) violate the net neutrality rule set forth by *Marco Civil*?

CDNs are large distributed system of servers deployed in multiple data centers across different places, aimed to serve content to end-users with high availability and high performance, since it reduces the distance between hosts and end-user devices.

Few contributions addressed concerns over CDNs. Contributions followed two lines of arguments: one privileges economic consequences of using CDNs while the other focus on its relevance to Internet's information flow.

Controversial positions on the subject:
(A) CDNs do not breach net neutrality.
(B) Depending on the circumstances, CDNs may be a bypass to a net neutrality standard. The use of CDNs should be regulated..

Summary of the positions and its supporters:

***(A)** CDNs do not breach neutrality.*

As argued by some experts, CDNs are only an efficent way to allocate network content by bringing content geographically closer to the users. It is, therefore, an arrangement that involves the content layer, and it does not allows *per se* traffic discrimination.

It should also be noted that the use of CDNs is beneficial to all those who are involved in the transmission of data packets over the Internet. Users and application providers benefit from faster content delivery while ISPs benefits from less network traffic congestion. Finally, advocates of this position state that costs of CDNs services are not significant enough to be deemed as a access barrier to small applicationsproviders.

Who stands for that? *Pedro Ramos, Roberto Taufick and Claro S/A*.

(B) *Depending on the circumstances, CDNs may be a bypass to a net neutrality standard. The use of CDNs should be regulated.*

As argued by CTS-FGV, it is not clear whether article 9 of *Marco Civil* prohibits or not the use of CDNs. It is true that CDNs provide relief to traffic congestion and, therefore, need of traffic management (which might lead to possible abuse), and might benefit small application providers, thus assuring faster access to its content.However, as stated by CTS-FGV, CDNs discriminate data packets, which may become problematic particularly when such CDN is owned by a content or an application provider.

Who stands for that? *CTS-FGV.*

4.1.6. Do private networks violate net neutrality?

Private networks such as intranets operate under structures that are separated from the so-called "public Internet" that we access and use on a daily basis. Such kind of private network is deployed to meet specific needs of each customer, usually corporate customers. The issue regarding the relationship between private networks and net neutrality arises since traffic discrimination on the public internet may arise as a result of the deployment of such private networks by ISPs.

Controversial positions on the subject:
(A) Private networks do not violate net neutrality *per se* and, therefore, the non discrimination obligation set forth by Marco Civil should not apply to private networks.
(B) It is necessary to include in the specific regulation a precise definition of what is a "private IP network". Without such definition, there is a potential risk of encouraging net neutrality violations.

Summary of the positions and its supporters:

(A) *Private networks do not violate net neutrality per se and, therefore, the non-discrimination obligation set forth by Marco Civil should not apply to private networks.*

According to the supporters of this position, private networks are different and separated from the public Internet, as it operates through private IPs, dedicated infrastructure and serves to meet specific needs of its customers.

In this sense, if private network operators are released from non-discrimination obligations, that would not affect the goals set forth by net neutrality, especially the open Internet and the protection to the different requirements of companies' models that currently use the Internet.

It should also be noted that corporate clients have greater influence on the negotiation of their internet provision services before ISPs. As a result, companies would be capable of ordering special services that would better meet their needs.

Who stands for that? *Telecommunications Industry Association.*

(B) *It is necessary to include in the specific regulation a precise definition of what is a "private IP network". Without such definition, there is a potential risk of encouraging net neutrality violations.*

Private networks are not within the scope of net neutrality regulation since this kind of infraestructure are private and separated from the public internet

However, it is necessary to have a precise definition of what is and what is not considered a private IP network. That would prevent attempts to defraud net neutrality rules based on the argument that certain actions took place on a "private network" rather than on the public Internet.

For instance, one of the supporters of such argument, **Barão de Itararé**, shows the relevance of precise definition of private IP network:

> *"a private company that uses VoIP for its internal communication is entitled to establish priority for this kind of protocol on its internal web. However, this is totally different when this company is compelled to contract differentiated services from an ISP so as to offer such priorization.*
> *In other words, an ISP cannot offer a differentiated service under a private contract, assuming that such contract would guarantee a different level os service to certain classes of applications".* [free translation]

Who stands for that? *Laura Tresca and Barão de Itararé*.

4.1.7. Should the specific regulation allow the blockage of data packet so as to protect copyright claims?

Should the decree expressly include an exception to net neutrality allowing ISPs to block data packets originated from servers that host unlawful content (for instance, copyright violations)? It is true that copyright is not directly addressed by *Marco Civil*. However, the public consultation platform hosted a discussion assessing the relationship between copyright protection and net neutrality.

Such debate focused on the possibility of blocking (which entails discriminatory treatment to data packets) content sponsored by websites that host unlawful content in general and, more specifically, a content that infringes copyright.

INTERNETLAB comment – Author: Mariana Giorgetti Valente (research coordinator)

In the course of the discussions of the *Marco Civil da Internet* in the House of Representatives, it was determined that third-party content removal due to violation of copyright is a more complex discussion, and should not be addressed by *Marco Civil*. The reason argued by players involved was that *Marco Civil* embodies a wide range of different interests, and keeping copyright as a topic would prevent the approval of the statute, since there was no political consensus on this matter. As a result, Brazil still lacks a clear legal specification with respect to procedures to be followed by copyright owners, as well as what are the liabilities of the application provider that hosts infringing content. Notwithstanding this position, article 18 of *Marco Civil* established that ISPs will not be held liable for damages arising from content hosted by application providers, which includes copyright claims.

Establishing a provision allowing blocking of data packets originated from servers that host illegal content, as an exception to the general net neutrality rule established in article 9, involves three issues. The first one lies in the realm of legal interpretation and refers to the exceptions to net neutrality set forth in article 9, which does not include blocking of data packets from specific servers. Moreover, the aforementioned safeguard granted to ISPs seems to indicate a legal rationale based on the assumption that the liability fro coyright violations should not be focused on such players.

The second issue is political by its own nature: establishing a system to pursue copyright-infringing content mean getting ahead of the discussions that should be organized in a democratic manner so as to balance with other fundamental rights. Advocates of blocking argue that this would be a minor issue if compared to the fact that there would be no other manner to remove certain content, given the difficulty to securily remove content hosted in other countries. That is a matter of legal venue and, in fact, it affects all sorts of content (and not only content that is protected by copyright). Neither few nor simple are the international discussions involving this issue.

The third one relates to long existing disputes created around the protection of business models based on the exploitation of copyright versus the technological innovation and other lawful interests. Blocking of packets on a logical layer level could not assess whether there are not other fundamental rights at stake, such as the ban on censorship. Brazil is quite a case in this sense. For instance, a court ordered the full blocking of *YouTube* in 2007. Another example was the decision to block *WhatsApp* in the entire country in 2015, which was turned down before being enforced. In turn, identification of specific content stemming from certain sites gives rise to great concern referring to monitoring and freedom of expression.

Controversial positions on the subject:

(A) Regulation should expressly include the possibility of blocking data packets originated from certain sources (servers) that host unlawful content.

(B) There should not be a net neutrality exception allowing ISPs to block unlawful content.

