Instituto
de Tecnologia
& Sociedade
do Rio

Brazil's Internet Bill of Rights: A Closer Look

Carlos Affonso Souza, Mario Viola
& Ronaldo Lemos (eds.)

Instituto
de Tecnologia
& Sociedade
do Rio

Brazil's Internet Bill of Rights: A Closer Look

Carlos Affonso Souza, Mario Viola
& Ronaldo Lemos (eds.)

Second Edition

Editing
Carlos Affonso Souza, Mario Viola & Ronaldo Lemos

Revision
Beatriz Nunes

Cover and design
Thiago Dias

Publication, bound and print
Editar Editora Associada – Juiz de Fora – MG, Brazil
+55 32 3213-2529 / +55 32 3241-2670

International data for the purposes of cataloging of the publication

S719b Souza, Carlos Affonso
V795b Viola, Mario
L544b Lemos, Ronaldo

Brazil's Internet Bill of Rights: A Closer Look / Carlos Affonso Souza, Mario Viola & Ronaldo Lemos. _____

ISBN: 978-85- 7851-172- 2

1. Information technology. 2. Internet.

CDD 004
CDU 004.7

Summary

Introduction

The idea to create a Bill of Rights for the Internet is not exactly new. Since 2006 the United Nations' Internet Governance Forum (IGF) has enabled an on-going debate around several Internet Bill of Rights initiatives.

Brazil has been in the forefront of this debate right from the start. For reasons that are further explained in this book, the initiative to create an Internet Bill of Rights took a hard law approach.

This book makes the law accessible for English readers and provides an analysis on some of the main topics regulated by the Internet Bill of Rights. A translated version of the Bill and its regulatory decree (Decree no. 8.771/2016) is also included to facilitate the readers' comprehension of the main topics annotated by ITS Rio's team and fellows.

The first chapter provides a glimpse on how the law has affected Brazilian society and what are the present and future challenges threatening this legislation. On the following two chapters, the authors explain how the process of creation was inspired by multistakeholder and collaborative principles. The fourth chapter illustrates how the law treats privacy issues such as data protection. The fifth chapter is an overview on how the Marco Civil treats intermediaries' liability when it comes to different kinds of providers. The sixth chapter compares the intermediary liability regime adopted by the Brazilian Law to the one currently in force in North America. The seventh chapter shows how the Internet Bill of Rights influenced other countries. The final chapter explores the issue of revenge porn and how the Law tackles it.

This book is an extended, reviewed and updated version of ITS Rio's "Understanding Brazil's Internet Bill of Rights". It was only possible due to the revision and suggestions made by Beatriz Laus Marinho Nunes. The authors of this book and the entire ITS team hope you enjoy reading the next pages as much as we did writing them!

Law no. 12.965 of April 23, 2014: The Internet Bill of Rights

Internet Bill of Rights

OFFICE OF THE PRESIDENT OF THE REPUBLIC

CIVIL CHIEF OF STAFF

DEPARTMENT OF LEGAL AFFAIRS

Law No. 12.965 of April 23, 2014

Sets forth principles, guarantees, rights, and duties for Internet use in Brazil.

I, THE PRESIDENT OF THE REPUBLIC, make it known that the National Congress has decreed and I have sanctioned the following Law:

CHAPTER I
PRELIMINARY PROVISIONS

Art. 1. This Law sets forth principles, guarantees, rights, and duties for Internet use in Brazil and establishes guidelines for action by the Union, the States, the Federal District, and the Municipalities regarding the Internet.

Art. 2. The foundations of Internet governance in Brazil are based on the respect for freedom of expression and:

I – recognition of the global scale of the network;

II – human rights, individual development, and the exercise of civic awareness through digital media;

III – pluralism and diversity;

IV – openness and collaboration;

V – free enterprise, free competition, and consumer protection; and

VI – the social purposes of the network.

Art. 3. The following principles underlie Internet governance in Brazil:

I – freedom of expression, communication, and thought, as provided for in the Federal Constitution;

II – protection of privacy;

III – personal data protection, as provided by law;

IV – preserving and guaranteeing network neutrality;

V – ensuring stability, security, and functionality by technical means consistent with international standards and by encouraging the use of best practices;

VI – holding agents liable for their actions, as provided for by law;

VII – preserving the network's participatory nature;

VIII – freedom to do business on the Internet, as long as it does not conflict with other principles established in this Law.

§1. The principles set out in this Law do not exclude others related to the same subject matter under Brazilian law or international treaties to which Brazil is party.

Art. 4. The purpose of Internet governance in Brazil is to promote:

I – Internet access for all;

II – access to information and knowledge, and participation in cultural life and public affairs;

III – innovation and widespread availability of new technologies and models to use and access the Internet; and

IV – adherence to open technology standards that allow for communication, accessibility, and interoperability between applications and databases.

Art. 5. For the purposes of this Law, the following terms have the meaning ascribed to them below:

I – Internet: a system formed by a set of logical protocols, structured on a worldwide scale for unrestricted public use, enabling data communication between terminals through different networks;

II – terminal: any computer or device that connects to the Internet;

III – Internet protocol address (IP address): a code defined according to international standards, assigned to a terminal connected to a network, allowing it to be identified;

IV – autonomous system administrator: a person or legal entity that administers specific blocks of IP addresses and the corresponding autonomous routing system, and that is duly registered with the national authority responsible for registration and distribution of IP addresses geographically allocated to the country;

V – Internet connection: the assignment or authentication of an IP address, enabling a terminal to send and receive data packets over the Internet;

VI – connection log: a record of information regarding the date and time that the Internet connection begins and ends, its duration, and the IP address used by the terminal to send and receive data packets;

VII – Internet applications: the set of functionalities that can be accessed by a terminal connected to the Internet, and

VIII – Internet application access log: a record of information regarding the date and time when a given Internet application was accessed from a certain IP address.

Art. 6. In interpreting this Law, the nature of the Internet, its particular uses and traditions, and its importance in promoting human, economic, social, and cultural development must be taken into account, in addition to the foundations, principles, and objectives set forth herein.

CHAPTER II
USERS' RIGHTS AND GUARANTEES

Art. 7. Internet access is essential for the exercise of citizenship rights and duties, and users have the right to:

I – privacy and private life, and to compensation for material and moral damages resulting from violation of the right to privacy and private life;

II – confidentiality of communications made via the Internet, which may only be disclosed by judicial order in the manner provided for by law;

III – confidentiality of stored private communications, which may only be disclosed by judicial order;

IV – maintenance of Internet connection, unless it is terminated due to the user's failure to pay for its use;

V – a consistent Internet connection in accordance with the quality contracted with the provider

VI – clear and complete information in contracts with Internet service providers, including a detailed description of the measures taken to protect connection logs and Internet application access logs, and of network management practices that could affect the quality of the service;

VII – non-disclosure of their personal data to third parties, including connection logs and Internet application access logs, except with their free, express, and informed consent or in the cases provided for by law;

VIII – clear and comprehensive information on the collection, use, storage, and protection of users' personal data, which may only be used for purposes that:

a) justify collecting the data;

b) are not prohibited by law; and

c) are specifically stated in Internet service contracts or in terms and conditions for use of Internet applications.

IX – express consent for the collection, use, storage, and processing of personal data, which must be presented in a way that distinguishes the consent clause from the other contractual clauses;

X – full removal of personal data supplied to Internet applications, at the users request, at the end of the agreement between the parties, except when this Law requires records to be kept;

XI – policies on use that are clear and publicized, when Internet service providers or Internet applications providers adopt such policies;

XII – accessibility, taking into account users' physical, motor, perceptual, sensory, intellectual, and mental abilities, as provided for by law; and

XIII – application of consumer protection rules to consumer relations that take place on the Internet.

Art. 8. Protection of the right to privacy and freedom of expression in communications is a necessary condition for the full exercise of the right to Internet access.

§1. Contractual clauses that violate the above provision are void, as are those that:

I – violate the right to privacy and confidentiality of private communications over the Internet; or

II – do not offer users, in adhesion contracts, the option of adopting Brazilian jurisdiction for the resolution of disputes in connection with services provided in Brazil.

CHAPTER III
INTERNET SERVICE AND APPLICATIONS PROVIDERS

Section I
Net Neutrality

Art. 9. The agent in charge of transmission, switching, and routing must give all data packets equal treatment, regardless of content, origin and destination, service, terminal or application.

§1. Traffic discrimination and degradation will be subject to regulations issued under the exclusive powers granted to the President of the Republic in article 84(iv) of the Federal Constitution, for the better implementation of this Law, after hearing the Brazilian Internet Steering Committee (CGI.br) and the National Telecommunications Agency (Anatel), and may only result from:

I – technical requirements essential to the adequate provision of services and applications, and

II – prioritization of emergency services.

§2. In the event of traffic discrimination or degradation, as contemplated in §1, the agent in charge must:

I – refrain from causing damage to users, as provided for in article 927 of the Civil Code (Law no. 10.406 of January 10, 2002);

II – act in a fair, proportionate, and transparent manner;

III – provide users, in advance, with clear and sufficiently descriptive information on its traffic management and mitigation practices, including network security measures; and mitigation,

IV – provide services on non-discriminatory commercial terms and refrain from anticompetitive practices.

§3. Subject to the provisions of this article, the content of data packets may not be blocked, monitored, filtered or analyzed in Internet connections, either paid or free of charge, or in transmission, switching, and routing.

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

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

§1. The provider responsible for maintaining the logs may only be required to make those logs available, either alone or together with personal data or other information that could help to identify a user or terminal, by judicial order as contemplated for in Section IV of this Chapter, subject to the provisions of article 7.

§2. The content of private communications may only be disclosed by judicial order, in the cases and in the

manner provided for by law, subject to the provisions of article 7(II) and (III).

§3. This article does not prevent access to users' identification information and addresses by administrative authorities holding powers under the law to requisition that information.

§4. Security and confidentiality measures and procedures must be clearly communicated by the service provider and must meet regulatory standards, subject to the service provider's right to protect trade secrets.

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

§1. The provisions of this article apply to all data collected in Brazilian territory and to the content of communications if at least one of the terminals is located in Brazil.

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

§3. Internet connection and application providers must provide, in the manner established by regulation, information needed to determine whether Brazilian law has

been complied with concerning the collection, retention, storage, and processing of data and on protection of privacy and confidentiality of communications..

§4. Regulations on the procedure for determining whether infractions of this article have occurred will be issued by decree.

Art. 12. In addition to any civil, criminal or administrative sanctions that may apply, any infraction of the rules under articles 10 and 11 is subject to the following sanctions, applied singly or in conjunction, according to each case:

I – a warning, which will establish a deadline for any corrective measures;

II – a fine of up to 10% of the economic group's sales revenue in Brazil in its most recent financial year, excluding taxes, to be fixed in light of the offender's financial condition and the principle of proportionality between the seriousness of the offense and the severity of the penalty.

III – temporary suspension of activities that involve the acts referred to in article 11; and

IV – prohibition of activities that involve the acts referred to in article 11

§1. In the case of foreign companies, any subsidiary, branch, office or establishment located in Brazil will be jointly liable for the payment of the fine referred to above.

Subsection I
Maintenance of Internet Connection Logs

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

§1. Responsibility for keeping connection logs may not be transferred to third parties.

§2. The police or administrative authorities or the Public Prosecution Service may require as a precaution that connection logs be kept for longer than the period provided for in this article.

§3. In the event provided for in §2, the requesting authority will have a period of 60 days from the date the request is made to file an application for judicial authorization to access the logs referred to in this article.

§4. The provider responsible for keeping the logs must keep the request provided for in §2 confidential; the request will become void if the application for judicial authorization is rejected or is not filed within the time period established in §3.

§5. In all cases, judicial authorization must be obtained before logs are made available to the requesting authority, in compliance with Section IV of this Chapter.

§6. In applying sanctions for failure to comply with this article, the nature and severity of the infraction, the resulting

damage, the potential benefit to the offender, the aggravating circumstances, and the offender's record and repeat offenses, if any, will be taken into consideration.

Subsection II
Maintenance of Internet Application Access Logs in Providing Internet Connection

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

Subsection III
Maintenance of Internet Application Access Logs in Providing Applications

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

§1. Internet applications providers that are not subject to the above provisions may be required by judicial order to keep access logs to Internet applications in connection with specific facts for a determined period of time.

§2. The police or administrative authorities or the Public Prosecution Service may require any Internet application provider, as a precaution, to keep Internet application logs, and to keep them for a period longer than the period established in the head of this article, subject

to the provisions of article 13 §3 and §4.

§3. In all cases, judicial authorization must be obtained before logs are made available to the requesting authority, in compliance with Section IV of this Chapter.

§4. In applying sanctions for failure to comply with this article, the nature and severity of the infraction, the resulting damage, the potential benefit to the offender, the aggravating circumstances, and the offender's record and repeat offenses if any will be taken into consideration.

Art. 16. In providing Internet applications, either paid or free of charge, it is forbidden to keep:

I – logs of access to other Internet applications unless the data subject has given consent in advance, subject to the provisions of article 7; or

II – personal data that exceeds the purpose for which the data subject gave consent.

Art. 17. Except in the cases provided in this Law, the choice not to keep logs of access to Internet applications does not result in liability to third parties for damage suffered because of their use of such services.

Section III
Liability for Damage Caused by Content Produced by Third Parties

Art. 18. Internet connection providers do not have civil liability for damages resulting from content produced by third parties.

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

§1. Under the penalty of nullity, the judicial order referred to above, must specifically identify the offensive content for the unequivocal location of the material.

§2. This article will apply to violations of copyright and related rights only when specific legislation to that effect is adopted; the legislation, when adopted, must respect the freedom of expression and other guarantees provided for in article 5 of the Federal Constitution.

§3. Actions dealing with damage reparation resulting from content related to the claimant's honor, reputation or personality rights made available on the Internet, or with Internet applications providers' removal of such content, may be brought before small claims courts.

§4. The court may grant the relief requested in the complaint on a preliminary basis, in whole or in part, if there is unmistakable proof of the facts and after considering the public's interest in making the content available on the Internet, as long as the claimant shows that his claim is prima facie good and that there is reason to believe that irreparable harm, or harm that would be difficult to repair, would occur if the relief was not granted in advance.

Art. 20. If the Internet application provider has contact information for the user who is directly responsible for the content referred to in article 19, the provider must notify the user for the reasons for removing the content and other information related to its removal, with sufficient detail to enable a full answer and defense in court, unless applicable legislation or a reasoned court order expressly stipulates otherwise.

§1. At the request of the user who posted the content that was removed, the Internet applications provider, if it is a legal entity providing applications in an organized, professional manner, for profit, must replace the removed content with a statement of the reasons for removal or the judicial order to remove the content.

Art. 21. Internet applications providers that make available content created by third parties will be secondarily liable for the violation of privacy resulting from the disclosure, without the participants' authorization, of images, videos, and other materials containing nudity or sexual acts of a private nature, if after receiving notice from the participant or the participant's legal representative, the Internet applications provider fails to

promptly to remove the content from its service, subject to technical limitations of the service.

§1. Under the penalty of nullity, the notice referred to in this article must contain elements that allows the Internet applications provider to identify the specific material that allegedly violates the participant's right to privacy and to determine that the person making the request has a lawful interest to do so.

Section IV
Judicial Order for Disclosure of Records

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

§1. In addition to other legal requirements, the application will not be admissible unless it contains the following:

I – good grounds to suggest that an unlawful act was committed;

II – good reason to believe that the requested logs will be useful as evidence or for purposes of investigation; and

III – the period to which the records relate.

Art. 23. The court has powers to impose measures to ensure the confidentiality of the information received and to preserve privacy, private life, honor, and public image of

the user, and may order that public access to the information, including the application for production, be limited.

CHAPTER IV
THE ROLE OF PUBLIC AUTHORITIES

Art. 24. The following are guidelines for action by the Union, the States, the Federal District, and the Municipalities for the development of the Internet in Brazil:

I – establishing multistakeholder, transparent, collaborative, and democratic governance mechanisms, with the participation of the government, the private sector, civil society, and the academic community;

II – promoting rationalization in the management, expansion, and use of the Internet, with the participation of the Brazilian Internet Steering Committee;

III – promoting rationalization and technological interoperability of electronic government services among the different branches and levels of government, allowing the exchange of information and expeditious procedures;

IV – promoting interoperability between different systems and terminals, including the different levels of government and various sectors of society;

V – adopting preferably free and open technologies, standards and formats;

VI – promoting access to and dissemination of public data and information in an open and structured manner;

VII – optimizing infrastructure networks and encourag-

ing the creation of data storage, management and dissemination centers in Brazil and promoting technical quality, innovation, and widespread availability of Internet applications, without detriment to the openness, neutrality, and collaborative nature of the Internet;

VIII – developing actions and training programs for Internet use;

IX - promoting culture and citizenship;

X – providing integrated, effective, and simplified public services to citizens through multiple channels, including remote access.

Art. 25. Government Internet applications must promote:

I – compatibility of e-government services with different terminals, operating systems, and access applications;

II – accessibility for all interested parties, regardless of their physical and motor skills, or perceptual, cultural, and social characteristics, while ensuring confidentiality and compliance with administrative and legal restrictions;

III – compatibility with both human reading and automated data processing;

IV – user friendliness of all e-government services, and

V – strengthened social engagement in public policies.