Summary of responses and their advocates:

(A) *Regulation should expressly include the possibility of blocking data packages packets originates originated from certain sources (servers) that host unlawful content.*

Such argument states that the possibility of blocking by means of a court order should be viewed as an assumption of the regular provision of services and applications, as referred to in article 9, *§* 1, subsection I, which deals with net neutrality exceptions.

A court order served on an ISP for blocking of packages is often the only way courts have to dispense actual relief and protection of several rights. Without such remedy, decisions might be ineffective or, in case of Rogatory Letters, might become effective only in the long run.

Who stands for that? *MPAA, Fórum Nacional Contra a Pirataria e Ilegalidade and ABPI.*

(B) *There should not be a net neutrality exception allowing ISPs to block unlawful content.*

Existence of unlawful content in a given website does not entail blocking of the whole content by ISPs. Users' right to use the site for lawful purposes should be preserved and presumption of innocence should prevail.

Who stands for that? *Ivella.*

4.1.8. How should regulation address the exception to the net neutrality rule for "emergency services"?

Note by authors*: due to disparity of recommendations on this subject, contributions were organized as "recommendations" rather than as scattered answers. The difference here is that regulatory option of one recommendation does not prevent other recommendations from being selected as well.*

Individual recommendations for regulation of the matter:
(A) Paid prioritization for should not be construed as emergency service. The exception to the net neutrality rule for the sake of "emergency services" should only take place in case of excessive network traffic, without regard to payment. **Author of recommendation:** *CTS-FGV.*
(B) Regulation should define the meaning of "emergency services" and, if possible, provide an exhaustive list of the entities entitled to quality as such. **Author of recommendation:** *CEPI and OAB/RS*

(C) Services deemed as "emergency" might be determined pursuant to law n. 7.783/1989, which addresses services deemed "essential" and Resolution of ANATEL n. 614, of May 28, 2013, which regulates procedures for multimedia communications services.

Author of recommendation: *Procon/SP*

(D) "Emergency services" should be defined as: public emergency services (Police, Fire Fighters, First Respondent Medical Services and Hospitals) and services and applications used to send official messages in cases of public calamity or natural disasters.

Author of recommendation: Cristiana Gonzalez

4.2. Retention of access logs

4.2.1. How should regulation address retention and access, by authorities, to access logs[2] referred to in articles 13 and 15 of the *Marco Civil da Internet*?

INTERNETLAB comment – Author: Jacqueline de Souza Abreu (researcher)

Obligations to preemptively retain metadata generated using telecommunications means, as a general rule, have grounds on the argument that such obligations are critical to avoid "loopholes" preventing (i) user's liability for offenses committed using such telecommunications means, or (ii) use of such data to assist prevention and punishment of other offenses, and dispute resolution. In case of obligations to retain Internet connection and access to application logs, per articles 13 and 15 of the Brazil's Internet Bill of Rights, the goal would be to ensure the validity of Internet user's liability for offenses committed through the web and the availability of such data for investigative or evidentiary purposes, even in the event of criminal and civil cases off the web.

Such predictions, however, give rise to controversies. Within the scope of the political agenda, concerns revolve around the growth of State's surveillance over citizens. Within the legal framework, questions are raised about the constitutionality of such measures. This is because review of metadata such as connection logs under article 13 and, in particular, application access logs under article 15, is able to offer portraits of user's personality, habits, interests, social contacts and location that are directly related to such user's privacy and affect secrecy of communications. In addition to that, the fact that retention records takes place preemptively, with no relation to an immediate threat or individualized suspicion, would not be in compliance with the principle of presumption of innocence.

Within the legal framework, some argue the fundamental inconsistency of metadata preemptive retention obligations with basic rights, others attempt a way out through the proportionality principle, specially by limiting possibilities and requirements to access logs safekept, by way of restricting access solely for purposes of prosecuting serious criminal offenses at the existence of concrete evidence of authorship and participation, as well as creating safety rules to retain data and transparency rules regarding data usage.

When, in April 2014, the Court of Justice of the European Union invalidated the European Directive determining mandatory retention of data generated using telecommunications services to prevent and punish crimes (Data Retention Directive) under the argument that restrictions to basic rights imposed by the Directive were disproportionate, repercussions in Brazil were immediate and are reflected in the debate over the regulation of the Marco Civil da Internet. It is worthwhile mentioning that at the same time that several local laws issued by European countries which complied with the terms of the Directive were also declared no longer effective because of their "disproportionatily" (as more recently occurred in Holland), new bills of law are already being created in an attempt to "proportionally" regulate metadata retention obligations (as currently in Germany). This is an issued yet to be solved even there.

Controversial positions on the subject:

(A) The decree should limit possibilities of access.

[2] The *Marco Civil da Internet* establishes a difference between applications access logs (art. 15) and connection logs (art. 13). In this report all logs will be referred to as "*access logs*".

(B) The decree should expand collection of access logs.
(C) The decree should not regulate this topic.

Summary of the positions and its supporters:

(A) *The decree should limit possibilities of access.*

Contributions arguing in favor of limiting possibilities of obtaining to access logs safekept pursuant to the terms of articles 13 e 15 of the *Marco Civil* take into account that records retention is, in fact, unconstitutional.

There is a reference, among others, to an example of the European Union according to which the Council of Europe's Commissioner for Human Rights - CEDH stated that "mass retention of communications data, without cause, is fundamentally contrary to the rule of law, inconsistent with basic data protection principles and ineffective" (**CTS-FGV**).

The solution to limit access varied among participants. **CTS-FGV** argued for the adoption of International Principles on the Application of Human Rights to Communications Surveillance.[3] Other group of participants argued that similar to breach of telephone secrecy, access to access logs shall only be made available by court order issued within the course of a criminal investigation or discovery within the scope of a criminal proceeding, pursuant to the terms of article 5, XII, of the Constitution, and articles 1 and 3 of Law 9.296/96, thus, outside the scope of jurisdictional orders issued by non criminal courts.

Who stands for that? *CTS-FGV, Câmara Brasileira de Comércio Eletrônico, ABEMID, ANER, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores.*

(B) *The decree should expand collection of access logs.*

Due to exhaustion of "version 4" public IP numbers (IPv4) and consequent sharing of such IP numbers by several users concurrently, it is not possible to segregate and locate potential offenders with only an IP number, date and time of access.

In view of the above, a request is made to also retain data relative to the logic port used. This measure shall enable segregation of suspects while the new IP version (IPv6) is not implemented. In addition to the logic port, **OAB/SC** also defends creation of retention obligations applicable to *MAC*

[3] See: https://pt.necessaryandproportionate.org/text

(*media access control*) address, a number created by routers on domestic or professional networks that would allow accurate identification of the device connected to the activity under investigation.

Furthermore, with regard to article 13, the **Federal Attorneys' Office (MPF)** argues for retention of connection logs relative to any user, with no room for exceptions, not even to individuals providing free Internet access within their private premises. This proposal represents an expansion of the scope of the Brazil's Internet Bill of Rights to the extent it only forces administrators of autonomous systems[4] to retain connection logs and not any company, individual or organization offering some kind of Internet access. The **MPF** does not make reference to such classification in its contribution.

Who stands for that? *TIM Brasil, MPF and OAB/SC.*

(C) *The decree should not regulate this topic*

With regard to article 15, also taking into account the assumption of unconstitutionality of mass records retention and in line with the European understanding, an alternative to remedy the unconstitutionality of the law would be not to regulate it. Therefore, it would remain a rule of limited effectiveness, pursuant to the recent understanding of the State of São Paulo Court of Appeals[5], thus not generating effects. **ITS-Rio** also provided an alternative to regulate the topic, in case a decision is made that the decree shall approach the matter of data retention (see below the topic "*Limits for retention of and access to records on connection and access to Internet applications*").

Who stands for that? *ITS-Rio.*

4.2.2. Which application providers should be required to retain access logs (regulation of article 15 of the *Marco Civil*)?

Public debate brought-up controversy over which applications providers shall be forced to retain access logs of their users. The core of the debate is the definition of the applications that may be excluded from the retention rule.

---

[4] According to the *Request For Comments* (RFC) 1930 of the IETF (Internet Engineering Task Force), international technical entity that monitors the Internet from start and proposes technologies and protocols standards, "autonomous system" corresponds to a "*set of routing prefixes connected by Internet Protocol (IP) under the control of one or more network operators presenting a common and clearly defined routing policy to the Internet*". In Brazil, the *Núcleo de Informação e Coordenação do Ponto BR* of the Brazilian Internet Steering Committee (NIC.br), operational branch of the *Comitê Gestor da Internet*, is responsible for creating the rules on how connection providers may enroll "autonomous systems", thus taking part of the distribution of blocks of IP numbers performed by NIC.br. Per NIC.br, the entities shall have, by way of example, "a minimum network infrastructure" and "2 or more independent Internet connections or a connection with one operator and one connection to a traffic exchange point", in addition to a series of technical standards and a compatible team. Sources: <http://registro.br/tecnologia/provedor-acesso.html?secao=numeracao> e <ftp://ftp.registro.br/pub/gter/gter28/07-Asbr.pdf >.

[5] Opinion of the appellate decision under Interlocutory Appeal nº 2168213-47.2014.8.26.0000, author of the first opinion, Justice Rômolo Russo (10/03/2015).

Controversial positions on the subject:
(A) Retention shall only be mandatory for applications hosting content created by users.
(B) Retention shall only be mandatory for application providers that profit through treating personal data.

Summary of the positions and its supporters:

(A) *Retention shall only be mandatory for applications hosting content created by users*

It is suggested that decree should establish that the retention shall only be mandatory for applications hosting content created by users. Such suggestion takes into account the intent of the obligation to store records: the identification of those liable for infringement of third parties rights.

When content created by users is not hosted there is no possibility of infringement of rights by users, thus rendering access logs retention unnecessary. In line with the above, **ITS-Rio** established:

> *"It is important to emphasize that even with regard to financial services such obligation would not be deemed proper under the argument of investigation of money laundering and other financial crimes, as there is already a Law ruling on the subject matter, which determines that these companies shall have to provide information relative to "suspicious" financial transactions to COAF, rendering unnecessary and redundant to retain access records".*

Who stands for that? *ITS-Rio, ABRANET, CNseg.*

(B) *Retention shall only be mandatory for application providers that profit through treating personal data.*

The profile of the obligation to retain may be defined by requirements, such as revenue cap, scope of activities and, finally, need to login (or not), that is the moment in which existence of an enrolled user performing actions is characterized.

Who stands for that? *Cristiana Gonzalez, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega and PROTESTE – Associação de Consumidores.*

4.2.3. Which additional rules should the decree establish on retention of access logs?

***Note by authors**: due to disparity of recommendations on this subject, contributions were organized as "recommendations" rather than as scattered answers. The difference here is that regulatory option of one recommendation does not prevent other recommendations from being selected as well.*

Individual recommendations for regulation of the matter:
(A) The decree should establish an express exception regarding retention access logs regarding activities related to the so-called "Internet of Things". Such exception should take place for three reasons: (i) volume of this kind of record is huge, which would give rise to high and disproportionate costs, (ii) there are implications to citizens privacy; and (iii) most part of such data would be excessive for purposes of law enforcement activities. **Author of recommendation:** *ITS-Rio.*
(B) Regulation should clarify initial and end date for access logs retention period as a matter of legal security. **Authors of recommendation:** *IASP, ABPI, José Antônio Milagre, ANER, ABRANET and Fundação Procon – SP.*
(C) The decree should establish the criteria according to which requests for access to information by authorities shall be justified (motive, period to which the access logs refer to, reasonable evidence of wrongdoing, among others). **Authors of recommendation:** *FIESP, GEPI – FGV, ABRANET, Câmara Brasileira de Comércio Eletrônico.*
(D) Regulation should address standards to provide and have access to access logs and other kind of data (article 10, head). According to participant **Laura Tresca**, such standards should take into account the definition of article 5 for the elements encompassed by access logs. **Authors of recommendation:** *FIESP, José Antônio Milagre, ANER, ABRANET and Laura Tresca.*
(E) The decree shall establish a rule determining that upon expiration of the periods of time prescribed by law, access logs shall be deleted from records held by connection provider and Internet application providers. There may be exceptions for access to applications logs in case their deletion is detrimental to the service provided. The idea is to render mandatory retention less harmful to users' privacy, thus prohibiting indiscriminate retention of users' access logs. **Authors of recommendation:** *ITS-Rio, Veridiana Alimonti, Joana Varon, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores.*

4.2.4. How should the decree address the possibility of determination of preemptive retention of data for "longer period"?

The Brazil's Internet Bill of Rights establishes that administrative or law enforcement authorities may request retention of access logs for a period longer than the one prescribed for application providers (6 months) and connection providers (1 year).

This possibility, however, is not fully detailed in the letter of the law and, for this reason, gave rise to several discussions in the platform.

What are the requirements legitimizing access logs retention for longer periods?

Individual recommendations for regulation of the matter:
(A) Authorities having appropriate jurisdictionshall specify "reasonable evidence of wrongdoing" (article 22, I, of the *Marco Civil*) and provide substantiated justification to use the access logs requested for investigation or discovery purposes (article 22, III) **Authors of recommendation:** *CTS-FGV, IASP, ABRANET, ITS-RJ, ANER.*
(B) The decree shall state which administrative and law enforcement authorities have appropriate jurisdiction are to request preemptive retention. **Authors of recommendation:** *Sky Brasil, ITT, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega and PROTESTE – Associação de Consumidores.*

How long shall last the "longer period" referred to in articles 13, § 2, and 15, § 2?