Art. 26. The government's constitutional duty to provide education at all levels of learning, includes

training, in combination with other educational practices, for safe, aware, and responsible use of the Inter-

net as a tool for exercising citizenship rights and duties, promoting culture and developing technology.

Art. 27. Public initiatives to promote digital literacy and use of the Internet as a social tool must:

I – promote digital inclusion;

II – seek to reduce inequalities in access to and use of information and communication technologies, particularly between different regions of Brazil; and

III – foster production and dissemination of national content.

Art. 28. The government must, at regular intervals, design and encourage studies, and establish goals, strategies, action plans, and timelines, for the use and development of the Internet in Brazil.

CHAPTER V
FINAL PROVISIONS

Art. 29. Users are free to use the software of their choice to facilitate parental control over content that parents consider inappropriate for their minor children, subject to the principles under this Law and of Law no. 8069 of July 13, 1990 – The Child and Adolescent Statute.

§1. Government, in conjunction with Internet connection and applications providers and civil society, has the duty to promote education and provide information on use of the software referred to in this article, and to define best practices for the digital inclusion of chil-

dren and adolescents.

Art. 30. The rights and interests established in this Law may be enforced through the courts, in individual or collective actions, in the manner provided for by law.

Art. 31. Until the specific legislation referred to in article 19, §2 comes into force, the liability of Internet applications providers for damages resulting from content generated by third parties, in the case of copyright infringements and related rights, will continue to be governed by the legislation on copyright in effect on the date that this Law came into force.

Art. 32. This Law comes into force 60 days after its official publication.

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

DILMA ROUSSEFF

José Eduardo Cardozo

Miriam Belchior

Paulo Bernardo Silva

Clélio Campolina Diniz

This text does not replace the text published in the Diário Oficial da União dated April 24, 2014.

Brazil's Internet Bill of Rights
Regulatory Decree
no. 8.771/2016

OFFICE OF THE PRESIDENT OF THE REPUBLIC

CIVIL CHIEF OF STAFF

LEGAL AFFAIRS DEPARTMENT

DECREE No. 8.771 of May 11 2016

Regulates Law No. 12.965 of April 23, 2014 to address the cases in which traffic discrimination and degradation is permitted, indicate procedures for data storage and protection to be followed by Internet connection and applications providers, set out transparency measures for requisitions of user identification data by public authorities and establishes parameters for monitoring and investigating infractions.

THE PRESIDENT OF THE REPUBLIC, in the use of the powers conferred under article 84(IV) of the Constitution, and in view of the provisions of Law no. 12.965 of 23 April 2014,

DECREES:

CHAPTER I
GENERAL PROVISIONS

Art. 1. This Decree relates to cases in which traffic discrimination and degradation is permitted, indicates procedures for data storage and protection to be followed by Internet connection and applications providers, sets out transparency measures for requisitions of user identification data by public authorities, and establishes monitoring and investigating infractions con-

tained in Law no. 12.965 of April 23, 2014.

Art. 2. The provisions in this Decree apply to agents in charge of transmission, switching and routing and to Internet connection and applications providers operating on the Internet, as that term is defined in article 5(I) of Law no. 12.965 of 2014.

Sole paragraph. The provisions in this Decree do not apply:

I – to telecommunications services that are not intended to provide Internet connection; and

II – to specialized services, defined as optimized services by reason of their assured quality of service, speed or security, even though they use TCP/IP or equivalent protocols, as long as:

a) they do not constitute a substitute for the Internet in its public and unrestricted character; and

b) they are intended for specific groups of users with strictly controlled admission.

CHAPTER II
NET NEUTRALITY

Art. 3. The equal treatment requirement under article 9 of Law no. 12.965 of 2014 must preserve the public and unrestricted character of Internet access and the foundations, principles and objectives of Internet use in Brazil, as provided for in Law no. 12.965 of 2014.

Art. 4. Traffic discrimination or degradation are exceptional measures, in that it may result only from tech-

nical requirements that are essential to providing adequate service and applications or from prioritization of emergency services, and must comply with all the requirements under article 9 §2 of Law 12.965 of 2014.

Art. 5. The technical requirements that are essential for the adequate provision of services and applications must be complied with by the agent in charge of transmission, switching or routing activities, within its respective network, and must be intended to maintain the network's stability, security, integrity and functionality.

§ 1. The essential technical requirements referred to above are those resulting from:

I – handling network security issues, such as restriction on sending bulk messages (spam) and controlling denial-of-service attacks; and

II – handling exceptional network congestion situations, such as alternative routes in case of main route interruptions and emergencies.

§ 2. The National Telecommunications Agency (Anatel) will conduct inspections and investigations of infractions as to the technical requirements set out in this article, taking into consideration the guidelines established by the Internet Management Committee (CGIbr).

Art. 6. In order to provide adequate Internet services and applications, network management is permitted when it is intended to preserve network stability, security and functionality, and uses only technical measures compatible with international standards developed for the proper functioning of the Internet, subject to compliance

with the regulatory standards issued by Anatel and taking into consideration the guidelines established by CGIbr.

Art. 7. The agent in charge of transmission, switching or routing must adopt transparency measures designed to ensure that users understand the reasons for implementing network management practices that result in the discrimination or degradation referred to in article 4, such as:

I – including provisions in service contracts entered into with final users and application providers; and

II – disclosing information on network management practices on their websites, using easily understood language.

Sole paragraph. The information contemplated in this article must contain at least:

I – a description mentioned practices;

II – the effects the adoption of mentioned practices on the quality of users' experience; and

III – the reasons and need for adopting the practices.

Art. 8. Degradation or discrimination due to the prioritization of emergency services may only result from:

I – communications directed to emergency services providers, or communications among emergency service providers, as provided in regulations issued by the National Telecommunications Agency - ANATEL;

II – communications necessary to warn the population of disaster risks, emergency situations or states of public calamity.

Sole paragraph. Transmission of data in the cases listed in this article will be free of charge.

Art. 9. Unilateral conduct is prohibited, as are agreements made between agents in charge of transmission, switching or routing and applications providers that:

I – compromise the public and unrestricted nature of the Internet and the foundations, principles and objectives of Internet use in Brazil;

II – prioritize data packets by reason of commercial arrangements; or

III – prioritize applications offered by the same agent that is in charge of transmission, switching or routing or by a company within its economic group.

Art.10. Commercial offers and Internet access pricing models must preserve the unity of the Internet and its open, plural and diverse nature, serving as a means to promote human, economic, social and cultural development, and contributing to build an inclusive and non-discriminatory society.

CHAPTER III
PROTECTION OF LOGS, PERSONAL DATA AND PRIVATE COMMUNICATIONS

Section I
User identification data requisition

Art.11. The administrative authorities referred to in arti-

cle 10 §3 of Law no. 12.965 of 2014 will state the legal provisions that expressly give them powers to access the data, and the reasons for the request for access to user identification data.

§ 1. Providers that do not collect user identification data must inform the requesting authority of the fact, and is released from the obligation to provide the data.

§ 2. The following is considered user identification data:

I – the names of the user's mother and father;

II – the user's address; and

III – the user's personal qualifications, which are his or her family name, first name, civil status and profession.

§ 3. The requests referred to above must specify the individuals whose data are requested and the information desired. Collective requests that are generic or non-specific are prohibited.

Art. 12. The highest authority of each entity within the federal public administration will publish annually on its website statistical reports on user identification data requisitions, containing:

I – the number of requests made;

II – a list of Internet connection and applications providers from which data were requisitioned;

III – the number of requests accepted and refused by the Internet connection and applications providers; and

IV – the number of users affected by the requests.

Section II
Standards for security and confidentiality of logs, personal data and private communications

Art. 13. In keeping, storing and processing personal data and private communications, Internet connection and applications providers must comply with the following guidelines on security standards:

I – strict control of access to data, by defining the responsibilities of those people who are able to access the data, and determining exclusive access privileges for certain users;

II – authentication mechanisms for access to logs, using, for example, double authentication systems to ensure that the personal responsible for log processing is individually identified;

III – detailed inventory of access to connection logs and access to applications containing the time, duration, identity of the employee or person responsible for the access designated by the company and the file accessed; the inventory will also serve for the purposes of compliance with article 11 §3 of Law no. 12.965 of 2014;

IV – record management solutions using techniques that ensure data security, such as encryption or equivalent protection measures.

§1. CGIbr will carry out studies and recommend procedures, rules and technical and operational standards for the purposes of this article, in accordance with the

specific characteristics and the size of the Internet connection and application providers.

§ 2. In view of article 7(VII) to (X) of Law no. 12.965 of 2014, Internet connection and applications providers must retain the least possible amount of personal data, private communications and logs of connection and access to applications, which must be removed:

I – as soon as the purpose for which the data or log was kept has been achieved; or

II – at the end of the time period established by law.

Art.14. For the purposes of this Decree:

I – personal data means data related to identified or identifiable natural person, including identifying numbers, location data and electronic identifiers, when they are related to a person; and

II – processing of personal data means any operation carried out using personal data, such as collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, removal, evaluation or control of the information, modification, communication, transfer, distribution or extraction.

Art. 15. The data referred to in article 11 of Law 12.965 of 2014 must be kept in an interoperable and structured format, to facilitate access under judicial decision or provision of law, subject to the guidelines set out in article 13 of this Decree.

Art. 16. Information on the security standards adopted

by application providers and Internet connection providers must be disclosed in a clear and accessible way to any interested party, preferably through their websites, subject to the right to confidentiality of trade secrets.

CHAPTER IV
SURVEILLANCE AND TRANSPARENCY

Art. 17. Anatel will act in the regulation, monitoring and investigation of infractions, in accordance with Law no. 9.472 of 16 July 1997.

Art. 18. The National Consumer Secretariat will act in the monitoring and investigation of violations under Law no. 8.078 of 11 September 1990.

Art. 19. The Brazilian Competition Defense System will be in charge of investigation of economic infractions, in accordance with Law no. 12.529 of 30 November 2011.

Art. 20. The entities and agencies of the federal public administration having specific powers with respect to the matters related to this Decree will work collaboratively, taking into consideration CGIbr guidelines, and will ensure compliance with Brazilian legislation, including on application of penalties, even if the activities are carried out by a foreign-based legal entity, as provided for in article 11 of Law no. 12.965 of 2014.

Art. 21. Investigation of infractions of Law no. 12.965 of 2014 and of this Decree will follow the internal procedures of each investigating entity and may be initiated ex officio or upon application by any interested party.

Art. 22. This Decree comes into force thirty days after the date of its publication.

Brasilia, 11 May 2016, the 195th year of Independence and the 128th of the Republic.

DILMA ROUSSEFF

Eugênio José Guilherme de Aragão

André Peixoto Figueiredo Lima

João Luiz Silva Ferreira

Emília Maria Silva Ribeiro Curi

This text does not replace the published in DOU of 11.5.2016 - Extra Edition.

CHAPTER 1

The Internet Bill of Rights as an Example of Multistakeholderism

Ronaldo Lemos

Ronaldo Lemos is the director at the Institute for Technology & Society of Rio de Janeiro (ITS Rio) and professor at the Rio de Janeiro State University's Law School. He is a member of the Mozilla Foundation Board and the Access Now Board, among others. Ronaldo earned his LL.B. and LL.D. from the University of São Paulo, and his LL.M. from Harvard Law School.

When Edward Snowden revelations hit Brazil in September 2013, following his first leaks four months earlier, the government took an immediate interest. Willing to respond quickly, the most comprehensive and feasible reaction was the so-called Internet Bill of Rights, a draft bill then under analysis in the Brazilian Congress.

What is the Internet Bill of Rights and what rights does it set forth?

The difference between the Internet Bill of Rights and other pending draft bills lies in the form of its proposal. Rather than as an initiative of the State itself, the bill was proposed by the civil society. The Bill's drafting process began years before the Snowden case, and was the product of an open and collaborative effort – one described as a Multistakeholder Process, a process which enhances democracy by increasing opportunities for effective participation by those who are directly impacted by decisions. Converted into law in April 2014, the Internet Bill of Rights sets forth a framework for the Internet. The enactment of the new law came shortly after the web's 25th anniversary and Sir Tim Berners-Lee's call for a Magna Carta for the Internet, positioning Brazil as the first country to heed that call.

From a process standpoint, as soon as it became clear that Brazil needed a bill of rights for the Internet, it also became clear that the Internet itself should be involved in drafting it. An 18-month consultation process followed, including soliciting contributions from a vari-

ety of stakeholders in a truly hybrid and transparent forum: Internet users, civil society organizations, telecom companies, governmental agencies, and universities all provided comments publicly, so that all stakeholders were able to consider one another's contributions. Ultimately, this process successfully led to a draft of a law adopted by the government and taken into consideration by the Brazilian Congress.

The final version protects rights such as net neutrality, privacy, and takes a strong stance against NSA-like practices. For instance, the use of Deep Packet Inspection at the physical layer of the connection is now illegal in Brazil. The Marco Civil, as the Bill is referred to in Portuguese, also protects freedom of expression, creating safe harbors for online intermediaries in Brazil, and determining that online platforms will have to takedown specific content when served with a valid court order[1].

The Internet Bill of Rights actually embeds multistakeholderism as a principle for Internet governance in Brazil[2]. This is important because it will influence Brazil's position regarding Internet governance at international forums, where Brazil now stands, according to law, alongside of initiatives promoting broader partic-

1 This safe harbor does not apply to infringement of copyright- related materials. Copyright has been excluded from the Internet Bill of Rights.

2 Article 24. The following are guidelines for action by the Union, the states, the Federal District, and the municipalities in developing the Internet in Brazil:
I – establishing multistakeholder, transparent, collaborative, and democratic governance mechanisms, with the participation of the government, the private sector, civil society, and the academic community.

ipation, and in opposition to trends that privilege the State's role in implementing Internet governance.

In short, the Internet Bill of Rights translates the principles of the Brazilian Constitution to the online world. It is a victory for democracy, and stands in stark contrast to other laws that were recently passed in countries such as Turkey or Russia, which expanded governmental powers to interfere with the Internet. Brazil's law is an example for countries willing to acknowledge the importance of the web in facilitating both development and a rich and open public sphere.

The Bill also includes a requirement that ISPs providing connectivity services and other Internet services retain user data for a year and six months respectively. Although criticized by privacy activists, this is significantly shorter than the five years that previously proposed.

The Internet Bill of Rights is a standard for the improvement of current practices of data retention in Brazil, which were not defined by law, but by agreements between law enforcement authorities and service providers, and were thus quite nontransparent. From start to finish, the approval of the Internet Bill of Rights took about seven years of intense debate with numerous stakeholders. The support of civil society and active participation of the Brazilian public was crucial.

A Brief History of the Project

The Internet Bill of Rights was created as part of a strong public reaction against the passing of a draco-

nian cybercrime bill in Brazil in 2007, named Azeredo Law, in reference to a Senator called Eduardo Azeredo, rapporteur and lead proponent of the bill. If the bill had been passed, it would have established penalties of up to four years in jail for anyone "jailbreaking" a mobile phone, and four years in jail for anyone transferring songs from an iPod back into their computers.

With such a broad scope (presaging SOPA and PIPA discussions in the United States years later), the bill would have turned millions of Internet users in Brazil into criminals. Moreover, it would have been detrimental to innovation, rendering illegal numerous practices necessary for research and development.

The Azeredo Law sparked broad public criticism, first from the academy, followed by strong social mobilization, which included an online petition that quickly received 150,000 signatures online. Congress took notice of the reaction and postponed consideration of the bill. However, the question of regulation remained: if a bill based on the criminal code was not the best way to regulate the Internet in Brazil, what should be the alternative? In May 2007, I wrote an article for Folha de São Paulo, the biggest newspaper in Brazil, claiming that rather than a criminally based bill, Brazil should have a "civil rights framework" for the Internet— in other words, an Internet Bill of Rights or, in Portuguese, a Marco Civil[3]. That was the first time the term appeared in public.

3 Internet Brasileira Precisa de Marco Regulatório. Folha de São Paulo. Available at: https://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm. Accessed on: 22 May 2017.

The idea took off and was endorsed by the Ministry of Justice in Brasilia. In 2008, the Ministry invited the group of professors I was then leading at Fundação Getulio Vargas to create an open and multistakeholder process for drafting the bill. It was clear from the beginning that the Internet should also be part of it.

Our team built and launched a platform for debate and for collaboration on the bill, whose archives are still available at www.culturadigital.org/marcocivil. A list of principles were proposed, among them freedom of expression, privacy, net neutrality, the right to Internet access, limits on intermediary liability, openness, and promoting innovation, all of which were supported in public debate.

Each principle developed into law, leading to the creation of specific articles of the Internet Bill of Rights, which were subsequently open to new rounds of debate. The government accepted the final draft of the bill and four ministries supported its implementation. Said ministries included the Ministry of Culture, the Ministry of Science and Technology, the Ministry of Communications, and the Ministry of Justice. The bill was sent to Congress on August 24, 2011 and was then officially implemented on April 23, 2014.