Individual recommendations for regulation of the matter:
(A) The authority shall not have more than 60 days to file a request for a Court order to access data subject to been deemed an unjustified and unknown burden. **Authors of recommendation:** *IASP, GEPI – FGV, Barão de Itararê, Laura Tresca, Veridiana Alimonti, Cristiana Gonzalez, ABRANET, Ana Cristina Azevedo, Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital*

– IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores.
(B) In addition to the 60-day period to request a Court order, the decree shall also establish a subsequent term (additional 60 days recommended) during which the provider shall have to remain retention data. Upon expiration of the additional term the provider may cease preemptive retention of data. **Author of recommendation:** *Brasscom.*
(C) Preemptive retention shall last no longer than 1 additional year to connection providers and 6 additional months to application access providers. **Author of recommendation:** *Sky Brasil.*
(D) Because it is more beneficial to the consumer, it is suggested that the maximum renewal period shall not exceed 3 years, per article 206, paragraph 3, V, of the Brazilian Civil Code and adopted by the STJ (*Agravo Regimental* under AREsp 614778 , Justice Rapporteur Marco Aurélio Bellizze). **Author of recommendation:** *Fundação Procon – SP.*
(E) The ideal term, in case of a crime, should be the statute of limitation prescribed for the act under investigation. For civil cases, the term should be that of forfeiture applicable to the cause of action. **Author of recommendation:** *Emerson Wendt*

What additional rules decree shall create regarding requests for precautionary retention of data for a period longer than that established by the* Marco Civil*?

Individual recommendations for regulation of the matter:
(A) The decree should create mechanisms to challenge preemptive requests from providers. **Authors of recommendation:** *Sky Brasil.*
(B) The decree shall limit a maximum term for preemptive retention of access logs in case of silence on the part of the Courts. It is recommended a period of 180 days counted as of the request for preemptive retention by an administrative or law enforcement authority or the Public Attorneys Office. **Authors of recommendation:** *SINDITELEBRASIL and CLARO.*

(C) The decree shall establish a maximum term for preemptive retention to be complied with by the judge upon acceptance of a request for preemptive retention filed by an administrative or law enforcement authority, or the Public Attorneys Office.

Authors of recommendation: *SINDITELEBRASIL, CLARO and Procon –SP.*

(D) User shall be informed of a request for additional preemptive retention relative to its activities.

Authors of recommendation: *Veridiana Alimonti, Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega and Proteste - Associação de Consumidores*

4.3. How should the decree address the issue of account information and the possibility of having them subpoenaed by the authorities?

In addition to the proposals mentioned above, many participants emphasized the importance of a better definition for personal data forms, despite the definition already prescribed by the law: "account information regarding personal qualification, name of parents and address".

4.3.1. Which authorities have jurisdiction to subpoena personal data forms?

Individual recommendation for regulation of the matter:

(A) The decree shall be consistent with the opinion of 17-B of Law n. 9.613/1998 (Money Laundering Act) and of Law n 12850/13 (Criminal Organizations Act).

Authors of recommendation: *Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações, Câmara Brasileira de Comércio Eletrônico, CTS-FGV, SindiTeleBrasil, ANER, ABRANET, Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega and Proteste - Associação de Consumidores.*

4.3.2. Which additional rules should be created on account information?

Individual recommendations for regulation of the matter:

(A) The decree shall establish a mandatory obligation to inform users that their data was accessed for any other purpose than those they agreed to - even for investigation purposes (exception cases shall also be determined and exceptional requests shall be justified).

Authors of recommendation: *Cristiana Gonzalez, Francisco Brito Cruz, Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, Proteste - Associação de Consumidores.*

(B) To comply with the warranties set forth under the head of article 10, regulation shall be clear that such account information shall only be accessed upon submission of an user name or other information relative to the user account applicable to the Internet service at issue. In turn, paragraph 3, may allow any authority holding an IP to request to a connection provider ("administrator of an autonomous system"), responsible for the administration of the IP number in question, information about the user registration without a proper Court order.

Author of recommendation: *Francisco Brito Cruz*

4.4. Need of an independent authority for personal data protection

***Note by authors**: due to disparity of recommendations on this subject, contributions were organized as "recommendations" rather than as scattered answers. The difference here is that regulatory option of one recommendation does not prevent other recommendations from being selected as well.* ***Despite the fact that two proposals mentioned below converge with regard to the creation of a body, we chose to separate them and highlight the nuances of each one**.*

Individual recommendations for regulation of the matter:

(A) It is necessary the creation of an independent guarantor authority with powers to enforce the provisions on privacy and personal data established by the Brazil's Internet Bill of Rights, as follows:

> *"As the* Marco Civil *establishes principles and obligations regarding rights to privacy and personal data - in particular with regard to mandatory retention of logs relative to connection and access to applications -, the creation of a guarantor authority in the form mentioned above and with the required resources and technical capacity may be justifiable to define safety and privacy standards to be complied with while collecting and storaging such access logs, following studies and consultation to the applicable industry sectors. An independent guarantor authority shall also be responsible for periodic reviews of applicable standards and rules to ensure that they are updated and fit for their purposes. Especially, it shall deliver statistics on conservation of data generated or processed within the scope of an Internet access offering or access to Internet applications offering.*
>
> *Statistics shall not contain personal data and shall include: (i) cases in which information was provided to the authority having appropriate jurisdiction; (ii) period of time elapsed between the date data was conserved and date in which authorities having appropriate jurisdictionrequested such data to be transmitted; and e (iii) cases in which data requests were not satisfied".*

Author of recommendation: *CTS-FGV.*

(B) To implement the provisions of articles 7, 8, 10, 13, 14, 15 and 16 of the Brazil's Internet Bill of Rights, an authority to protect personal data shall have to be created.

It shall not be taken lightly that consumer protection bodies and the public attorneys office shall have an important role, but in view of good practices, in particular those of European countries known for their high standards of privacy protection, another type of authority shall be required to enforce such legal provisions. Among its attributions would figure to ensure that such data is safely kept; that consent is given clearly, freely and expressly or even to establish procedures to provide "information allowing examination of compliance with Brazilian laws applicable to collection, retention, storage or treatment of data", so that there may be effective compliance with laws and guarantee that such procedures are not being used in an abusive way against users, with occasional sharing of data for commercial purposes or infringement of privacy rights by the State.

In line with the above, a discussion of the bill of rights regulation parallel to the debate regarding the Data Protection Draft Bill would be welcome, as the latter shall review the best structure for this type of data protection authority, which existence should be mentioned, even if broadly, by the Brazil's Internet Bill of Rights regulation.

Authors of recommendation: *Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores.*

4.5. Determination of Security Standards

4.5.1. How should data security standards be determined?

Controversial positions on the subject:
(A) Regulation is not the proper place to define security parameters.
(B) Regulation shall only define minimum security standards.
(C) Regulation shall be technology neutral and shall not require disclosure of the adopted security standards.

Summary of the positions and its supporters:

(A) *Regulation is not the proper place to define security parameters***.**

For those supporting this argument, the parameters defined by the decree may become obsolete. If the parameters are defined by decree, they should at least establish how such provisions shall be reviewed and updated.

As mentioned by **CTS-FGV** in its contribution, "*during storage, data shall be protected against unlawful, accidental or willful destruction, accidental loss or change, unauthorized or illegal disclosure and treatment or access. Moreover, proper measures are required to ensure that records shall only be accessed by duly authorized individuals and that data is destroyed at the end of the retention period prescribed by law. Data security measures, including encryption and authentication using encryption techniques, shall be defined according to risks and potential damages that may take place considering the following steps: creation and maintenance of records relative to connection and access to applications; · Process to transfer records of connection and access to applications to authorities;· Storage of records relative to connection and access to applications by the authorities*".