The Importance of Multistakeholderism: Mapping the Controversies in the Project

The Internet Bill of Rights political negotiation took place over many years and was extremely complex.

Ultimately, the success of the project is attributed to the multistakeholder process that guided the discussions on the bill. Furthermore, the transparency of each party's position helped reduce the possibility of asymmetric information, and facilitated negotiations and necessary compromises of those involved.

Below is a controversy map of the Internet Bill of Rights, listing the main stakeholder interests and disputes during the negotiations. This is a rough and simplistic sketch of a much more complex reality. However, it

	NET NEUTRALITY	HIGHLY ENHANCED PRIVACY	SAFE HARBOR FOR SPEECH	DATA RETENTION	FORCED DATA LOCALIZATION	SAFE HARBOR FOR COPYRIGHT	EXPRESS REMOVAL FOR REVENGE PORN
TELCOS	Against	Against	Neutral	Neutral	Neutral	Neutral	Neutral
CIVIL SOCIETY	For	For	For	Against	Against	For	Against
GLOBAL INTERNET COMPANIES	Neutral	Against	For	Neutral	Against	For	Neutral
BRAZILIAN INTERNET COMPANIES	For	Against	For	Against	Against	Against	Neutral
BROADCAST SECTOR	For	For	For	Neutral	Neutral	Against	Neutral
GOVERNMENT	For	Neutral	Neutral	For	For	Neutral	For
LAW ENFORCEMENT/ LAWYERS / FEDERAL POLICE	Neutral	Against	Against	For	For	Against	For
RESULT	PASSED	ONLY PARTIALLY	PASSED	PASSED	NOT PASSED	NOT PASSED	PASSED

helps in comprehending the disputes and the ways in which the multistakeholder process rendered them visible and their negotiation feasible.

Conclusion

The chart attempts to illustrate the complexity of the Internet Bill of Rights negotiation process, both in terms of the number of parties involved and the variety of issues under debate. In terms of substance and process, the Bill is a significant achievement for Brazil and for the global community, and represents symmetry between collaborative process and substantive results achieved so far. Similar efforts involving complex issues with multiple stakeholders can benefit from the Internet Bill of Rights achievements. However, that the term "multistakeholderism", which is currently more of a mantra than anything else, is insufficient as a concept to solve the contradictions and disputes involved in something like the Internet Bill of Rights, which required intense negotiations and compromises. Multistakeholderism is merely a helpful (and important) point from which to start. In order to achieve effective results, a much bigger effort is necessary, building bridges between the different stakeholders, avoiding radicalism and polarization, and being prepared to reach compromises—one of the main lessons learned from the Internet Bill of Rights creation process.

The Future of the Internet Bill of Rights

The Internet Bill of Rights approval is not the end of the fight. The bill faces at least two immediate challenges. The first is how the government defines the terms of its application by means of a presidential decree. Even though the decree cannot change or go beyond the law itself, it can specify how the law is to be interpreted and applied. The Decree that regulates the Internet Bill of Rights was finally issued in 2016 and the interpretation of its terms is a on-going debate concerning issues such as net neutrality and privacy protection.

The Internet Bill of Rights has already inspired other nations that are interested in following Brazil's footsteps, while other governments are already launching their own online consultation processes for writing their versions of our Internet Bill of Rights. In Europe, members of the Italian parliament have contacted the Internet Bill of Rights rapporteur, the Brazilian Internet Steering Committee (CGI.br) as well as the Institute for Technology & Society of Rio de Janeiro (ITS Rio) in order to explore a similar process. In 2015 the Italian Parliament issued a Declaration on Internet Rights[4]. Therefore, in a context in which even democracies like Turkey and Russia have started passing laws that expand governmental control over the Internet, the Internet Bill of Rights presents itself as a viable alternative. It provides a model, both in process and in substance, on how to approach Internet regulation in a way that takes democratic values into account.

4 Available at: http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf. Accessed on: 22 May 2017.

CHAPTER 2

Notes on Brazilian Internet Regulation

Sérgio Branco

Sérgio Branco has a PhD and a Master's Degree in Civil Law from the Rio de Janeiro State University (UERJ), and an Undergraduate Law Degree from UERJ. He is a guest researcher at the Centre de Recherche en Droit Publique from the Montreal University. He was a civil and intellectual property professor at Fundação Getulio Vargas (FGV Rio), from 2006-2013. In 2006, he was the Attorney in Chief at the Nacional Institution of Technology (ITI) and the academic development Coordinator of the undergraduate law school program at FGV in 2005. Sérgio has written and published a few books. Among them: Copyright in the Internet and the Use of Third Party's work; Public Domain in Copyright Brazilian Law – A Work in Public Domain; and What is Creative Commons – New Copyright Models in a More Creative World. He has undergone an extension course in intellectual property at the Pontifical Catholic University (PUC-Rio) and has an extension course in film documentary (FGV). He is one of the Co-founders and a Director of the Institute for Technology & Society of Rio de Janeiro (ITS Rio). The author would like to thank Beatriz Laus Marinho Nunes for her assistance in the research and review of this article.

The Brazilian Internet Bill of Rights encompasses a series of controversial yet necessary issues that have arisen considering the constant evolution of technology as well as the Internet. The series of articles that follow address some of the problems that resulted not only from the elaboration of the law, but also from its application. Regulating the Internet has proven to be a challenge in itself and the Internet Bill of Rights is a first step towards this goal. Thus, the articles below provide a glimpse on how the Internet Bill of Rights came into existence and some of the main controversies its application has drawn out. These include, but are not limited to, the possibility of crowdsourcing a piece of legislation, the global removal of a website and how it contributed to the regulation of the Internet, intermediary liability, net neutrality, and the right to be forgotten, all of which have been constantly present in international media.

Is it possible to crowdsource a law?

In 2015, Brazilian Congress passed 162 laws[1]. Among them, a law that honors humorists'[2], a law declaring November 16 as "national dyslexia awareness day"[3], and a law that celebrates corn day[4].

1 Portal da Legislação. 2016 – Leis Ordinárias. Available at: http://www4.planalto.gov.br/legislacao/portal-legis/legislacao-1/leis-ordinarias/leis-2016. Accessed on: 17 May 2017.

2 Law no. 13.082/2015. Available at: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2015/Lei/L13082.htm. Accessed on: 17 May 2017.

3 Law no. 13.085/2015. Available at: http://www.planalto.gov.br/CCIVIL_03/_Ato2015-2018/2015/Lei/L13085.htm. Accessed on: 17 May 2017.

4 Law no. 13.101/2015. Available at: http://www.planalto.gov.br/CCIVIL_03/_

Ideally, we would say, for societal benefit, that Legislators are elected to legislate. Some laws are easy to pass - I do not see much discussion when it comes to the best day in which to celebrate corn (which, by the way, is on May 24, according to the Brazilian law), although anything is possible. However, with the complexity of the contemporary world, subjects get more and more sophisticated, technology challenges our certainty about daily aspects of life and what once was easy to understand is now full of subtleties. To legislate the internet is surely not as easy as deciding on the best day to laud Poetry (which, out of curiosity, is on October 31)[5]. Indeed, nothing is very poetic when opposite interests are concerned.

The lack of Internet regulation in Brazil was leading to uncanny decisions. For instance, YouTube's website was taken down because of a video that, allegedly, violated a model's intimacy. Under such circumstances, it would be difficult to convince innovative Internet companies to base themselves in Brazil, considering the uncertainty of Internet regulation - the so-called "legal certainty" principle was non-existent.

However, how could we delegate to Congressmen the power to decide on the Internet's regulation, as this is such a specific issue? Considering that Congressional representatives usually don't know much about technology and those who know, are frequently out of the scope of democratic decision-making game, nothing seemed

---

Ato2015-2018/2015/Lei/L13101.htm Accessed on: 17 May 2017.

5 Law no. 13.131/2015. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13131.htm Accessed on: 17 May 2017.

more reasonable than to use the Internet to create a law to regulate itself.

The year was 2009 and technology was not as developed as it is nowadays. A partnership between a group of professors from FGV (which are now at ITS Rio) and the Ministry of Justice led to the creation of a platform where the discussion of a new law would take place from the very beginning. The platform is still available at http://culturadigital.br/marcocivil/.

During the first stage, the debate focused on ideas, principles, and values[6]. The topics in discussion were privacy, freedom of expression, intermediaries' liability, net neutrality, infrastructure, among others. Each paragraph of text-based produced by the Ministry of Justice remained accessible for a couple of months to the insertion of comments by anyone who wished to participate. Contributions from foreign countries were also included.

At the end of the first phase, the Ministry of Justice compiled the contributions and prepared the draft of a bill that would be the basis for the second part of the project[7], which occurred in the first half of 2010 and consisted of the discussion of the draft of the text itself. Again, each article, paragraph or item remained available for the submission of comments from any interested party. A summary of the offered contributions resulted in the Bill

6 Marco Civil da Internet – seus deveres e direitos em discussão. Available at: http://culturadigital.br/marcocivil/consulta/. Accessed on: 17 May 2017.

7 Marco Civil da Internet – seus deveres e direitos em discussão. Available at: http://culturadigital.br/marcocivil/debate/. Accessed on: 17 May 2017.

of Law no. 2.126/2011, sent to Congress for discussion.

The final vote on the Internet Bill of Rights, however, was postponed more than 20 times. Several were the economic interests in dispute, especially concerning net neutrality and intermediary liability. On April 23, 2014, former President Dilma Rousseff signed the Internet Bill of Rights, Law no. 12.965/2014[8], during the Net-Mundial conference, which took place in São Paulo.

As the result of this process, Brazil had a law regulating the Internet - at last. "Marco Civil" (as it is usually called, meaning "civil framework") is composed of 32 articles. The first part concerns rights, principles, and safeguards. Then, we have provisions on net neutrality, data protection, intermediaries' liability, and the role of the State.

However, as anyone can imagine, many are the problems arising from the application of the law. Its interpretation is leading to some misunderstandings, and it has not prevented hugely popular Internet apps to be taken down more than once. A brief view of the law and how the Brazilian Courts are interpreting it, is the subject of our next texts.

How a Top Model Helped Regulate Brazilian Internet

Consider the following scenario: The year was 2006. Brazilian top model and TV presenter, Daniella Cicarelli, was spending some time with her boyfriend at a beach in

8 Law no. 12.965/2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on: 17 May 2017.

Cadiz, which is located in the south of Spain. It was a beautiful day, at a public beach, with other sunbathers around. Nevertheless, the couple decided to share intimate moments while bathing in the sea. These intimate moments, recorded in detail, were subsequently shared online.

The interest in Daniella Cicarelli was not surprising - she got married to Ronaldo, also known as Ronaldo Fenômeno, one of the most famous Brazilian soccer players, just a year before. By that time, he played for Real Madrid, and she was a famous model. The marriage did not last long, but it certainly contributed to making her famous in Spain.

After the recording became popular (so popular that even street vendors had the video to sell[9]), Cicarelli decided to address her discontentment publicly. She demanded the video be taken down from all websites, including YouTube. The attempts to remove such content were, however, unfruitful. For such reason, she sued Google[10].

Cicarelli wanted the video to be taken down permanently and promptly. Google tried many times, but right after the content became unavailable, another user uploaded the video once again, and again, and so on. Frustrated due to the impossibility of getting rid of the

9 Vídeo polêmico de Cicarelli é vendido por camelôs no Rio. Terra. Published on: 24 September 2006. Available at: http://www.perfilnews.com.br/brasil-mundo/video-polemico-de-cicarelli-e-vendido-por-camelos-no-rio. Accessed on: 23 May 2017.

10 Daniella Cicarelli é coautora de ação contra YouTube. GI Tecnologia. Published on: 11 January 2007. Available at: http://g1.globo.com/Noticias/Tecnologia/0,,AA1416616-6174,00-DANIELLA+CICARELLI+E+COAUTORA+DE+ACAO+CONTRA+YOUTUBE.html. Accessed on: 23 May 2017.

video, Cicarelli requested that YouTube should be taken down, considering it could not enforce the court decision. The judge thought this was a good idea. Therefore, on the following days, YouTube was no longer available in Brazil[11]. Evidently, the results of this decision were disastrous. Civil society claimed for YouTube to become available again and two days after, the same judge annulled his first decision. However, if YouTube was there again, the truth is that the king was naked, right before everybody's eyes: Brazilian Internet needed clear rules concerning its use and its regulation.

While all these events were going on, Brazilian Congress started a debate to approve the first Brazilian Internet framework - and it would be a criminal one[12]. It was naturally a terrible possibility. If people could not agree on the responsibilities regarding the uploading of Cicarelli's video on YouTube, how could we impose criminal penalties on the involved parties?

2007 was the year during which civil society organized itself in order to discuss a civil framework for Brazilian Internet. It led to the creation of a project referred to as the Marco Civil da Internet[13], or as the Brazilian Internet Bill of Rights. This project aimed to regulate several

11 Telefônica e Brasil Telecom bloqueiam acesso ao YouTube. GI Tecnologia. Published on: 09 January 2007. Available at: http://g1.globo.com/Noticias/Tecnologia/0,,AA1412609-6174-363,00.html. Accessed on: 23 May 2017.

12 LANDIM, Wikerson. Conheça a Lei Azeredo, o SOPA brasileiro. Tecmundo. Publsihed on: 24 January 2012. Available at: https://www.tecmundo.com.br/ciencia/18357-conheca-a-lei-azeredo-o-sopa-brasileiro.htm. Accessed on: 23 May 2017.

13 Marco Civil da Internet – seus direitos e deveres em discussão. Available at: http://culturadigital.br/marcocivil/. Accessed on: 23 May 2017.

issues concerning the Internet and its varied possibilities, such as net neutrality, data protection and, naturally, intermediary liability.

However, the old traditional way of discussing bills of law was unexciting and inefficient, considering that congressional representatives are, more often than not, unwise when it comes to technological related subjects. For this reason, it seemed inevitable that the bill of law be discussed directly on the Internet, crowdsourcing the expertise of anybody who was willing to contribute. Thus, during the following years, this discussion was actively undertaken.

What are you liable for?

As mentioned above, the recording of intimate moments of a top model at the beach was one of the most relevant facts that led to Brazilian Internet regulation[14]. The upload of such video on YouTube's website triggered a national discussion on intermediaries' liability, given that we had no rules, at that time, that could clearly define if YouTube was somehow liable - and to what extent, if so - for the distribution of the recording.

After seven years of discussion, Brazilian National Congress finally passed Brazil's Internet Bill of Rights, known in Portuguese as the "Marco Civil da Internet"[15].

14 COSTA, Camilla. Por que caso de Cicarelli contra Google pode ser último do tipo no Brasil. BBC Brasil. Published on: 15 October 2015. Available at: http://www.bbc.com/portuguese/noticias/2015/10/151014_google_cicarelli_cc. Accessed on: 17 May 2017.

15 Law no. 12.965/2014. Available at: http://www.planalto.gov.br/ccivil_03/_

As one can easily imagine, defining liability for damages caused by content produced by third parties was crucial in such context. After all, the inexistence of clear rules and definitions was resulting in conflicting, and many times competing judicial decisions as well as reckless understandings (interpretations), such as the one in which a blogger is guilty due to a comment written by one of his readers[16].

During the discussion of the Internet Bill of Rights, the first system mechanism suggested in order to deal with intermediaries' liability was the notice and takedown, inspired by American law. However, civil society criticized this option because it was considered an open door to private censorship. Indeed, if websites were automatically liable for third parties' content after extrajudicial notices, they would most certainly remove the controversial content without further examination. Thus, during discussion, this hypothesis was replaced by the removal of material after receiving a judicial court order. Article 19 of Brazil's Internet Bill of Rights establishes this rule:

> Article 19. In order to ensure freedom of expression and to prevent censorship, internet application providers may only be held civilly liable for damage resulting from content generated by third parties if, after specific judicial order, the provider fails to take action to make the content

ato2011-2014/2014/lei/l12965.htm. Accessed on: 17 May 2017.

16 MANDEL, Gabriel. Blogueiro é condenado por comentário de leitor. ConJur. Published on: 24 September 2013. Available at: http://www.conjur.com.br/2013-set-24/blogueiro-condenado-comentario-ofensivo-feito-leitor. Accessed on: 17 May 2017.

> identified as offensive unavailable on its service by the stipulated deadline, subject to the technical limitations of its service and any legal provisions to the contrary.

On the other hand, because judges are overloaded by work, waiting for a judicial decision in order for an intermediary to be held liable would be, in some cases, not only inefficient but also unfair. This is why the law foresees at least one possibility of notice and takedown, after which the intermediary becomes liable, notwithstanding a court's decision:

> Article 21. Internet application providers that make available content created by third parties will be secondarily liable for violations of privacy resulting from the disclosure, without the participants' authorization, of images, videos and other material containing nudity or sexual acts of a private nature, if, after receiving notice from the participant or the participant's legal representative, the internet application provider fails to take prompt action to remove the content from its service, subject to technical limitations of the service.