In addition, the experience of the European Union on the matter shall be taken into account. In particular, that of the European Commission Work Group for Article 29.

Who stands for that? *CTS-FGV.*

(B) *Regulation shall only define minimum security standards.*

To ensure protection to citizens' privacy and intimacy, the *Marco Civil* regulation shall define mandatory encryption of data bases containing users information (such as access logs) as minimum standard of security. Such obligation shall apply to retention any data and information and not only those

created to comply with the law. ISPs and application providers shall only provide encryption keys upon Court order determining access to data.

Who stands for that? *Actantes, Artigo 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, Instituto Bem Estar Brasil, Instituto Brasileiro de Defesa do Consumidor – IDEC, Instituto Brasileiro de Políticas Digitais - Mutirão, Instituto Goiano de Direito Digital – IGDD, Instituto Telecom, Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, PROTESTE – Associação de Consumidores*

(C) *Regulation shall be technology neutral and shall not require disclosure of the adopted security standards.*

Regulation shall not provide excessive details about security standards to be adopted subject to rendering new businesses difficult or unfeasible as time goes by and technology evolves (thus conflicting with economic freedom of ISPs and application providers).

Instead of thorough details of security standards, the decree shall encourage innovation and choice on the part of security standards agents that, based on their expertise of the business, better fulfill their service requirements.

With regard to the obligation to disclose security standards (article 10, paragraph 4), it is suggested that the obligation shall be solely for purposes of information to the general public, without jeopardizing trade secrets and actual security. Supporters of this argument claim that this kind of disclosure does not guarantee stricter security but rather a possible risk to information security.

Who stands for that? *ABRANET and Câmara Brasileira de Comércio Eletrônico*

4.6. Penalties

Article 12 of the Brazil's Internet Bill of Rights sets forth a list of penalties for agents who fail to properly comply with data retention and availability obligations prescribed by articles 10 and 11 of the law. Participants submitted contributions providing details as to how such penalties should be imposed.

4.6.1. How should the decree address the penalties imposed under article 12 of the Bill of Rights?

***Note by authors**: due to disparity of recommendations on this subject, contributions were organized as "recommendations" rather than as scattered answers. The difference here is that regulatory option of one recommendation does not prevent other recommendations from being selected as well.*

Individual recommendations for regulation of the matter:
(A) The decree shall establish that authorities having appropriate jurisdiction are to impose penalties. MPF supports this argument shall apply without prejudice to the penalties determined by the Court, whenever provoked, including by the Public Attorneys Office. **Author of recommendation:** *MPF (the Public Attorneys Office).*
(B) One single federal authority shall be responsible for imposing such penalties so as to ensure their consistent application in Brazil. In addition, with regard to item II, that establishes a fine of up to 10% of revenue, it is important to clarify that revenue only encompasses income generated from the activities that gave rise to the fine in Brazil. **Author of recommendation:** *Information Technology Industry Council.*
(C) As prescribed by article 11, paragraph 4, the decree shall make reference to the federal administrative procedure act (Law No. 9.784/99) in case of violation of records retention obligations and duties. **Authors of recommendation:** *GEPI–FGV, ABRANET and Câmara Brasileira de Comércio Eletrônico.*
(D) The decree must take into account article 50 of the Data Protection Draft Bill to establish penalties, to wit: *Art. 50. Violations of the rules set forth hereunder by privately owned legal entities shall be subject to the following administrative penalties imposed by the authority having appropriate jurisdiction:* *I – simple or daily fine;* *II – publication of the violation;* *III - unbundling of personal data;* *IV - block of personal data;*

V - suspension of personal data treatment operation for a period of time not to exceed two years;

VI - cancellation of personal data;

VII - prohibition to treat sensitive data for a period of time not to exceed ten years; and

VIII - prohibition of data bank operation for a period of time not to exceed ten years.

Paragraph 1. Penalties shall apply cumulatively.

Paragraph 2. Procedures and criteria to impose penalties shall be reasonable with regard to the severity and extent of the violation, nature of personal rights affected, recurrence, economic status of the violator and damages caused, per the terms of the regulation.

Paragraph 3. The periods of time for prohibition set forth in items VII and VIII of the head of this article may be renewed by the authority having appropriate jurisdiction provided failure to comply with its provisions, recurrence of violations or lack of full compensation for the damages caused by the violation is confirmed.

Paragraph 4. The terms of this article shall not prevent imposition of administrative, civil or criminal penalties prescribed by specific laws.

Paragraph 5. The terms of items III to VII shall apply to government owned entities and bodies, without prejudice to the provisions of Law No 8.112, of September 11, 1990 and Law No 8.429, of June 2, 1992.

Author of recommendation: *FIESP.*

(G) Regulation shall make sure it is clear that, except with regard to the fine set forth in item II, there is no joint or concurrent liability among legal entities of the same economic group with regard to the penalties thereunder. This means that in compliance with the principles of independence of legal entities and that no sentence shall produce any effect beyond the person accused, the penalties set forth in items I, III and IV shall only be imposed to the legal entity that actually violated the provisions of articles 10 and 11, and shall not apply to legal entities of the same economic group.

Author of recommendation: *Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (ABDTIC).*

4.7. Transparency

***Note by authors**: due to disparity of recommendations on this subject, contributions were organized as "recommendations" rather than as scattered answers. The difference here is that regulatory option of one recommendation does not prevent other recommendations from being selected as well.*

Individual recommendations for regulation of the matter:
(A) Article 11, paragraph 3, of the *Marco Civil* determines that all connection and applications providers shall provide, pursuant to the regulation, information allowing confirmation of compliance with Brazilian laws regarding collection, retention, storage or treatment of data. A recommendation is made that regulation shall clarify that such information shall be provided to the Public Attorneys Office whenever requested, with grounds on their respective institutional laws. The Public Attorneys Office, as an institution responsible for, among other attributions, protection of collective rights, shall have access to such data whenever required for citizen protection. **Author of recommendation:** *MPF (the Public Attorneys Office).*
(B) The decree shall request regular publication of reports and statistic data (available in open form and machine readable format) by the authorities and transparency on use of the mechanisms prescribed by the Brazil's Internet Bill of Rights. Such reports shall include all data and information accessed and how many were used on administrative or court proceedings. **Authors of recommendation:** *CTS-FGV, Francisco Brito Cruz, Laura Tresca, Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, Proteste - Associação de Consumidores.*

4.8. Personal data

The Brazil's Internet Bill of Rights, in particular article 7, makes reference to "personal data" and "treatment of data" without defining these terms.

4.8.1. Should the decree define expressions that refer to personal data?

***Note by authors**: due to disparity of recommendations on this subject, contributions were organized as "recommendations" rather than as scattered answers. The difference here is that regulatory option of one recommendation does not prevent other recommendations from being selected as well.*

Individual recommendations for regulation of the matter:
(A) Such definitions shall be addressed by the future personal data protection law. **Authors of recommendation:** *CTS-FGV, GEPI-FGV, Associação Nacional de Jornais - ANJ, Associação Brasileira de Marketing Direto - ABeMD, Associação Brasileira de Internet - ABRANET.*
(B) The decree shall establish (i) minimum criteria for services agreements with grounds on consumer protection laws; (ii) that personal data shall only be used for justifiable reasons vis-a-via the service/product offered; (iii) a specific and separate authorization for collection, use, storage, treatment and collection purpose of personal data; and (iv) that consent shall not be one-off to all product features. **Authors of recommendation:** *Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia, Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, Proteste - Associação de Consumidores.*

5. OTHER MATTERS AND CONSIDERATIONS

5.1 Jurisdiction: how should the decree address article 11 of the *Marco Civil*?

***Note by authors**: due to disparity of recommendations on this subject, contributions were organized as "recommendations" rather than as scattered answers. The difference here is that regulatory option of one recommendation does not prevent other recommendations from being selected as well.*

Individual recommendations for regulation of the matter:
(A) Contribution from researcher **Nicolo Zingales** aims to give meaning to the expressions of article 11 and to answer a few questions: (i) What does "content of communications" mean in Brazil? (ii) When shall an offering be deemed a "service offering to the Brazilian community"? (iii) When a data collection may be considered in Brazil? and (iv) What does "to have an establishment in Brazil" mean? (i) Content of communications shall be understood as content that, probably, may cause damages to the rights of Brazilian users. Therefore, it shall be possible to prevent the application of the Bill of Rights to situations without sufficient territorial connection. (ii) Shall only be deemed a services offering an action that actually seek to target the Brazilian community. Examples of elements that may determine whether the Brazilian community is targeted: (a) use of Brazilian currency or language, (b) list telephone numbers with Brazilian area code, (c) marketing or advertising focusing characteristics of Brazilian consumers, and (d) use of a Brazilian domain (.br). (iii) Collection of data shall refer to those collections aiming to create a user profile (*profiling*). That is, do not include that, potentially, cannot [sic] cause damages to users (e.g. *cookies*) (iv) For a company to be deemed established in Brazil it shall have human and technical resources required to provide certain services on a permanent basis, particularly taking into account the connection between services provided and activities with regard to which data is being treated. **Author of recommendation:** *Nicolo Zingales.*
(B) The decree shall make clear that the scope of article 11 is solely the application of Brazilian laws and not legitimacy or liability of a Brazilian legal entity regarding acts practiced by a foreign legal entity of the same group, as often argued in court and embraced by judges (that is, liability remains with the foreign legal entity, with no transfer of liability). **Author of recommendation:** *Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (abdtic)*
(C) Regulation shall clarify that only sites taking objective measures to attract Brazilian consumers shall be held liable under article 11 of the Brazil's Internet Bill of Rights. By way of example: marketing services to Brazilians, in Portuguese; contracts, services terms and user agreements in Portuguese; and offering of local content. **Author of recommendation**: *Information Technology Industry Council*

5.2. Objective requirements for determination of infringing content

5.2.1. How should content under court order for deletion be designated (article 19)?

Controversial positions on the subject:
(A) Designation shall be made by URL (*uniform resource locator*).
(B) URL is only one of the means that may be used to unambiguously identify content.

Summary of the positions and its supporters:

(A) *Designation shall be made by URL (uniform resource locator).*

Note by authors*: use of URL as a designation method is supported by participants not only in case of request for deletion by court order (article 19), as well as request for deletion by "unavailability notice" (article 21), as mentioned below.*

Designation by URL is sufficient to unambiguously identify content. There is even STJ (Brazil's Superior Court of Justice) precedent already referring to the understanding that this shall be the objective requirement to a clear and specific identification of content.

Furthermore, this kind of identification prevents application providers from being forced by a court order to create any type of content filter or monitoring without specific review of such content by the Judiciary.

Who stands for that? *Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (abdtic), ABRANET, Grupo de Ensino e Pesquisa em Inovação - FGV Direito SP (GEPI) and IASP.*

(B) *URL is only one of the means that may be used to unambiguously identify content.*

The decree shall list the means that may be used to identify content to be deleted by court order. Examples of this criteria are (i) content's URL; (ii) content posting code; (iii) name of infringer user (or identification code), jointly with data and time of content posting; among other criteria.

Regulation shall also bring examples of identification means that do not comply with legal requirements, such as key-words identification.

Finally, so as to protect freedom of expression, Decree shall clarify provider's duties after deletion of content. Provider shall not be forced to perform continued control fearing occasional reposting of the content subject to deletion by court order.

Who stands for that? *Associação Brasileira da Propriedade Intelectual – ABPI.*

5.2.2. How should content under court order for notice of content unavailability be designated (article 21)?

This provision states that Internet application providers shall be held liable for content created by third parties in the event images, videos or other material containing nude scenes or sex acts of a private nature are disclosed without authorization from their participants, **as of receipt of notice by participant or his/her legal representative**, and failed to render such content unavailable, diligently and within the scope and technical limits of their services.

Controversial positions on the subject:
(A) Designation shall be made by URL (*uniform resource locator*).
(B) The decree shall establish other requirements in addition to the URL.

Summary of the positions and its supporters:

(A) *Designation shall be made by URL (uniform resource locator).*

Designation by URL is sufficient to unambiguously identify content. There is even STJ (Brazil's Superior Court of Justice) precedent already referring to the understanding that this shall be the objective requirement to a clear and specific identification of content.

Furthermore, this kind of identification prevents application providers from being forced by a court order to create any type of content filter or monitoring without specific review of such content by the Judiciary.

Who stands for that? *Associação Brasileira de Direito da Tecnologia da Informação e das Comunicações (abdtic), ABRANET, Grupo de Ensino e Pesquisa em Inovação - FGV Direito SP (GEPI) and IASP.*

(B) *The decree shall establish other requirements in addition to the URL.*

For the content to be deleted, notice shall be submitted jointly with personal document or by a legal representative with a power of attorney, as well as a statement of the victim confirming to actually be a participant of the infringing content. The person who posted the content shall be notified to take appropriate measures in case he/she considers that the deletion of the content was undue and affects his/her freedom of expression.

Who stands for that? *Laura Tresca, Actantes, Antivigilância.org, ARTIGO 19, Centro de Estudos da Mídia Alternativa Barão de Itararé, Ciranda Internacional da Comunicação Compartilhada, Clube de Engenharia,*

Coletivo Digital, HackAgenda, IBIDEM - Instituto Beta para Internet e Democracia, Idec - Instituto Brasileiro de Defesa do Consumidor, IGDD - Instituto Goiano de Direito Digital, Instituto Bem Estar Brasil Instituto, Telecom Intervozes - Coletivo Brasil de Comunicação Social, Movimento Mega, Proteste - Associação de Consumidores.

5.2.3. Which should be the deadline for deletion of content following notice (article 21)?

Individual recommendation for regulation of the matter:

(A) Despite the general rule requiring specific court order to hold providers liable for illegal content, the Brazil's Internet Bill of Rights created a few exceptions. This is the case, by way of example, of article 21, applicable to cases involving "nudity or sex acts of a private nature". Under these circumstances, "upon receipt of notice by participant or his/her legal representative, provider shall make the content unavailable, diligently and within the scope and technical limits of his/her service, subject to be deemed subsidiarily liable from violation of intimacy resulting from unauthorized posting of infringing content.