Legislators considered that these cases require fast results. When we are talking about acts of private nature, it is not only a matter of goods, money and patrimonial interests – human dignity and human rights are in danger, and must be protected. For this reason, the law contains this exception. It is important to note, however, that a website is not forbidden to remove a content considered offensive or that violates its terms of use out

of its own accord. The removal can always take place. Nevertheless, the intermediary will be liable only after judicial order, unless the content relates to the ones described in Article 21.

Net Neutrality: You Love It, Even If You Don't Know What It Is.

In Brazil, the same company that provides me Internet connection is responsible for the fixed telephone service. Every time we connect to Skype, for example, we do not use the telephone line. Although quality is many times inferior, VoIP apps are far less expensive, and that is why it is worth using them. However, if telecommunication companies are losing money because we choose to use Skype instead of a telephone, why don't they just worsen the Internet connection to the point that the use of Skype becomes unfeasible, forcing users to use a fixed telephone? The answer is net neutrality.

Tim Wu[17] coined this principle, defining it as "the principle that Internet service providers and governments regulating the Internet should treat all data on the Internet the same, not discriminating or charging differently by user, content, website, platform, application, type of attached equipment, or mode of communication". In short, we could say that if "all humans are equal before the law", the correspondent parallel in Internet would be, and "all data is equal before the web".

17 See: WU, Tim. Network Neutrality, Broadband Discrimination. J. ON TELECOMM. & HIGH TECH. L. Vol.2. 2003-2004. p.141. Available at: http://www.jthtl.org/articles.php?volume=2. Accessed on: 23 May 2017.

Additionally, net neutrality may also prevent telecommunication companies from entering into agreements with content providers to benefit a website over another. For example, a company could have a financial agreement with, let's say, YouTube, so whenever a user connects to any other video platform (Vimeo, Netflix), her/his Internet connection would be so slow that this user would give up on watching the content of his interest or would look for it on YouTube. Brazil's Internet Bill of Rights[18] regulates net neutrality in the following terms:

> Article 9. The agent in charge of transmission, switching and routing must give all data packets equal treatment, regardless of content, origin and destination, service, terminal or application.
>
> §1 Traffic discrimination and degradation will be subject to regulations issued under the exclusive powers granted to the President of the Republic in Article 84 (iv) of the Federal Constitution, for the better implementation of this Law, after hearing the Brazilian Internet Steering Committee (CGI.br) and the National Telecommunications Agency (Anatel), and may only result from:
>
> I – technical requirements essential to adequate provision of services and applications, or
>
> II – prioritization of emergency services.
>
> §2. In the event of traffic discrimination or degradation, as contemplated in §1, the agent in charge must:

18 Law no. 12.965 of 2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Accessed on: 23 May 2017.

> I – refrain from causing damage to users, as provided for in article 927 of the Civil Code (Law 10.406 of 10 January 2002);
>
> II – act in a fair, proportionate and transparent manner;
>
> III – provide users, in advance, with clear and sufficiently descriptive information on its traffic management and mitigation practices, including network security measures; and
>
> IV – provide services on non-discriminatory commercial terms and refrain from anti-competitive practices.
>
> §3. Subject to the provisions of this article, the content of data packets may not be blocked, monitored, filtered or analyzed in Internet connections, either paid or free of charge, or in transmission, switching and routing.

Brazilian law protects the idea of net neutrality with two exceptions: technical requirements essential to the adequate provision of services and applications, or prioritization of emergency services. The first refers, for example, to services that need synchronous communication (VoIP and streaming) over e-mails and social networks, for instance. The second relates to public calamities or catastrophes, in which case, certain online services must prevail over others.

Despite the approval of the law and a legal regulation (as foreseen in the text above copied), a question remains unanswered according to Brazilian legislation: Is

the practice of « zero rating » legal[19]? Zero rating consists in offering « free » content to users of an Internet service provider (ISP). For example, I may use Facebook and WhatsApp free of charge depending on my ISP. «Free of charge» means that when I use such apps, the data consumed is not discounted from the total amount of data I contracted.

The issue is highly controversial. Some countries consider zero rating illegal, while other countries do not[20]. It is and will remain, at least for the next years to come, a disputable thematic. The question of whether zero rating is legal or not is one of these almost invisible concerns regarding the Internet that interests everyone, but very few are aware of.

Nine Questions on "the Right to Be Forgotten"

L. is a Brazilian professor and translator. In the 1970s, she was arrested and convicted for drug dealing in the USA. She spent two years in jail and was then released. By that time, only her family and closest friends were aware of her situation. Most of the people she knew, believed she was in a cultural exchange program. When she came back to Brazil, she led a normal life, got mar-

19 See: https://en.wikipedia.org/wiki/Zero-rating. Accessed on: 23 May 2017.

20 BODE, Karl. India Bans Zero Rating as the U.S. Pays the Price for Embracing It. TechDirect. Published on: 08 February 2016. Available at: https://www.techdirt.com/blog/netneutrality/articles/20160208/06220233547/india-bans-zero-rating-as-us-pays-price-embracing-it.shtml. Accessed on: 23 May 2017.

ried, and had children. She did not regret her misadventures in the 1970s, but she clearly became another person as time went by. Fortunately, her past was behind. That is, until Google opened it widely.

If you search for L's name on Google, you will find, on the third page of research, the judicial decision convicting her 40 years ago. It seems important to understand, now, the reasons why somebody would go to prison for drug dealing in the 1970s. Access to such information is certainly relevant to the history of law, the development of public policies, and the enhancement of criminal law and criminal procedure. However, is the exposure of her full name actually necessary? Doesn't it represent an extra burden, considering her judicial debts are already paid? What can she do, taking into account that people who have access to such information can harm her social interactions?

The term "right to be forgotten" or RTB is not new and did not appear for the first time on the Internet. In the 1960s, in Germany, we can find the roots of this discussion in a criminal case known as "Case Lebach"[21]. At the time, a man was arrested for participating in the assault of a military base and for the murder of some soldiers. After six years in prison, a TV channel decided to broadcast a documentary telling his story, emphasizing on some personal aspects of his personality, including the fact that he was a homosexual. He sued the TV channel, and the German court decided that the public

21 See: Texas Law. Case VerfGE 35, 202 Federal Constitutional Court (First Division). Available at: https://law.utexas.edu/transnational/foreign-law-translations/german/case.php?id=644. Accessed on: 23 May 2017.

exhibition of the program would impair his reinsertion in society since he was about to be released. Thus, his privacy should prevail.

Since 2014, however, the debate concerning the RTB has taken a dimension never seen before. It all began when a Spanish lawyer requested Google do delist[22] (or delink or deindex) him because, after searching for his name on Google, you would find that he had some unpaid debts in 1998. He asserted that he had paid such debts and that the information was not only outdated, but also unimportant. European Court decided in his favor and soon after, Google received more than 100,000[23] requests for delisting results in favor of an alleged right to be forgotten. Should Google accept such requests?

There are many problems arising from the implementation of such a right on the Internet. In Brazil, there are two notorious cases in which the RTB was brought up by the victims, although, curiously enough, neither of those cases involved the Internet. In one of them, one of the most influential TV channels in Brazil reenacted a terrible murder involving children, which took place in Rio de Janeiro, in 1993. During the show, they mentioned a man possibly involved in the crime. However, the Court considered him not guilty, and any reference

22 See: Google Spain v AEPD and Mario Costeja González. Available at: https://en.wikipedia.org/wiki/Google_Spain_v_AEPD_and_Mario_Costeja_Gonz%C3%A1lez. Accessed on: 23 May 2017.

23 Cerca de 100 mil pedidos de 'esquecimento' foram enviados à Google. O GLOBO. Published on: 26 July 2014. Available at: https://oglobo.globo.com/sociedade/tecnologia/cerca-de-100-mil-pedidos-de-esquecimento-foram-enviados-google-13394843. Accessed on: 23 May 2017.

to him would harm his social life once many years had passed since the crime. The TV channel was found guilty[24] because, in short, they could tell the story without mentioning his name. Thus, in this case, freedom of expression triumphed.

The second decision was the exact opposite. The same TV channel (in fact, the same TV show) reenacted the murder of a young woman[25] in 1958. Her siblings sued the TV channel arguing they went through all the suffering once again with the retelling of the story. The court decision, however, was in favor of the TV channel - the story could not be told without naming the victim, unlike the first case described above. Although unfortunate, the prohibition of referring to her name would make freedom of expression unfeasible.

After European decision, Brazilian Congress has also tried to draft bills of laws in order to regulate the RTB. However, those bills represent an attempt to privatize censorship or to increase the costs of the Internet in Brazil. In one of the proposed bills, anyone could request content removal that is irrelevant[26]; in another,

24 Superior Tribunal de Justiça. Globo terá de pagar R$ 50 mil por violar direito ao esquecimento. JUSBRASIL. Available at: https://stj.jusbrasil.com.br/noticias/100547749/globo-tera-de-pagar-r-50-mil-por-violar-direito-ao-esquecimento. Accessed on: 23 May 2017.

25 Uso de imagem de Aida Curi no programa Linha Direta não gera dano. MIGALHAS. Published on: 04 June 2013. Available at: http://www.migalhas.com.br/Quentes/17,MI179753,31047-Uso+de+imagem+de+Aida+Curi+no+programa+Linha+Direta+nao+gera+dano. Accessed on: 23 May 2017.

26 Câmara dos Deputados. Projetos de Lei e Outras Proposições. PL 7881/2014. Available at: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=621575. Accessed on: 23 May 2017.

service providers on the web should have a call center to remove any material that would fit the frame of the right to be forgotten[27].

The fact is that there is still a lot to be discussed before we can finally make a good public policy towards this subject. It seems to me that the right to be forgotten should be regarded as a very exceptional situation, to be applicable to private (or anonymous) individuals, in private spheres and for private purposes only.

Here are some questions that need addressing to better comprehend the RTB, its limits and the consequences of its application:

- Is it a real right or an extension of the right to privacy?
- Is the expression 'right to be forgotten' or 'right to be delisted' the most adequate or rather, a right to be delinked or deindexed?
- Does it refer to a public person or an anonymous individual?
- If it relates to an anonymous person, did she/he contribute to the information becoming public?
- Is there any public interest in keeping that information on the Internet?
- Is the information necessary to assure free-

27 Câmara dos Deputados. Projetos de Lei e Outras Proposições. PL 1676/2015. Available at: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1295741. Accessed on: 23 May 2017.

dom of expression?

- Is it a case of devoir de mémoir (like Nazism or historical and political issues; in these cases, not only a right to be forgotten is not applicable but there is a duty to remember);
- If the information is deleted, delisted, or deindexed, can it constitute private censorship?

Last, but certainly, most importantly:

- Who should decide in which cases a RTB is applicable? Private entities, such as Google, or only Judicial Courts?

CHAPTER 3

A collaborative and open Internet Bill: the policy-making process of the Internet Bill of Rights

Celina M.A Bottino and Fabro Steibel

Celina Bottino is a Brazilian lawyer, researcher, and General Coordinator at the Institute for Technology & Society of Rio de Janeiro (ITS Rio). She is a Harvard Law School graduate (LLM'10) with a focus on International Human Rights, and a former Kaufman fellow at Human Rights Watch.

Fabro Steibel is the Executive Director of the Institute for Technology & Society of Rio de Janeiro (ITS Rio), a professor of new technologies and innovation at ESPM Rio (Brazil), an Independent Researcher for the Open Government Partnership in Brazil, and an open government fellow at the Organization of the American States.

The Internet Bill of Rights is a unique bill for two main reasons: first, it establishes principles, rights, and duties for Internet use in Brazil in accordance with the principles of democracy; secondly, due to the policy-making process involved in its creation, debate, and approval. This article reviews these two milestones, discussing the creation of this Internet regulation and how it was achieved with the help of the Internet itself.

Coining the terminology "Internet Bill of Rights" or Marco Civil da Internet

The Marco Civil da Internet or the "Internet Bill of Rights" is a term coined in May 22, 2007, by Ronaldo Lemos, in an article published in the national press venue Folha de São Paulo. The terminology was used as a response to a bill that intended to incriminate several citizens' conducts in the online world; a cybercrime law known as Azeredo Law. Although written in 1999, this law went for congressional hearing only in 2007, and amongst its provisions, penalties of up to 4 years in prison were included for jailbreaking phones, or transferring songs from one device to another.

The term "Marco Civil" was one of many used in social media and by newspapers to indicate the opposition to the criminalization of Internet practices and used alongside other terms such as the "Digital AI-5", a reference to the most authoritarian law issued in Brazil by the Military Government in the 1960s. Azeredo Law could have turned millions of Internet users in Brazil into

criminals overnight. Moreover, many players, from inside and outside the government, were involved in supporting the overthrow of this law. A milestone, for example, was the launch of an online petition calling for a veto on the bill. This initiative received over 160,000 signatures (NOLASCO, 2014[1]), and was done by think tanks and activists such as André Lemos, a Communications professor at the Federal University of Bahia (UFBA), João Caribé, a digital activist, and Sergio Amadeu, a sociologist and advocate for free software in Brazil.

The difference between the Internet Bill of Rights and the other terms used to mobilize stakeholders is that "Bill of Rights" suggested not only an opposition against the criminalization of Internet use, but also a proposition to define rights for Internet use. As such, it mobilized not only those willing to oppose the Azeredo Law, but also those who wished to promote a bill of Internet rights. In June 20, 2008, when the Azeredo Law passed the Constitutional and Legal Commission in the Lower Chamber, the Ministry of Justice, legislative representatives of the running political party, and academics such as Ronaldo Lemos and Sérgio Amadeu, reorganized themselves around the term "Bill of Rights" in order to find ways for designing a new legislation to protect rights.

By May 2009, it was clear that without an alternative agenda, the simple opposition to the Azeredo Law would fail. Therefore, Ronaldo Lemos decided to propose a the-

1 COLEMAN, Stephen; BLUMLER, Jay G. The Internet and Democratic Citizenship: Theory, Practice and Policy.

matic discussion for a bill of Internet Rights, supported by the Ministry of Justice, who suggested using the Internet for the drafting of the bill collaboratively.

Drafting the Internet Bill of Rights

In June 2009, formal President Lula attended the 10th International Free Software Forum in Porto Alegre. In his opening speech, the formal President recognized the discontentment of social movements and acknowledged the role of cybercrime laws in the promotion of online censorship. Lula's speech provided a window of opportunity for the Ministry of Justice to collaborate with the academic institution where Ronaldo Lemos, Carlos Affonso, and Sérgio Branco worked, to propose a new framework for Internet regulation in the country, via online consultation.

The Internet Bill of Rights Consultation connected politics and technology in a way that injected some new and different elements into the relationship between representatives and represented, and governments and governed (COLEMAN; BLUMLER, 2009[2]). The online consultation occurred from October 2009 to April 2010 and had two phases: one, which focused on the principles for an Internet Bill of Rights and the other, based on the proposed law draft that would be sent to Congress. The

2 COLEMAN, Stephen; BLUMLER, Jay G. The Internet and Democratic Citizenship: Theory, Practice and Policy. April 2009. Available at: http://www.cambridge.org/br/academic/subjects/politics-international-relations/comparative-politics/internet-and-democratic-citizenship-theory-practice-and-policy?format=HB&isbn=9780521817523%22#iJm8ibeWdkdTIfUm.97. Accessed on: 4 May 2017.

technology used was a WordPress website created by the Ministry of Culture (culturadigital.br), resulting in the country's first formal online consultation. Altogether, it connected 275 authors, who submitted over 1,500 comments on how and why to regulate Internet rights (STEIBEL, 2015[3]).

The consultation, carried out online was open to all, making the debate inclusive for all Internet users. It succeeded in connecting four key elements on the regulation of the Internet:

> (1) A government institution with a real interest in direct public participation;
>
> (2) An active online community with a strong in terest on the topic under discussion;
>
> (3) An active research institution or think tank willing to bring its own expertise and influence into the project; and
>
> (4) A web 2.0 interface capable of engaging poli cy makers and citizens in a coherent narrative structure for deliberation (STEIBEL; BELTRA MELLI, 2012[4]).

The consultation also explored the benefits of support-

3 STEIBLE, Fabro; ESTEVEZ, E. Designing Web 2.0 Tools for Online Public Consultation. In: Arul Chib; Julian May; Roxana Barrantes. (Org.). Impact of Information Society Research in the Global South. First Edition.Washington: Springer, 2015, v. 1, p. 243-263.

4 STEIBEL, Fabro & BELTRAMELLI, F. Online Public Policy Consultations In: GIRARD, B. 'Impact 2.0: New mechanisms for linking research and policy'. 1. ed. 2012.

ing an open Multistakeholder Process, through which members of the public, government, global and local Internet companies, civil society, and others could engage in negotiations.

As a result, the Internet Bill of Rights Consultation was a transparent policy-making process, where participants could see the others' contributions side-by-side, and where all parties had to be transparent in order to foster an open debate. Due to this transparency policy, we were able to identify those who opposed net neutrality during the consultation process: Telcos, law enforcement agents, and global Internet companies all were against such provisions, whereas Brazilian Internet companies and the broadcast sector were neutral, and those in favor of net neutrality included the Executive branch and civil society (LEMOS; STEIBEL, 2015[5]).

The last straw

Once the consultation process ended, it was submitted, by the Ministry of Justice to the Presidency, who then sent it to Congress for appreciation on August 24, 2011. The bill faced a difficult and long approval process in Congress, but legislators eventually voted in favor of it on April 23, 2014, during the NETmundial conference.

Before being passed, the Draft Law faced regulatory

5 LEMOS, Ronaldo; de SOUZA, Carlos Affonso; STEIBLE, Fabro; NOLASCO, Juliana. A Bill of Rights for the Brazilian Internet (Marco Civil) A Multistakeholder Policymaking Case. In: GRASSER, Urs; BUDISH, Ryan; WEST, Sarah Myers (Org.). Multistakeholder as Governance Groups: Observations from Case Studies. First edition. Boston: Berkman Center, 2015, v. 1, p. 0-24.

challenges, such as the controversy surrounding the leak of nude photos of famous Brazilian actress, Carolina Dieckmann, in 2012. The story quickly became a hot topic of public gossip, and, in November of that year, there was an update to our Criminal Code in order to specify crimes committed in the digital environment. Another controversy involved Edward Snowden's revelations, confirming that Brazil was also a target of US surveillance. The evidence, brought forth during the event, energized the government's will to finally cast their votes considering the Internet Bill of Rights, determining a regime of constitutional urgency to pass the bill on September 11, 2013, which prevented Congress from voting on any other issues until the Bill of Rights vote was completed (NOLASCO, 2014[6]). On March 25, 2014, the Lower Chamber voted on the Draft bill. The event happened after several delays and rescheduled agendas. Even so, when voted, the bill kept its most controversial articles, such as the support of net neutrality, data privacy, and freedom of expression. When it reached the Senate, days later, it received more than 40 amendment requests, none of which considering major alterations were accepted when the bill was finally approved on April 22. Finally, it was enacted as Law no. 12.965/2014 (PAPP, 2014[7]).

6 NOLASCO, Juliana. Building the Marco Civil: A Brief Review of Brazil's Internet Regulation History In: STAKES ARE HIGH: Essays on Brazil and the Future of the Global Internet. 2014. Available at: http://www.global.asc.upenn.edu/publications/stakes-are-high-essays-on-brazil-and-the-future-of-the-global-internet. Accessed on: 04 May 2017.

7 PAPP, Anna Carolina. Em nome da Internet – os bastidores da construção coletiva do Marco Civil. 2014. Available at: https://issuu.com/annacarolinapapp/docs/em_nome_da_internet. Accessed on: 04 May 2017.

From Congress approval to permanent debate

The Internet Bill of Rights passed with grand political support, which was essential for its overcoming of the following year's legislation challenges. It was clear nonetheless, that the regulatory process will continue in the coming years, due to the requirement expressed in the Law, to introduce further legislation in order to regulate topics related, for example, to net neutrality.

Regarding the regulation of the bill, from January to April 2015, the Ministry of Justice opened an online consultation in the portal "Pensando Direito", contemplating three thematic topics (i.e. net neutrality, Internet privacy, and retention of access logs) and one open-for-all topic. The consultation received 1,109 contributions, in the first round[8], and other minor summaries of contributions, carried out by non-government members, in the second round of consultation (2015). A second challenge refers to the constant desire to specify Internet crimes. A bill, supporting the "Right to be Forgotten", for example, has been submitted to Congress for appreciation (draft bill no. 215/15), as well as legal reforms to reduce protection for political online criticism (draft bill no. 1589/15) and to create massive surveillance databases (draft bill no. 2390/15). All of those continue to face multistakeholderism public scrutiny, most of which used enhanced networks during the first consultation of the bill.

8 Pensando Direito. Available at: http://pensando.mj.gov.br/marcocivil/%22. Accessed on: 04 May 2017.

Conclusion

The Internet Bill of Rights, created by proposals from civil society, rather than by an initiative of the State itself, is a product of an open government initiative, where the Ministry of Justice collaborated with civil society to promote an open and collaborative effort to draft the bill, which they managed to approve together. On the year the Web celebrated its 25th birthday, Tim Bernes-Lee argued that, "through this concept of linking, the web has grown up significantly in 25 years, from a collection of interlinked static documents to a much richer environment of data, media, and user interaction"[9]. This web structure is part of what the Internet Bill of Rights encompasses. On the one hand, it refers to the architecture, which the Bill intends to regulate. As such, the Internet Bill of Rights is, as an Internet milestone, a product of interlinking data and user interaction that supports precisely what first originated it. This is how the Bill's policy-making process began, and how it continues to ring true today.

9 BERNES-LEE, Tim. Tim Berners-Lee on the Web at 25: the past, present and future. Wired. 06 Feb 2014. Available at: http://www.wired.co.uk/article/tim-berners-lee. Accessed on: 04 May 2017.

CHAPTER 4

Data Protection & Privacy in the Internet era: the Internet Bill of Rights

Mario Viola

Mario Viola is a researcher at the Institute for Technology and Society of Rio de Janeiro (ITS Rio) and is currently a research associate at the Centre for Media Pluralism and Media Freedom of the Robert Schuman Centre for Advanced Studies (European University Institute).

The Internet Bill of Rights, a Law approved in April 2014, following the Snowden Scandal[1], despite not being a general data protection law, deals with privacy and data protection in different provisions. Brazil, unlike other countries (including its neighbors Argentina and Uruguay), has yet to enact a general law on personal data protection. As of now, there are few constitutional provisions and sectorial rules, one of which is the Internet Bill of Rights. The following analysis will begin with other existing provisions on privacy and data protection available in the Brazilian legal system.

Article 5 of the Brazilian Federal Constitution establishes as fundamental rights: private life, intimacy, honor, and image rights protection. This same article guarantees the protection of other aspects of privacy (namely article 5, items XI, XII, XIV)[2], determining, in item LXXII,

1 For an overview of the Snowden Scandal see: FARRELL & FINNEMORE. The End of Hypocrisy: American Foreign Policy in the Age of Leaks. 2013. 92 Foreign Aff. p.22.

2 See: EPIC - Privacy and Human Rights 2006. An International Survey of Privacy Laws and Developments. Electronic Privacy Information Center and Privacy International. 2007. Available at: http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006.html. Accessed 09 May 2017. "Article 5 of the 1988 Federal Constitution of Brazil 1. Provides that privacy, private life, honor and the image of people are inviolable, and ensure the right to compensation for property or moral damages resulting from their violation. 2. The Constitution also holds the home as 'inviolable', and that no one may enter therein without the consent of the dweller except in the event of: blatant criminal offence or disaster; or to provide help; or, during the day, by court order. 3. Correspondence and electronic communication are also protected, except by court order for purposes of criminal investigation or criminal procedural finding of facts. 4. Access to information is ensured to everyone and the confidentiality of the source shall be safeguarded, whenever necessary to the professional activity. 5. Finally, the Constitution provides for habeas data, which guarantees certain rights:

a new judicial remedy known as the Habeas Data.

Similarly, the Brazilian Civil Code, in its article 21, established the right to privacy as a 'personality right'. Moreover, there are other laws dealing with some aspects of information privacy (data protection), besides the Habeas data[3] writ contained in the Brazilian Federal Constitution, namely the Brazilian Consumer Code[4], the Positive Credit History Act[5], the Access to Public Information Act[6], and the Brazilian Internet Bill of Rights[7].

Articles 43 and 44 of the Brazilian Consumer Code regulate the maintenance of databases and consumer files, establishing certain rights for consumers[8]. Amongst

---

a) To ensure the knowledge of information related to the person of the petitioner, contained in records or databanks of government agencies or of agencies of a public character; and, b) for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative".

3 BESSA, Leonardo Roscoe. O Consumidor e os Limites dos Bancos de Dados de Crédito. Biblioteca de Direito do Consumidor V. 25. Revista dos Tribunais. São Paulo, 2003. P.107.

4 The Complementary Law no. 105/01 regulates the exchange of negative information between financial institutions and the Brazilian Central Bank.

5 Law no. 12.414 of 2011. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm.

6 Law no. 12.527 of 2011. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

7 The Internet Bill of Rights. Law no. 12.965 of 2014. Available at: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

8 The Brazilian Consumer Code, (Law no. 8.078 of 1990) does not define personal data; however, it applies to both natural and legal persons. See Article 2: "Consumer is any individual or corporate body who acquires or uses any product or service as an end user". Unofficial translation available at: http://www.caxias.rs.gov.br/_uploads/procon/codigo_defesa_consumidor_ingles.pdf.). Accessed on: 12 May 2017.

other provisions, it recognizes the rights to access[9] and rectification[10], allowing consumers the possibility of accessing personal information stored in the database and the right to rectify it if they find any inaccuracies (Article 43, caption and paragraph 3)[11].

The other legislation that deals with information privacy issues is Law no. 12.414/2011, which regulates the creation of and access to information databases concerning payments, of either natural or legal persons, aiming to create credit history[12]. Within the data protection provisions of this Law are the definitions of sensitive data, some data protection principles (such as purpose principle) and data subjects' rights[13].

Moreover, the Law on Access to Public Information (Law no. 12.527/2011) also contains some data protection safeguards in its article 31, which restricts the access to personal information contained in governmental databases when it represents risks for intimacy, private life, honor, image, or to other freedoms and individual rights.

The Internet Bill of Rights, the so-called Marco Civil da Internet in Portuguese (Law no. 12.965/2014), contains similar safeguards as the ones mentioned above. It deals

9 Ibid. p. 413.

10 Ibid. p. 416.

11 The right of deletion is implicit, since in case there is any information in the database, which is wrong or where the storage is limit is exceeded, the consumer will be able to request the deletion of such information.

12 Law no. 12.414 if 2011. Available at: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Accessed on: 20 June 2015.

13 See article 3, §3, II and article 5.

with three different groups of provisions regarding the protection of privacy and of personal data: i) principles and users' rights; ii) log retention; and, iii) access and processing of personal data[14].

Following the approach adopted by the European Union in articles 7 and 8 of the Charter of Fundamental Rights of the European Union, the Internet Bill of Rights recognizes the protection of privacy and data protection as different rights, despite their similarities[15]. This recognition means that in some situations, although there can be no violation of privacy, it is impossible to violate the protection of personal data.

In addition, the Internet Bill of Rights refers to, in its article 3, to personal data protection and privacy protection as principles that are to be complied with when regulating Internet use. Article 8 considers the protection of privacy in communications is a necessary condition for the full exercise of the right to Internet access.

Additionally, it incorporates, in its Article 7, some data protection rights, principles, and requirements regarding the processing of personal data online. These principles and requirements include, but are not limited to the purpose limitation principle, the requirement of express consent for data processing, and the possibility for the data subject to require the full removal of his/her personal data supplied to Internet applications at

14 DONEDA, Danilo. Privacy and Data Protection in the Marco Civil da Internet (Brazilian Civil Rights Framework for the Internet Bill of Rights). Available at: http://www.privacylatam.com/?p=239. Accessed on: 20 June 2015.

15 Ibid.

the end of contract/relationship with the concerned application providers.

Finally, there are data retention provisions that pose a series of concerns regarding data protection and privacy. In that sense, a recent ruling from the São Paulo State Court of Appeals concluded that the data retention provisions of the Internet Bill of Rights have no direct or concrete effect and need specific rules[16].

The Brazilian Ministry of Justice, aware of the need to adopt implementing rules, launched an online public consultation on a Regulatory Decree Draft of the Internet Bill of Rights. Instead, however, the Ministry of Justice classified the provisions that need further implementation into four categories: i) net neutrality, ii) privacy, iii) data retention and iv) other issues[17].

After this first round of consultation, the Ministry of Justice launched a second round, asking society to present suggestions for a draft text based on the comments made during the first round. This new regulatory regime challenges all sectors that rely on the Internet for their activities, as well as raises concerns on privacy protection.

The Brazilian Ministry of Justice opened a public consultation for a general data protection bill[18] that follows,

16 The São Paulo Court of Law. Interlocutory Appeal no. 2168213-47.2014.8.26.0000. Justice who delivered the opinion: Rômulo Russo. Seventh Chamber of Private Law. Judgement occurred on 10 March 2015.

17 In May 2015, the Ministry of Justice launched a public consultation on the regulatory Decree of the Internet Bill of Rights, aiming to systematize all contributions received during the first public consultation. See: http://participacao. mj.gov.br/marcocivil/sistematizacao/. Accessed on: 20 June 2015.

18 See: http://participacao.mj.gov.br/dadospessoais/. Accessed on: 20 June 2915.

in general terms, the Directive 95/46/EC[19].

Brazil is facing an evolving scenario in terms of both data protection and Internet regulation, which started with the Snowden scandal and ended up with the approval of the Internet Bill of Rights and the appointment of a UN Special Rapporteur on the right to privacy[20], following a proposal supported by Brazil and Germany.

However, although Brazil has played an important role in fostering the debate on privacy protection in an international scenario, it still needs to establish the necessary comprehensive legal framework at a national level for ensuring a proper environment for the protection of privacy and personal data. The Internet Bill of Rights was a first step in that direction and the public consultation on the data protection bill – and its presentation to the National Parliament – were attempts to involve society in this debate and to define the future directions of privacy and data protection in the country. Now, it is up to the members of the parliament to decide which direction we will take in that respect[21].

---

19 There are also two bills of law under discussion in the Brazilian Senate aiming at regulating the processing of personal data: PLS 330/2013 and PLS 181/2014.

20 See: See http://www.ohchr.org/EN/HRBodies/SP/Pages/HRC29.aspx. Accessed on: 29 September 2015.

21 Currently, there are three data protection bills pending in the National Parliament – two of which are in the Lower House and one of which us in the Senate.

CHAPTER 5

Internet Intermediaries Liability: an overview of the Internet Bill of Rights

Carlos Affonso Souza

Carlos Affonso Pereira de Souza has a PhD and a Master's Degree in Civil Law from Rio de Janeiro State University (UERJ). He is a Law professor at UERJ and at Pontifical Catholic University (PUC-Rio), where he teaches Law & Technology, Contract Law, and History of Law. Carlos Affonso is a visiting researcher at the Information Society Project from Yale Law School. He is a member of the Copyright Commission at Rio de Janeiro Bar Exam Institute (OAB/RJ). He is a Consultant at the Brazilian Internet Observatory, an initiative from the Brazilian Internet Steering Committee (CGI.br). He is one of the Co-founders and a Director of the Institute for Technology & Society of Rio de Janeiro (ITS Rio).

The Internet Bill of Rights (Law no. 12.965/2014) seeks to establish "principles, guarantees, rights, and obligations for the use of the Internet in Brazil", according to its first article. During the online consultation that led to the creation of this law, the provisions regarding Internet intermediaries' liability were one of the most intensively debated by all participants, highlighting how the application of a specific liability regime could affect the enjoyment of rights such as freedom of expression and privacy, as well as innovation and copyright protection.

Law no. 12.965/14 provides two different regimes, which depend on whether the intermediary falls into the category of connection/access providers or application providers.

Access Providers

To hold the access provider liable for the acts of its users is a practice rejected by national and international courts since the late nineties.[1] There are two main arguments used to recognize the lack of responsibility of connection providers for the damages caused by third parties, which are simply using their services to connect to the Internet.

The first argument lies in the technical impossibility on the part of providers to avoid harmful behaviors of its users. It is noteworthy that this preventive conduct

1 See: Religious Technology Center v. Netcom OnLine Communication Services, Inc. 21.11.1995. In Brazil, among other decisions, see: TJRS, Ap. Civ. nº 70001582444, Judge Antônio Correa Palmeiro da Fontoura, 29.05.2002.

of connection providers is not only impossible, but also undesirable, since it would inevitably result in an increase in mass surveillance practices of controversial legal compliance.

The second argument transcends the technological aspect by focusing on the rupture of any link (nexo causal) between damages caused to third parties and the act of simply providing Internet access to the user. The simple act of providing Internet connection does not seem to be the direct and immediate cause of the damage suffered by a victim. The direct cause of damage would be the specific behavior of the user that created the illegal content. The Internet Bill of Rights echoes such arguments in Article 18, as it exempts connection providers from liability for the actions of its users:

> Article 18. Internet connection providers shall not be held liable for civil damages resulting from content produced by third parties.

It is important to point out that the exemption set forth in Article 18 only applies to cases in which the provider would be held liable for a third party conduct. Connection providers are still liable for the damages they cause directly through their own activities, as provided by a large pool of cases decided in national courts. Among those cases are situations involving damages to their own users, such as the failure to provide services dully contracted or rendered in different conditions than the ones previously established by contract or by the relevant sectorial regulation.

Application Providers

Article 19 of the Internet Bill of Rights establishes the regime for Internet application providers' liability. The article begins with a reference to freedom of expression and states that the chosen liability regime is set in force "to prevent censorship". Such choice of words highlights the importance of defining a liability regime that recognizes the role of intermediaries as vehicles that allow for freedom of speech on the Internet, and at the same time, that it avoids creating excessive burdens for intermediaries, creating incentives for private censorship.

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

The Internet Bill of Rights determines that the general rule for intermediaries' liability in Brazil is based on the fault of the provider. By doing so, it denies attempts to hold them liable in typical strict liability standards, either by the simple availability of harmful content based on the risk theory or on the rendering of a defective service.