Proponents recommend to regulate the way such unavailability shall take place. They believe that to subject provider to comply with a deletion order only "in a diligent way" may render this article ineffective and contrary to court precedents already settled.

STJ precedent already referred to a 24-hour deadline for deletion of unlawful content from Internet applications:

> *"Once notified that a given text or image contains unlawful content, provider must delete such material within twenty-four (24) hours subject to be held jointly liable with the author who directly caused the damage, as a result of its omission".* (RESP 1323754/RJ, Third Chamber, Justice Nancy Andrighi, date: 19/06/2012)

Thus, proponents recommend to regulate such "diligent way" so as to specify a deadline, which could be the same already referred to by STJ, that is, 24h.

Authors of recommendation: *Comissão Especial de Propriedade Intelectual (CEPI) from OAB/RS*

5.3. How should the decree address incentive to use open formats?

Individual recommendation for regulation of the matter:

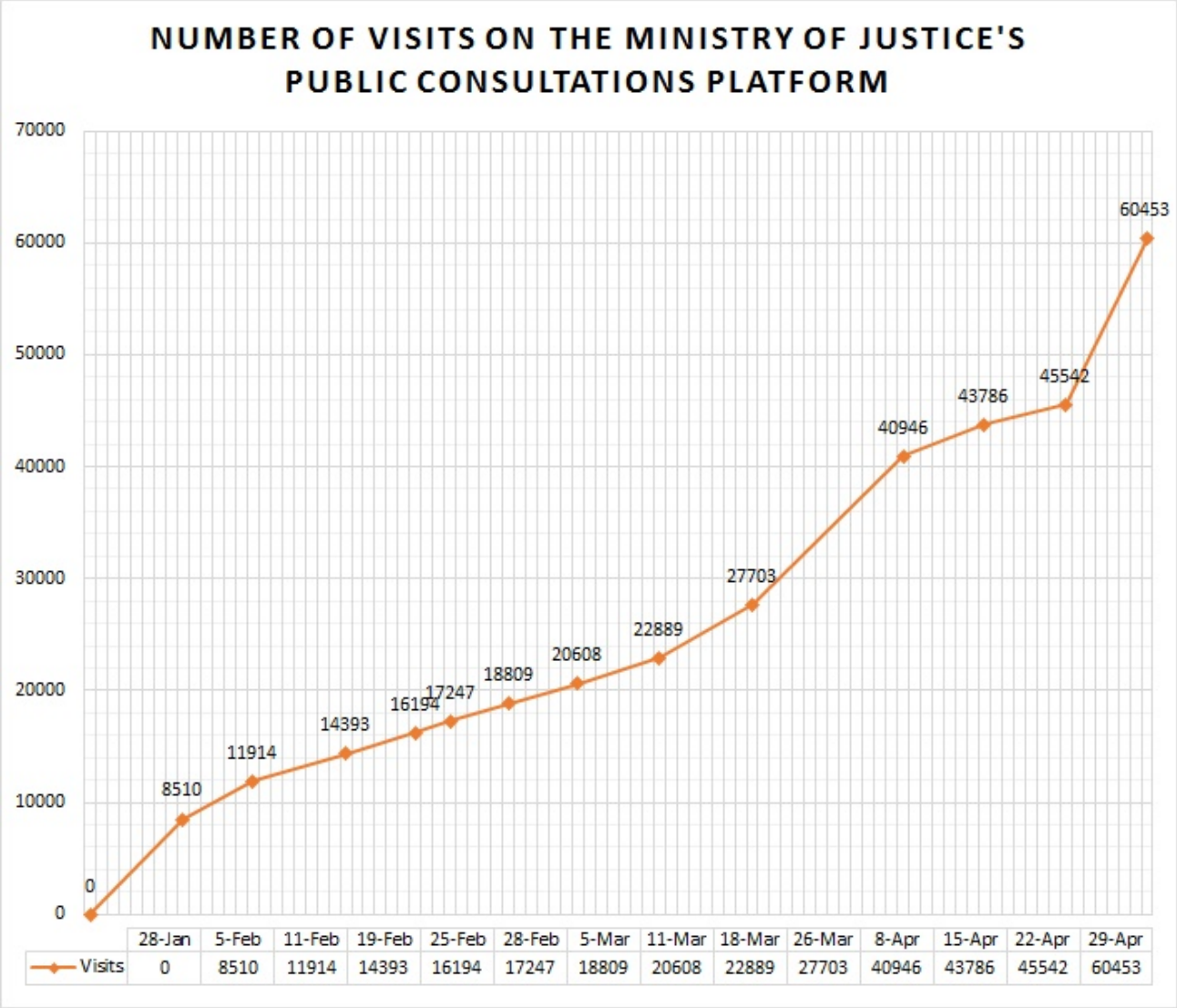
(A) "*We emphasize that item III of article 25 of the Brazil's Internet Bill of Rights establishes that 'Internet applications from Government owned entities shall seek (...) compatibility both with format readable by human as well as automated treatment of information.*

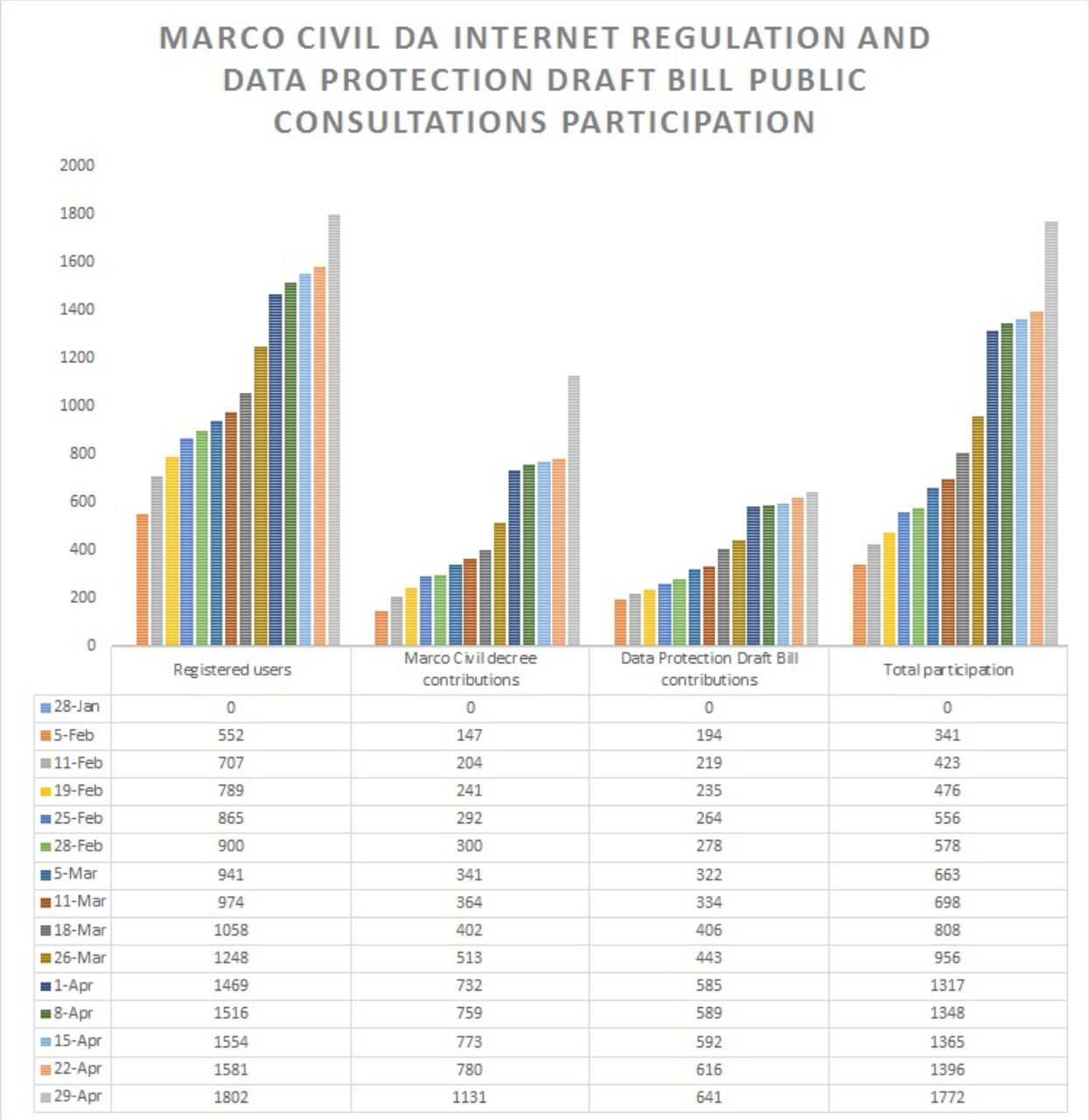
We consider the Regulation an excellent opportunity to guide, as a practical matter, how Public Authorities shall treat and make their data available to contemplate Web Semantics logic. It is only by establishing technical communications requirements to operate data, as well as by mandatory adoption of standardized data that an effective policy on open data may generate concrete results to improve society democratic mechanisms.