While the Internet Bill of Rights evades strict liability[2],

2 It is important to point out that the Supreme Court of Argentina decided that Internet application providers should not be held liable by a strict li-

the approach it provides for the liability based on fault is quite different from the usual liability arising out of the simple lack of action after notification that damages have occurred due to the availability of certain material (a notice and takedown regime).

Here lies perhaps one of the most heated controversies of the law, since the Internet Bill of Rights provides that intermediaries would only be liable if they fail to comply with a court order requesting the removal of certain content.

One of the most frequent criticisms to such provision is that Internet Bill of Rights would only allow content removal by a court order. However, that is a common misinterpretation of the aforementioned provision. What the Bill sets forth is the safeguard of application providers, meaning they will only be held liable if they fail to comply with a court order requesting the removal of the offensive material. However, the provision does not prevent intermediaries from determining their own requirements for content removal once notified by the alleged victims for damages arising out of content made available through their platforms. Such requirements are usually contemplated in their respective Terms of Services or Use, and, therefore, content might be removed because the provider recognizes that a specific

---

ability regime as well. The decision, which uses the Brazilian Internet Bill of Rights as one of its references, concerned the claims brought by Maria Belen Rodriguez against Google over Plaintiff´s photos displayed under Google search. The decision is available at:http://www.telam.com.ar/advf/documentos/2014/10/544fd356a1da8.pdf. For comments on the decision, see: PAVLI, Darian. Case Watch: Top Argentine Court Blazes a Trail on Online Free Expression. Available at: https://www.opensocietyfoundations.org/voices/casewatchtopargentinecourtblazestrailonlinefreeexpression.

photo, video, or text is indeed infringing its own Terms.

Nevertheless, in order to avoid creating incentives for private censorship, providers are not obliged to do so. The reason for such determination is due to the fact that the infringing nature of a specific content might be a very subjective matter, and also because the Internet Bill of Rights recognizes that the Judiciary Power is the competent authority to determine whether a content is in fact illicit or not.

In this sense, the Internet Bill of Rights gives freedom of expression a high stance in this debate, guaranteeing providers with an immunity that neutralizes any concern that they might have on liability for the lack of content removal once notified[3].

Judicialization and its effects

The Internet Bill of Rights fosters the understanding that an intermediary should not be compelled to remove a content simply because a notification has been received. The provision of Article 19 creates incentives for the claim to be brought to the Judiciary.[4]

3 As mentioned by André Zonaro Giacchetta, analyzing the text while on debate in the National Congress: "The text of the Draft Bill clearly favors the guarantee of users Internet rights, instead of restricting their liberties. This is a standard created for the user in good faith. There is a clear choice for ensuring freedom of thought and expression, as well as the privacy of Internet users and the protection of personal data". In: A Responsabilidade Civil dos Provedores de Serviços de Internet e o Anteprojeto de Reforma da Lei n. 9610/98. Revista da Associação Brasileira da Propriedade Intelectual, n. 117. p. 39).

4 See: THOMPSON, Marcelo. The Insensitive Internet – Brazil and the Ju-

One recurrent argument in this regard is the fact that the speed in which contents are copied and shared in the Internet is not compatible with the time it takes for a lawsuit to be brought to the Judiciary. On the other hand, it is important to stress that the Internet Bill of Rights expressly provides that a judge may order the removal by granting the victim an injunction in cases in which it is clear that the delay in taking the content down would worsen the victim's situation.[5] In order to make this solution easier and faster for the victim of a damage, the Internet Bill of Rights states that such cases can be brought to the Special Small Claims Courts. The provision of the third paragraph of Article 19 references cases of "compensation disputes for damages arising from content made available on the Internet related to honor, reputation, or personality rights, as well as the removal of related contents by Internet application providers".

The balance that the Internet Bill of Rights strives to achieve aims at accommodating the interests at stake. By doing so, it attempts to protect freedom of expression by clearly defining where the provider stands and ensuring that they must play a prominent role in the prevention and elimination of damage, so that this result will not be achieved through arbitrary judgments or mere fear of future liability.

dicialization of Pain. Available at: http://www.iposgoode.ca/wpcontent/uploads/2010/05/MarceloThompson-TheInsensitiveInternet Final.pdf. Accessed on: 12 May 2017.

5 See: LEONARDI, Marcel. Responsabilidade Civil dos Provedores de Serviços na Internet. Brasília: Juarez de Oliveira. p.207.

If the situation is brought to a Court, the Internet Bill of Rights recognizes the Judiciary as the most appropriate forum for the resolution of such cases. At the same time, an interesting side effect of the Bill is the fostering of continuous initiatives toward the capacity building of judges on the evolution of modern technologies for information and communication as such knowledge is crucial for the exercise of their functions.

In affirming that application providers must only be held liable in cases in which fault is found, and not by simply failing to comply with a notification, the Internet Bill of Rights distinguishes itself from the case law that has been construed in the last decade in Brazil, especially by the Superior Court of Justice (STJ).

One year after being in force, a clear result of the Internet Bill of Rights is the debate in the Superior Court of Justice regarding the necessity of the Plaintiff to inform the URL under which the infringing content is displayed. Law no. 12.965/14, in its Article 19, first paragraph, states that: "Under the penalty of nullity, the judicial order referred to above must clearly and specifically identify the offensive content, so that the material may be located unequivocally". Recent case law in the STJ confirmed the necessity of having the URL informed as to comply with the mentioned legal requirements.[6]

6 STJ, Especial Appeal no. 1512647/MG, Justice Luis Felipe Salomão, 13 May 2015.

Two exceptions to the liability regime

Law no. 12.965/14 has two important exceptions to the general liability regime, as described in Article 19: copyright infringement, as provided by the second paragraph of such article, and cases of so-called revenge porn, provided by Article 21.

In both cases, the general rule that intermediaries may only be held liable if they fail to comply with a court order, demanding the removal of the content is not applicable. The two hypotheses, for very different reasons, could trigger the provider's liability if it is notified, but still fails to remove a specific content.

Copyright

The exception concerning copyright was due to a continuous demand, especially by radio and television broadcasters. The demand was for the Internet Bill of Rights not to change the established practice of sending out notifications for the removal of copyrighted material made available without proper authorization or in circumstances not protected by the exceptions and limitations regime, as set forth by the Copyright Act (Law no. 9.610/98). Brazilian courts have recognized several times the liability of the application provider when, once notified, it fails to remove the content.

An additional circumstance explains why such exception was inserted in the review process of the original text of the Internet Bill of Rights during the National

Congress. The Federal Government, through the Ministry of Culture, has been developing a consultation process for the Copyright Act reform, dealing with topics such as liability for copyright infringements carried out online. In this regard, the removal of further considerations on liability through copyright infringement would prevent the existence of two different regimes for the very same issue in Brazil: one in the Internet Bill of Rights and the other as provided for an eventual reform of the Copyright Act.

It is worth noting that the Internet Bill of Rights has not simply deferred the treatment of such matter to the Copyright Act. The second paragraph of Article 19 of Law no. 12.965/14 states that the Copyright Act should tackle the regulation of online copyright infringement, while still conditioning that such treatment must "respect the freedom of speech and other guarantees provided for in Article 5 of the Federal Constitution."

The final part of this provision is quite revealing, since one of the guidelines of the Copyright Act reform is to achieve a better balance between copyright and other fundamental rights, such as access to knowledge and freedom of expression, while hindering abusive conducts in copyright enforcement. In this sense, the Internet Bill of Rights advances in some of the concerns of the Copyright Act reform, as envisioned by the Ministry of Culture, already setting an interpretive clause to whichever solution is adopted in the reform of the specific law.

Revenge Porn

The second exception is the provision of Article 21 for cases of revenge porn material. The provision, added during one of the last rounds of editing of the bill, was motivated by the suicide of two Brazilian girls after intimate adult videos were shared through WhatsApp. A number of Congressmen have referred to this case as the trigger for creating an exception to the general rule on intermediaries' liability.

> Art 21. Internet application providers that make available content created by third parties will be secondarily liable for violations of privacy resulting from the disclosure, without the participants' authorization, of images, videos, and other material containing nudity or sexual acts of a private nature, if after receiving notice from the participant or the participant's legal representative, the Internet application provider fails to take prompt action to remove the content from its service, subject to technical limitations of the service.
>
> §1. Under the penalty of nullity, the notice referred to in this article must contain elements that permit the Internet application provider to identify the specific material alleged to violate the participant's right to privacy and to determine that the person making the request has a lawful interest to do so.

Article 21 creates a different liability regime from that of the general rule in Article 19 for the cases in which the application provider fails to remove material that

falls into the category presented above. It is important to highlight that the final part of the provision conditions this exceptional liability to the evidence that the providers have not acted in a diligent manner ("take prompt action"). This section, together with the addition of the expression "technical limitations of the service" could provide an opportunity for discussion in the forthcoming lawsuits on what would be the standards for providers to act when they are notified of intimate material, such as the ones targeted by this provision, made available through their applications.

CHAPTER 6

Internet Intermediaries' Liability: A North American Perspective

Florian Martin-Bariteau

Florian Martin-Bariteau, LL.D., is an Assistant Professor of Law and Technology at the Faculty of Law, Common Law Section, and the Director of the Centre for Law, Technology and Society at the University of Ottawa. In 2015, he was an Internet Policy Global Fellow at the Institute for Technology & Society of rio de Janeiro (ITS Rio). He holds a Doctor of Law (LL.D., egregia cum laude) from Université de Montréal as well as a License in Law (cum laude) and a Master in Intellectual Property and Information Technology Law (cum laude) from the Université d'Aix-Marseille.

The Brazilian Internet Bill of Rights established a brand new framework for Internet intermediaries' liability regarding third parties' content and activities. As explained in the previous chapter[1], the new Act provides for generous legal safe harbours to the benefit of Internet access providers and Internet application providers while also framing two derogatory regimes for revenge porn and copyright.

This chapter compares the Internet Bill of Rights with both Canadian and U.S. frameworks and establishes that the Brazilian federal legislator is not the first to set different frameworks for varying matters, such as revenge porn and copyright. As the liability scheme for copyright infringement has yet to be designed, a comparison with Canada and the United States is particularly of interest. Indeed, the two North American jurisdictions have adopted different approaches to the matter. This chapter argues that Brazil should frame the upcoming copyright scheme following Canada's notice-and-notice approach, considering it is the only one to be consistent with principles set by the Brazilian Internet Bill of Rights.

As such, this chapter will only focus on legal frameworks advanced by statutes and case law. It should be borne in mind that the discussed provisions, while designing safe harbours for intermediaries, doesn't render them mandatory. Certainly, access and applications providers are free to provide for other mechanisms

1 See the previous chapter "Internet Intermediaries Liability: an overview of the Internet Bill of Rights".

through their terms of use, notably to streamline their process across jurisdictions. It is worth clarifying that the chapter will only consider intermediaries' liability with respect to the content of third parties – also known as "user-generated content" –, i.e. content they didn't directly author or actively contribute to.

A Common Principle: Intermediaries Are Not Liable for Users' Actions

As a matter of principle, the Brazilian legislator, in the Internet Bill of Rights, rejected the idea of holding Internet intermediaries liable on behalf of their users. According to Article 18, Internet access providers are not liable for content transiting through their networks. Similarly, Article 19 provides that, in order to ensure freedom of expression and prevent censorship, Internet applications providers shall not be held liable for user-generated content. That immunity continues even after they have been notified and made aware of the illegality of any content. Under the Brazilian Internet Bill of Rights, the only way to take down illegal content is through a court order, which, according to Article 22, shall indicate the exact material in question and its location by means of the URL. Only when a provider does not comply with the court order ruled under Article 22 will it be held liable for its users' actions and content. Of course, as previously stated, the provider can still specify, in its terms of use, its ability to takedown of any illicit content that would violate established standards without a prior court order. They are not legally

required to do so by the statutory provisions.

With such safe harbours, Brazil attempted to prevent the abuse of takedown notifications, avoid an uncompetitive legal burden for providers and, refrain from transferring decisional powers – generally entrusted to judges – over issues involving freedom of expression and other civil liberties to private actors. Undeniably, the idea of ensuring freedom of expression and preventing censorship pervades Section III of the Internet Bill of Rights and exudes from provisions framing the implementation of the judicial takedown.

To make sure Brazilians can defend themselves against abusive requests, Article 20 stipulates that the intermediary shall notify the user of any court order or legal challenge regarding its content. The provision aims to allow the user to bring a defense in court. Also, in order to achieve greater transparency, Article 20 § 1 additionally requires that a notice – explaining that the content has been taken down or displaying the court order – shall replace the illicit material.

Comparison with the United States of America

The approach followed in the Brazilian Internet Bill of Rights is very similar to the one set by the United States since the adoption of the Federal Communication Decency Act (CDA) of 1996. Despite the Act's title and its original purpose to restrict speech, the CDA provides a general immunity framework for intermediaries re-

garding third-party content[2]. According to Section 230 (c) (1) of the CDA, "[no] provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider". Therefore, Internet service providers cannot be held liable for any third parties' content – of course, they are immune from content they authored or in which they made an active contribution. It is worth noting that, intellectual property, notably copyright (as will be elaborated on later)[3], and federal criminal prosecutions fall outside the scope of this safe harbour.

Comparison with Canada

In Canada, the issue is considered differently even though the framework is still very ambiguous. Oddly enough, the court has not established strong and clear case law, nor has the federal legislator passed any statute on that matter, except in relation to revenge porn and copyright – as will later be discussed.[4]

Notwithstanding, Canadian common law has established a notice and takedown safe harbour for intermediaries consistent with the underlying principles shared by the Brazilian and U.S. frameworks. The Supreme Court of Canada set the cornerstone of the common law framework in 2004 in SOCAN v. CAIP [5]. The majority

2 47 US Code § 230.

3 See previous chapter

4 See previous chapter

5 SOCAN v. Canadian Association of Internet Providers, 2004 SCC 45.

actually relied on the 1891 precedent set in Electric Despatch v. Bell[6] on the immunity of telecommunications operators in regards to third party usage and referred to the general notice and takedown scheme provided under the European Union's Directive on electronic commerce[7]. Accordingly, intermediaries should not be held liable for content made available or acts performed by third parties on their network if they have no control or input over it. They are not required to monitor illicit content and practices; however, after proper notification, hosting providers should take down illicit content or stop the pursuit of illicit activity. Failing to do so, they will fall outside the scope of the safe harbour. Even though SOCAN v. CAIP was a copyright case, it should be considered as the common law framework. Indeed, the Supreme Court of Canada stated those principles in a general matter – not just in relation to copyright – and have since reaffirmed them outside of the copyright context[8].

The silence of the federal legislator is sometimes justified by Canadian federalism and its division of powers, as provinces should be the ones regulating civil liabilities. Nonetheless, provincial legislators did not author the framework, with the notable exception of Québec. In 2001, with An Act to Establish a Legal Framework

6 Electric Despatch Co. of Toronto v. Bell Telephone Co. of Canada, (1891) 20 SCR 83.

7 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, [2000] O.J. L. 178/1, Preamble, clauses 17, 19, 22, 42, art. 3(1) and 13(1).

8 See: SOCAN v. Canadian Association of Internet Providers, 2004 SCC 45 (with general and specific languages); Crookes v. Newton, 2011 SCC 47; Reference re Broadcasting Act, 2012 SCC 4.

for Information Technology[9] (ALFIT), the civil law province designed a unique statute providing intermediaries with a safe harbour. Under Section 22 of the ALFIT, intermediaries are not responsible for content hosted or transmitted on their networks by third parties. Additionally, Section 36 affords providers with immunity regarding the acts performed by third parties through their network or services. In addition, under Section 27, access and service providers are not required to monitor their networks and infrastructure to detect illicit content.

However, contrary to the CDA and the Brazilian framework, providers fall outside the scope of the safe harbour for not promptly blocking access to the content or preventing the pursuit of the illicit activity when they become aware of it. It is worth underlining that the mechanism differs from traditional notice and takedown as providers are not required to take down content upon notification, but rather solely when they are certain of its unlawfulness. Another difference is that their liability is engaged once they are made aware of the illicit content by anyone or by any circumstances that make the illicit use apparent, not just by notice from those whose rights were infringed.

Coping with Revenge Porn

While opting for a principle of intermediaries' immunity, Brazilian lawmakers decided to cope differently with revenge porn and designed, within the same Internet

9 CQLR, c. C-1.1.

Bill of Rights, a specific derogatory notice and take-down scheme for that type of privacy breach. Article 21 of the Internet Bill of Rights provides that intermediaries will be held liable for the breach of privacy arising from the disclosure of materials containing nudity or sexual activities if, upon notification, such content is not taken down in a diligent manner. To avoid general notifications and not impose an excessive burden on intermediaries, a Section-21 notice shall state the exact location and, contrary to Québec's ALFIT framework, can only be issued by the victim or by the victim's own legal representative.