There are not only a few cases in which information is made available, however, different formats prevent actual appropriation by those interested and relevant to the debate on digital democracy".

Author of recommendation: *Grupo de Ensino e Pesquisa em Inovação - FGV Direito SP (GEPI)*

6. CHARTS OF PARTICIPATION QUANTITY PROFILE





	Registered users	Marco Civil decree contributions	Data Protection Draft Bill contributions	Total participation
28-Jan	0	0	0	0
5-Feb	552	147	194	341
11-Feb	707	204	219	423
19-Feb	789	241	235	476
25-Feb	865	292	264	556
28-Feb	900	300	278	578
5-Mar	941	341	322	663
11-Mar	974	364	334	698
18-Mar	1058	402	406	808
26-Mar	1248	513	443	956
1-Apr	1469	732	585	1317
8-Apr	1516	759	589	1348
15-Apr	1554	773	592	1365
22-Apr	1581	780	616	1396
29-Apr	1802	1131	641	1772

7. TABLE OF ACTORS AND ITS SECTORS

Stakeholder	Category	Sector
FEBRATEL	Association	ISP sector
SINDITEBRASIL	Association	ISP sector
SINDISAT	Association	ISP sector
TELCOMP	Association	ISP sector
TELEBRASIL	Association	ISP sector
ABRAFIX	Association	ISP sector
ACEL	Association	ISP sector
ABINEE	Association	ISP sector
Tim Brasil	Corporation	ISP sector
Cisco Brasil	Corporation	ISP sector
Brasscom	Association	Large Application Providers Sector
Claro S/A	Corporation	ISP sector
COGPC/SEAE/MF	Government Bureau	Government
AccessNow	Think Tank / Watchdog / NGO	Civil Society
Artur	Individual	Civil Society
Sergio Deliconi	Individual	Civil Society
ABSTARTUPS	Association	Small Application Providers Sector
Actantes	Think Tank / Watchdog / NGO	Civil Society
Artigo 19	Think Tank / Watchdog / NGO	Civil Society
Centro de Estudos da Mídia Alternativa Barão de Itararé	Think Tank / Watchdog / NGO	Civil Society
Ciranda Internacional da Comunicação Compartilhada	Think Tank / Watchdog / NGO	Civil Society
Clube de Engenharia	Think Tank / Watchdog / NGO	Civil Society
Coletivo Digital	Think Tank / Watchdog / NGO	Civil Society
HackAgenda	Think Tank / Watchdog / NGO	Civil Society
Instituto Bem Estar Brasil	Think Tank / Watchdog / NGO	Civil Society
Instituto Brasileiro de Defesa do Consumidor – IDEC	Think Tank / Watchdog / NGO	Civil Society
Instituto Brasileiro de Políticas Digitais - Mutirão	Think Tank / Watchdog / NGO	Civil Society
Instituto Goiano de Direito Digital – IGDD	Think Tank / Watchdog / NGO	Civil Society
Instituto Telecom	Think Tank / Watchdog / NGO	Civil Society
Intervozes - Coletivo Brasil de Comunicação Social	Think Tank / Watchdog / NGO	Civil Society
Movimento Mega	Think Tank / Watchdog / NGO	Civil Society
PROTESTE – Associação de Consumidores	Think Tank / Watchdog / NGO	Civil Society
ABRINT	Association	ISP sector
CTS-FGV	Academic Organization	Academy
Netflix Brasil	Corporation	Large Application Providers Sector

ABDTIC	Association	Academy
Pedro Ramos	Individual	Academy
Cristiana Gonzalez	Individual	Academy
ANER	Association	Press Sector
IASP	Association	Academy
ABRANET	Association	ISP sector
ANJ	Association	Press Sector
ILCO	Association	Civil Society
Sky Brasil	Corporation	ISP Sector
Roberto Taufick	Individual	Civil Society
Telecommunications Industry Association	Association	ISP Sector
Laura Tresca	Individual	Civil Society
MPAA	Association	Copyright Owners Sector
Fórum Nacional Contra a Pirataria e Ilegalidade	Association	Civil Society
ABPI	Association	Academy
CEPI	Association	Civil Society
OAB/RS	Bar	Academy
PROCON/SP	Government Bureau	Government
ABEMID	Association	Marketing Sector
Câmara Brasileira de Comércio Eletrônico	Association	Large Application Providers Sector
Movimento Mega	Think Tank / Watchdog / NGO	Civil Society
MPF	Government Bureau	Government
OAB/SC	Bar	Academy
ITS-Rio	Academic Organization	Academy
Cnseg	Association	Insurance Sector
José Antonio Milagre	Individual	Civil Society
FIESP	Association	Industry Sector
Veridiana Alimonti	Individual	Civil Society
Joana Varon	Individual	Academy
ITT	Association	Large Application Providers Sector
GEPI-FGV	Academic Organization	Academy
Ana Cristina Azevedo	Individual	Civil Society
Emerson Wendt	Individual	Civil Society
Antivigilância.org	Think Tank / Watchdog / NGO	Civil Society
Francisco Brito Cruz	Individual	Academy
Information Technology Industry Council	Association	Large Application Providers Sector
Nicolo Zingales	Individual	Civil Society
OAB/RS	Bar	Academy