Comparison with the United States of America

In the United States, the federal law did not provide specific provisions regarding revenge porn materials. Admittedly, more than 25 states have enacted statutory provisions criminalizing, at least as a misdemeanour, the publication of revenge porn materials. However, Section 230 of the Communication Decency Act clearly states that the immunity prevails over any States' legislation[10]. Therefore, under the current statutory provisions, and in the absence of federal criminalization of revenge porn, Internet intermediaries cannot be held liable for not taking down such illicit content.

Comparison with Canada

If Canada has yet to clarify a general framework, the

10 47 US Code § 230(e)(3).

Protecting Canadians from Online Crime Act of 2014[11] enacted specific provisions criminalizing revenge porn, which considered intermediaries' liability and implemented a notice and takedown safe harbour mechanism[12]. Within Section 162.1 (a) of the Criminal Code[13], the Act created a specific criminal offence for the publication of intimate images of a person without his or her consent. Under the new section, not only those who publish the material will be found guilty of the offence but also any person "who knowingly [...] distributes, transmits, [...] makes available or advertises" such content. Arguably, this provides intermediaries with a notice and takedown safe harbour for which knowledge is the threshold. Internet access and service providers will not be liable as long as they are unaware of the offensive material. However, once alerted or given notice by any means, the provider must take down the content or risk a criminal conviction. Copyright Act, RSC 1985, c. C-42, s. 31.1(6) with s. 27(2.3).

Dealing with Copyright Infringement

Besides revenge porn, the Internet Bill of Rights sets a second derogatory scheme that could trigger intermediaries' liability where content infringes copyright and other related rights. According to Article 19 § 2, the general framework shall not apply to copyright and the relevant regime will be subject to specific provisions

11 SC 2014, c. 31.

12 Ibid, s. 3.

13 RSC 1985, c. C-46.

within the upcoming copyright reform. However, the new Copyright Act is still in the making ... and therefore the intermediaries' liability framework regarding copyright infringement by third parties has yet to be designed. Certainly, Article 31 of the Internet Bill of Rights provides that, until then, the current framework continues to govern the issue. However, the current Copyright Act nor any other federal statute provide for such a framework! As Brazilian courts have previously ruled in favour of a notice and takedown safe harbour[14], it is believed that, in the meantime, Internet intermediaries will not be held liable for user content, if they take it down upon notification[15].

Comparison with the United States of America

In the United States, the Online Copyright Infringement Liability Limitation Act of 1998, Title II of the well-known Digital Millennium Copyright Act[16], provides for an exception to Section 230 of the CDA with respect to copyright and related rights for hosting providers and search engines. However, other intermediaries, such as caching[17], network and access providers[18], remain im-

14 Carlos Affonso Pereira de Souza, "Responsabilidade civil dos provedores de acesso e de aplicações de Internet: evolução jurisprudencial e os impactos da lei no 12.695/2014 (Marco civil da Internet)" in George Salomão Leite and Ronaldo Lemos (eds.), Marco Civil da Internet (Atlas, 2014), 791.

15 See previous chapter.

16 Digital Millennium Copyright Act, Pub. L. 105-304, 112 Stat. 2860.

17 17 US Code § 512(b).

18 17 US Code § 512(b).

mune from liability for infringement if they did not author or interfere with the content.

The Digital Millennium Copyright Act enacts a strict notice and takedown safe harbour with respect to copyright infringement. According to Section 512 (c), hosting providers are not liable for copyright infringement by third-party content if they do not have actual knowledge of the content and, upon notification, expeditiously remove or disable access to it. A similar safe harbour for information location tool providers, i.e. search engines, is provided for under Section 512 (d).

Under both safe harbours, the provider is requested to take down the alleged illicit content upon notice without respect to the merits – and cannot be held liable for takedowns, notably abiding freedom of expression or fair use. Nevertheless, Section 512 (g) provides that intermediaries shall promptly notify users that the content has been taken down. The users can then send a counter-notification of non-infringement. From that time, the rights holder has 10 days to file a lawsuit seeking a court order against the user; if he fails to do so within the 10 days, the intermediary shall reinstate the content within the 14 days following the receipt of the counter notification.

This "notice and put back" mechanism was established to protect users from abuse and unlawful claims. However, as the alleged illicit content shall be taken down upon notification, it leaves room for frivolous notices leading to the removal of legitimate content. More often than not, users will be afraid to challenge legal claims

made by rights holders and will just drop the case.

Comparison with Canada

To address the challenge for freedom of expression, Canada decided to follow another path in its Copyright Modernization Act of 2012[19]. The updated Copyright Act[20], which last provisions came into force January 1, 2015, provided for a safe harbour for intermediaries and designed a one-of-a-kind "notice and notice" framework to protect users from false claims of infringement, and protect freedom of expression against unnecessary takedowns of legitimate content. Because of the uniqueness of the new provisions, the Canadian framework is often presented as the next-generation approach, striking a balance between all stakeholders' interests, from rights holders to users.

As a matter of principle, under Section 31.1, network, caching, and hosting providers can't be held liable for copyright infringement by third parties, unless the service is primarily for the purpose of copyright infringement[21]. However, under subsection 31.1 (2), caching providers will fall outside the scope of the safe harbour if, other than for technical reasons, they modify the content or interfere in its transmission. In addition, concerning hosting providers, subsection 31.1 (5) provides that the safe harbour will not apply if the intermediary

19 SC 2012, c. 20.

20 RSC 1985, c. C-42.

21 Copyright Act, RSC 1985, c. C-42, s. 31.1 (6) with s.27 (2.3).

is aware of a court order stating that the content or the use infringes rights. Contrary to Article 19 of the Internet Bill of Rights, the court order does not need to require the removal of the illicit content. Finally, Section 41.27 states that an Internet location service used as a search engine, and found to have infringed copyright by reproducing or communicating protected works, rights holders are not entitled to any remedy other than an injunction to remove the content.

If the safe harbour is, after all, quite similar to Article 19 of the Internet Bill of Rights, Canada innovated it with an ancillary "notice and notice" mechanism, inspired by the voluntary system in place within the music industry and intermediaries before the copyright reform. Under Sections 41.25 and 41.26, rights holders can send a notice of infringement to intermediaries, which shall then be forwarded to the infringing third parties. Providers shall also retain records that will allow the rights holders to present evidence of the infringement in court and discover the infringer's identity. Interestingly, costs supported by the intermediaries to notify the users can be invoiced back to right holders for reimbursement. It is worth noting that an intermediary who fails to comply with the notice-and-notice obligations will not fall outside Section 31.1's safe harbour but could be ordered to pay from $5,000 to $10,000 in damages to the rights holder[22].

This unique framework was quite unexpected as the Supreme Court of Canada called the legislator to design

22 Copyright Act, RSC 1985, c. C-42, s. 41.26(3).

a "notice and takedown" framework in 2004[23]. On the other hand, the Federal Government and Parliament believed that a "notice and notice" mechanism would have a sufficient deterrent effect. Moreover, while protecting legitimate uses, the mechanism isn't denying rights holders of any protection for copyright on the Internet as they still can file a lawsuit.

If the federal framework is quite clear, it should be noted that some doubts remain in relation to possible overlap with Québec's ALFIT. Indeed, some wonder whether providers located in Québec, or who are dealing with its rights holder, are subject to Section 22 of the ALFIT regarding copyright infringement, in addition to the Copyright Act framework. Under the federal paramountcy doctrine, the federal statute shall prevail over the provincial statute. Though both could coexist as provisions of the Copyright Act more closely resemble an exception, rather than immunity. As such, the ALFIT would not be inconsistent and incompatible with the federal safe harbour[24]. However, Courts still need to rule on that matter, as the wording of the federal statute is quite unclear.

The Future of the Brazilian Copyright Framework

With the upcoming copyright reform, Brazilian lawmakers will have to choose between a "notice and take-

23 SOCAN v. Canadian Association of Internet Providers, 2004 SCC 45, at 127.

24 A similar position was held by the Supreme Court of Canada in Rothmans, Benson & Hedges Inc. v. Saskatchewan, 2005 SCC 13, at 22-23 (regarding tobacco legislations).

down" scheme like in the United States and the European Union, or the Canadian innovative "notice and notice" framework. It is argued the latter exhibits the most consistency with the general philosophy underlying the Internet Bill of Rights.

Indeed, Article 19 § 2 calls for a specific implementation for copyright, i.e. a framework that follows a similar approach, and not for a new and different framework, as is the case with revenge porn. In the same vein, the Act specifies that the upcoming copyright framework shall "respect the freedom of speech and other guarantees provided for in Article 5 of the Federal Constitution".

A "notice and notice" framework would be very consistent with the general provisions of Article 19, simply adding specific mechanisms without deviating from the philosophy underlying the Internet Bill of Rights. As previously stated, a "notice and notice" framework also ensures a better protection of freedom of speech than possible abuses of the "notice and takedown" mechanism.

While protecting the freedom of speech and ensuring that rights holders can still go to court, the "notice and notice" framework, if correctly outlined, may further citizens' education regarding protected content and the limits of their conduct on the Internet. In fact, in the first months of its implementation in Canada, we saw a decrease in downloading and file sharing, with a sway toward legal streaming.[25]

25 Internet Security Task Force, "Six Strikes And You're (Not Even Close To) Out; Internet Security Task Force Calls for End of Copyright Alert System" (Press release), PR Newswire (May 12th, 2015). Available at: http://prn.to/1SiyYiA. Accessed on: 29 May 2017.

The Rule of Contract and the Notice and Takedown

On paper, intermediary compliance seems complex and risky, as legal frameworks appear to be as diverse as jurisdictions and types of content. However, the reality is quite the opposite. As we explained in the introduction, the legislation only sets the minimum requirements for Internet intermediaries and protects them through statutory safe harbours. Therefore, the opportunity to choose more stringent frameworks still remains. In the United States, Canada or even in Brazil, most of the providers have actually added self-designed "notice and takedown frameworks" within their Terms of Use; even outside the realm of copyright provisions. Together with notice-and-notice, this framework may actually be the best deal for protecting rights holders, users and intermediaries. Providers will take down obvious illegal content but will require court orders for the removal of uncertain content, notably those benefiting from protection under fair use, freedom of expression or freedom of information.

Summary of Internet Intermediaries' Liabilities

	Brazil	United States	Canada	Québec
ILLEGAL CONTENT (OTHER THAN COPYRIGHT INFRINGEMENT OR REVENGE PORN)	No liability until court order	No liability	Case law provides for Safe Harbour through Notice and Takedown	Safe Harbour through Notice and Takedown
COPYRIGHT INFRINGEMENT	Case law provides for Safe Harbour through Notice and Takedown	Safe Harbour through Notice and Takedown	No liability until court order	Safe Harbour through Notice and Takedown
REVENGE PORN	Safe Harbour through Notice and Take Down	No liability	Safe Harbour through Notice and Takedown	Safe Harbour through Notice and Takedown

CHAPTER 7

Transatlantic Perspectives on the Internet Bill of Rights

Daniel Arnaudo and Roxana Radu

Daniel Arnaudo is a Cybersecurity Fellow at the University of Washington's International Policy Institute where he has collaborated on projects in Seattle, Brazil and Myanmar. He was an Internet Policy Global Fellow at the Institute for Technology & Society of Rio de Janeiro (ITS Rio) in 2015. His research focuses on Internet governance, cybersecurity, and information and communication technologies for development (ICT4D).

Roxana Radu is a Research Associate at the Programme for the Study of International Governance at the Graduate Institute in Geneva. She was an Internet Policy Global Fellow at the Institute for Technology & Society of Rio de Janeiro (ITS Rio) in 2015. Her current research focuses on new modes of governance for global Internet policy-making.

Since its passage in 2014, the Internet Bill of Rights is no longer a reference only within Brazil. The law has become an example of collaborative effort to enshrine a set of rights and obligations for the online world. It is inspiring similar discussions in various contexts that are propagating connections throughout Europe, the United States and around the world. Among its many effects, it created momentum for consolidating support for an Internet Magna Carta - proposed by Tim Berners-Lee, inventor of the World Wide Web - similar to the Great Charter of Liberties, a law passed in England in 1215, and finally transformed into statute law in 1297, guaranteeing basic rights and freedoms.

Having started as an experimental initiative, the Internet Bill of Rights reached the Brazilian Congress at a time of prolonged political crisis following massive protests in 2013. Mobilized online, the crowds were initially spurred by exorbitant World Cup preparations, but the protests reflected a larger dissatisfaction in society over corruption, a lack of public services and rising prices, amongst other grievances[1]. Almost simultaneously, a contractor for the U.S. National Security Agency (NSA), Edward Snowden, leaked documents that showed the global reach of the American intelligence apparatus online[2]. Its programs especially targeted Brazil's net-

1 WALDRAM, H. Brazil protests continue as story develops over social media. The Guardian. Published on: 21 June 2013. Available at: http://www.theguardian.com/world/2013/jun/21/brazil-protest-social-media. Accessed on: 15 May 2017.

2 WELCH, C. Brazil allegedly targeted by NSA spying, demands explanation from United States. The Verge. Published on: 07 July 2013. Available at: https://www.theverge.com/2013/7/7/4501896/brazil-targeted-by-nsa-spying-demands-united-states-explanation. Accessed on: 15 May 2017.

works, from the President's office to the state owned oil company Petrobras, to the Internet Exchange Points that manage most of Latin America's traffic. With an election looming, former President, Dilma Rousseff responded by making the Internet Bill of Rights her government's top priority.

In this context, the Internet Bill of Rights passed into law in April 2014 alongside the inauguration of a new international initiative called the NET-Mundial. From the beginning, the government consciously linked the national and international structures of Internet governance. Domestically, this passage generated hopes of permeating the rather rigid political rule making with civil society-driven, participatory initiatives. It was the first consultation conducted entirely online in Brazil, a country that had more than 1,000 law proposals mentioning the word 'Internet' between 1995-2014[3].

Internationally, signing the Internet Bill of Rights collaborative outcome document into law – with a number of amendments – was publicly celebrated at the Global Multistakeholder Meeting on Internet Governance (Net-Mundial) event in São Paulo. The first of its kind, NET-Mundial added to a number of efforts to increase Brazil's visibility as a key actor in Internet governance discussions, among which the UN General Assembly resolution introduced on 07 November 2013 (co-sponsored with Germany, adopted by consensus on 18 December 2014), on digital privacy. While the NET- Mundial has

3 STEIBEL, Fabro. O portal da consulta pública do Marco Civil da Internet. 2014. In: LEITE, George; LEMOS, Ronaldo (Coords.) Marco Civil da Internet. São Paulo. Editora Atlas, p. 18-28.

faced challenges to its legitimacy and organization[4], there is no doubt that the Internet Bill of Rights provides principles for other countries to follow in both their own domestic systems and in organizing the governance of the Internet globally. What follows is an examination of how these principles have been reflected in the American and European contexts.

United States

In general, Americans are not familiar with the Internet Bill of Rights, unless they are Internet governance researchers in academia or foreign policymakers in Washington, DC. However, the Internet Bill of Rights relates to the U.S. in two ways. The first is in terms of domestic policy connections. The U.S. is grappling with the same problems concerning Internet governance as Brazil and on a similar grand scale. The second is in terms of its foreign policy, and how Brazil's position on Internet governance internationally, chiefly through the NET-Mundial initiative, connects with the goals of the U.S. It is worth examining both domestic and international linkages between Brazil and the birthplace of the Internet to understand how Internet governance operates in both contexts.

4 MCCARTHY, Kieren. International effort to wrangle t'Internet from NSA fizzles out in chaos. The Register. Published on: 04 March 2015. Available at: http://www.theregister.co.uk/2015/03/04/netmundial_council_meeting_cancelled_again/. Accessed on: 15 May 2017.

Domestic Linkages

Two essential principles of the Internet Bill of Rights reverberate in the United States. The first is network neutrality, an Internet governance concept that has struck a chord in both countries, as well as in other contexts around the world. Originally coined by the American legal academic Tim Wu, network neutrality dictates that all traffic should be treated equally, from one end of the network to the other, and has historically been a central tenet of online architecture going back to the creation of the Internet[5]. People are rightly curious on how their Internet access is provided and would like it to be in a fair, open and transparent fashion, and while the Internet Bill of Rights has made this a right in Brazil, in the U.S., events have taken a different course.

There is no easy way to make a constitutional change that would ensure neutral access to the Internet as a right, as it is now in Brazil, because network neutrality is part of Internet Bill of Rights. A similar right would require a constitutional amendment process through the approval of two thirds of Congress as well as over 38 states. However, under former President Barack Obama, the US Federal Communications Commission (FCC), which is responsible for regulating telecommunications in the United States, made changes to the 1934 Communications Act, to regulate Internet Service Providers (ISPs) as they do telephone companies, that is, as

5 WU, Tim. Network Neutrality, Broadband Discrimination. Journal of Telecommunications and High Technology Law. Vol. 2, p. 141, 2003. Available at SSRN: https://ssrn.com/abstract=388863. Accessed on: 15 May 2017.

"common carriers". This designation requires them to treat ISPs more like utilities providing a service equally, and gives them an entry to enforce network neutrality and ensure equal access in the same way that a telephone company needs to provide the same connection to any phone number.

Public comments drove the FCC's authority to make unprecedented changes in the way it governs the U.S. Internet by switching ISPs from regulation under Title I of the Act as "information service providers" to "common carriers" under Title II. A request for comments on the proposal to change the regulation of ISPs to enforce net neutrality drew over four million responses on the FCC website, shutting it down for a period of time, which eventually led the commissioner, a former telecom lobbyist, to change his position and vote in favor of the reclassification[6]. Under President Trump, this principle is again being challenged. His new FCC commissioner has suggested that he will scrap the Open Internet Order that mandated ISPs as common carriers and potentially move them back under Title I, but new proposals are already drawing similarly forceful inline responses[7].

Online collaborative and democratic governance methods are the second major way in which Americans can

6 LOHR, Steve; RUIZ, R. Rebecca. F.C.C Approves Net Neutrality Rules, Classifying Broadband Internet Service as a Utility. The New York Times. Published on: 26 Feb 2015. Available at: https://www.nytimes.com/2015/02/27/technology/net-neutrality-fcc-vote-internet-utility.html?_r=0. Accessed on: 15 May 2017.

7 BRODKIN, Jon. Flooded with thoughtful net neutrality comments, FCC highlights "mean tweets". ARS Technica. Published on: 15 May 2017. Available at: https://arstechnica.com/tech-policy/2017/05/most-fcc-commenters-favor-net-neutrality-but-you-wouldnt-know-it-from-ajit-pai/. Accessed on: 16 may 2017.

relate to the Internet Bill of Rights, a law that the public edited and developed through an online and open source tool. The process created the law but also embedded the principles that created it within the constitution. Democratic and collaborative governance through the Internet is now a part of the Brazilian Federal law.

In Brazil, this mandate has helped to create further public commentary systems such as the Ministry of Justice's requests for comments on corruption or participa.br, a website maintained by the President's office to gain public input on issues, especially on network neutrality. In both U.S. and Brazilian cases, net neutrality has become both the catalyst and the means of drawing online participation, and while we have different federal governance systems in place, it is important to note the role that this principle plays in driving larger changes in both process and policy.

International Movements

The second track of the American perspective is international, stemming from the Brazilian government's NET-Mundial initiative to encourage international dialogue on the Internet Bill of Rights and its multistakeholder Internet governance model, embodied by its Internet Steering Committee. The U.S. government originally developed and hosted the research network that became the Internet in partnership with universities and private companies, and its stewardship of the domain name system reflects this history. At first, the U.S. government directly managed these "Critical Infor-

mation Resources"[8] and later controlled them indirectly through its designation and continued control of the International Corporation of Assigned Names and Numbers.

Governments, civil society organizations and some companies punished the U.S. to complete the transition of its authority over ICANN's Internet Assigned Numbers Authority (IANA), which allocates blocks of IP addresses to regional Internet registries and manages the domain name systems that give countries, governments and organizations the .com suffix and a number of others. IANA and this system are part of a larger debate over the governance of international networks. This has traditionally been one dominated by the United States, but other countries have rightly questioned this arrangement as the size and importance of the Internet have grown and it has become a completely global network, which has put the U.S. on the defensive in terms of defending the status quo and resisting change.

Edward Snowden's revelations, in June 2013, also put the U.S. on the defensive about surveillance policy and added points to the argument that it should hand over greater control of the root level infrastructure to international bodies like the UN or its International Telecommunications Union. This eventually led to the U.S. announcing that it would give up control of the domain name system and support the transition to an international multistakeholder system of governance[9]. Brazil,

8 DeNardis, Laura. Hidden Levers of Internet Control. 2012. Information, Communication & Society, 15:5, 720-738. Available at: http://dx.doi.org/10.1080/1369118X.2012.659199. Accessed on: 15 May 2017.

9 FARIVAR, Cyrus. In Sudden Announcement, US to Give Up Control of DNS

one of the key points in the international network infrastructure and an influential Latin American government, was one of the major targets of the NSA's online surveillance systems and a major part of the push to change the U.S. government's control of the system. In reaction to the 2013 revelations, former President Dilma Rousseff cancelled a state dinner, gave a scathing anti-surveillance speech at the United Nations, and ordered her government to develop policies to encourage domestic technology development and build infrastructure to route traffic outside of the U.S.[10]. The scandal also became a major catalyst in making the Internet Bill of Rights a priority and cornerstone of Brazilian domestic policy, which brought it to a vote and passage in 2014[11].

The result has been to insert Brazil into the global debate on Internet governance as it pushes to bring the principles of the law, as well as its multistakeholder model, to the world through its NET-Mundial initiative. American diplomats have been publicly supportive up to a point, happy that Brazil is taking a larger role in global affairs and providing cover for it to champion democratic Internet governance principles that do not

---

Root Zone. ARS Technica. Published on: 14 March 2014. Available at: https://arstechnica.com/tech-policy/2014/03/in-sudden-announcement-us-to-give-up-control-of-dns-root-zone/. Accessed on: 15 May 2017.

10 WOODCOCK, B. On Internet, Brazil is beating US at its Own Game. AL-JAZEERA. Published on: 20 September 2013. Available at: http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html. Accessed on: 15 May 2017.

11 WATTS, J. Brazil to Legislate on Online Civil Rights Following Snowden Revelations. The Guardian. Published on: 01 November 2013. Available at: https://www.theguardian.com/world/2013/nov/01/brazil-legislate-online-civil-rights-snowden. Accessed on: 15 May 2017.

come from the U.S., now widely mistrusted in the wake of Snowden's revelations. Paradoxically, the NET-Mundial, which the U.S. government under Obama broadly supported, comes from a law that passed only thanks to a policy shift in the Brazilian government, spurred by an anti-American reaction.

Europe

Europe is currently in a 'digital' turmoil, trying to create a distinct regulatory space for Internet activity and business. With its recently launched Digital Single Market and the planned reform of the Data Protection Regulation, the European Union has taken a proactive stance to drive areas of global Internet regulations[12]. At the same time, in the aftermath of the Snowden revelations, transatlantic relations were disrupted, as in the case of Brazil and the US. When former President Rousseff called for domestic data centers during her response to the scandal and in her push for the Internet Bill of Rights, that idea also resonated among European leaders. German Chancellor Angela Merkel went as far as proposing the creation of a European communications network[13], which was subsequently dropped.

12 RADU, R. & CHENOU, J. Data control and digital regulatory space(s): towards a new European approach. 2015. Published on: 30 June 2015. Internet Policy Review, 4(2). DOI: 10.14763/2015.2.370. Available at: https://policyreview.info/articles/analysis/data-control-and-digital-regulatory-spaces-towards-new-european-approach. Accessed on: 15 May 2017.

13 Data Protection: Angela Merkel Proposes Europe Network. BBC News. Published on: 15 February 2014. Available at: http://www.bbc.com/news/world-europe-26210053. Accessed on: 15 May 2017.

At a domestic level, a number of parliamentary initiatives tackling rights and duties online have spurred. As an example, the report on Rights and Liberties in the Digital Age, by the "French Commission de Réflexion sur le Droit et les Libertés à L'âge du Numérique", the work of Bundestag's committee on the Digital Agenda in Germany, or the Declaration of Internet Rights, in Italy. A similar initiative was discussed in the UK at the proposal of Liberal Democrat leader, Nick Clegg.

On 28 July 2015, Italy became the first European country to introduce an (European) Internet Bill of Rights, prepared and released by the Committee on Internet Rights and Duties of Italy's Chamber of Deputies, after public consultation. As with similar practices in the U.S. and Brazil, this is the outcome document of a process started in August 2014 by the Commission and opened to public consultation from October 27, 2014 to February 27, 2015. The draft declaration was opened for public consultation on the Civici platform, where the work of the country's Commission on Constitutional Reforms is also published, but it attracted limited interest. In total, the draft was accessed 14,000 times and received 590 comments over four months.

Differently from the Brazilian Internet Bill of Rights, the Italian initiative is not backed by a legislative process[14]. Thus, it remains a political statement that raises

14 ZINGALES, Nicolo. Diritti e piattaforme: mettiamo la Dichia- razione dei Diritti di Internet in prospettiva. Media Laws. Published on: 12 February2015. Available at: http://www.medialaws.eu/diritti-e-piattaforme-mettiamo-la-dichiarazione-dei-diritti-di-internet-in-prospettiva/. Accessed on: 15 May 2017.

awareness – and hopefully shapes policies and behavior – around a number of critical guarantees covered in 14 articles, among which the right to Internet access, the right to online knowledge and education, the protection of personal data, right to informational self-determination, and right to anonymous speech. It stresses a participative approach to governing the Internet[15], calling for the involvement of 'all those concerned' to be promoted by public institutions.

The document adopts an explicit European approach, referring in its preamble to Article 8 of the EU Charter of Fundamental Rights as enshrining the 'greatest constitutional protection of personal data'. It also sees the right to be forgotten in light of the 2014 EU Court of Justice decision against Google Spain as the right to delisting citizen data in search engine results. While Brazil is still grappling with the 'right to be forgotten' discussed in two recent legal initiatives (no. 7881/2014 and no. 1676/2015), in Italy there is disagreement that the scope of the article is not broad enough to cover removal from source sites[16]. The Italian text also specifies that the 'right to neutral access to Internet is a necessary condition for the effectiveness of the fundamental rights of the person', thus essentially grounding net

15 BELLI, Luca. Dichiarazione dei diritti in Internet: cuius regio eius religio? Media Laws. Published on: 19 February 2015. Available at: http://www.medialaws.eu/dichiarazione-dei-diritti-in-internet-cuius-regio-eius-religio/. Accessed on: 15 May 2017.

16 BASSINI, Marco. Né costituzione né legge. La Dichiarazione dei diritti in Internet verso una missione culturale. Media Laws. Published on: 28 July 2015. Available at: http://www.medialaws.eu/ne-costituzione-ne-legge-la-dichiarazione-dei-diritti-in-internet-verso-una-missione-culturale/. Accessed on: 15 May 2017.

neutrality in the fulfilment of basic rights. This interpretation – though ambiguous – goes further than the (more specific) net neutrality rules adopted in the EU at the end of June, derived from a consumer approach.

Moving from the domestic to the supranational level, the different European initiatives in Italy, the UK, France and Germany coalesce through the collaboration of politicians and invited experts including academics, journalists, and representatives of the telecoms industry and of consumers' associations. In the Italian case, the jurist and politician Stefano Rodotà became a key figure behind the proposal, known for supporting a 'constitution for the Internet' back in 2006 and for heading the Italian privacy authority. In Brazil, the Internet Bill of Rights consultation process started with a similar proposal, with the legal academic Ronaldo Lemos, heading it during an editorial in 2007[17], but was ultimately driven by civil society, government and private actors, while garnering strong support from different social movements, making its ultimate development organic rather than top-down. The process itself is important in terms of ownership and collaborative drive.

The original intention behind the work of the Italian Committee on Internet Rights and Duties with this Declaration is not confined to national boundaries, however. Its preamble suggests that it aimed to create a European framework, and to provide the Italian people with 'the constitutional foundation for supranational

17 LEMOS, Ronaldo. Internet Brasileira Precisa de Marco Regulatório Civil. UOL Notícias Tecnologia. Published on: 22 May 2007. Available at: https://tecnologia.uol.com.br/ultnot/2007/05/22/ult4213u98.jhtm. Accessed on: 15 May 2017.

principles and rights'. Welcomed at this stage, the Declaration was discussed at the 10th annual meeting of the Internet Governance Forum, in Brazil, in November 2015, hoping to create international consensus around fundamental rights and obligations online.

Concluding remarks

The Magna Carta of the 13th century in England had a long-lasting impact on constitutional rights and guarantees. It was, romanticized at times. This danger is also true for initiatives similar to the Brazilian Internet Bill of Rights that do not turn into law, and remain only political statements. It is too early to evaluate what these recent initiatives might lead to in Europe, but not too early to recognize that turning political declarations into timely pieces of legislation needs a stronger commitment. The value of Internet Bill of Rights rests as much in the process as in the outcomes and preserving some of that spirit in propagating this model may bring about legitimacy.

In the United States, there is no direct connection between the Internet Bill of Rights process and the efforts to reform domestic telecom regulation as in the nascent Italian law, but there are a number of important similarities between the symbiotic work to enforce net neutrality and the online democratic systems that drive reforms in both countries. Internationally, the NET-Mundial movement has drawn both American and European attention and created a new point of reference within global Internet governance debates with a model Internet Bill of Rights and domestic Internet governance system for others to follow.

CHAPTER 8

What is revenge porn and how can I protect myself?

Chiara Antonia Spadaccini de Teffé

translated by Beatriz Laus Marinho Nunes

The original text, titled "Pornografia de Vingança: como se proteger?", is available at: https://feed.itsrio.org/pornografia-de-vingan%C3%A7a-como-se-proteger-eb16307b426.

Chiara de Teffé is pursuing a Doctorate Degree in Civil Law at Rio de Janeiro State University (UERJ). She has a Master's Degree in Civil Law from UERJ, having written and defended her dissertation in 2016, entitled "The Protection of the Human Image on the Internet: from the identification of the damage to its compensation". Chiara is currently a Researcher at the Institute for Technology & Society of Rio, a Civil Law Professor at the UFRJ and a lawyer.

Beatriz Laus Marinho Nunes holds a Law Degree from Fundação Getulio Vargas (FGV Rio, 2016) with the thesis Impressão 3D: mapeamento de problemáticas (3D Printing: examining legal implications), and is currently attending a post-graduate extension program on Intellectual Property at Pontifical Catholic University (PUC Rio). Beatriz is currently a Researcher at the Institute for Technology & Society of Rio de Janeiro (ITS Rio).

The practice of exchanging nudes[1] has become something of a trend among teens as means of spicing up the relationship as well as a form of provoking the other partner. However, while this practice stimulates desire and sexual freedom, it also endangers the rights to privacy and image of the person depicted in the photos.

The human body is a place for freedom and not coercion; it is a space for existential self-determination and expression of the personality. The exchange of images that depict a person in a sensual position is entirely supported by the principle of freedom of expression and reflects an aspect of the existential autonomy. However, due to the alarming number of women who are unduly exposed on the Internet, it has become necessary to rethink the existing legal standards in order to provide more protection for victims of this harmful practice.

Revenge pornography (or simply revenge porn) occurs when someone shares or leaks via websites, apps or emails intimate images (photos or/and videos) containing nudity or depicting a sexual act. These images or contents, registered or sent in confidence to the partner, are shared without consent of at least one of the people therein portrayed, subjecting him/her to undue exposure and embarrassment. The ultimate objective of revenge porn is to embarrass and humiliate the person exposed in the photos before his/her friends, family and

1 The term "nudes" comes from the English word "nude", which means: naked or undressed. In Brazil, the expression "manda nudes" or "send nudes" has become popular and is used by the person who wants to receive sensual images of his or her partner.

coworkers. As a rule, the offender's intention is to get revenge on someone who has hurt his or her feelings or ended a relationship.

One must not forget that consent is contextual. The consent given by a woman to someone she trusts to take or receive an image of her containing intimate content cannot be extended as to allow this trusted person to share it with others. Consent given for existential acts has a specific purpose and is directly related to the established relationships. Therefore, the understanding that the person who sends an intimate image concurs culpably for damages in the event of exposure of these images on the Internet is highly mistaken.

What form of protection do victims of revenge porn receive from Brazilian legislation?

In Brazil, there is not a specific penal norm that punishes the practice of revenge porn. Thus, victims of revenge porn claim they suffered slander or defamation or they try framing the described conduct in other criminal norms, depending on each specific case.[2] However, when the victim is a minor, there is a legal specification in the Child and Adolescent Statute ("ECA", Law No. 8.069/1990). Article 241-A to Article 241-E encompass the

2 There are a few draft bills in proceedings that aim to regulate the unauthorized disclosure of intimate images, such as Draft Bill No. 5.555/2013, which provides for the creation of a specific criminal type for cases of disclosure, by means of image, videos or any other means, of material containing nudity scenes or sexual acts of private nature.

conduct of such an offender. As an example, a decision pronounced at the Court of Justice of Minas Gerais stated that: "Commits the crime foreseen in article 241-A of the ECA who publishes or even discloses, via sharing, in his/ her personal Facebook page, naked photos of a fourteen-year-old"[3]. According to the rapporteur, the disclosure of images or videos on the Internet, providing free access and continuous exposure of the child's or the adolescent's image, should be vehemently restrained and cannot be treated as a simple joke.

In a civil framework, once the offender has been identified, he/she will have to indemnify the victim for moral and/or material damages. It seems reasonable that aside from the original offender, those who subsequently shared and sent the image to others, increasing the extent of the damages, also be held liable. In this case, the moral damage is configured in re ipsa: the misuse of the image is evident and so is the intent to cause damages, violating the victims' dignity. In addition, the victim may also request the exclusion of the content considered harmful. This request should be directed to the person who effectively inserted the material and/or to the internet applications provider responsible for the space in which the material was shared.

After the intimate image is released and subsequently shared, the victim should save all messages and publications related to the content, as well as print screens of everything made available online, saving each spe-

3 TJMG. Lawsuit No. 1.0447.14.000413-9/001. Appellate Judge Júlio Cezar Guttierrez. Trial date: 26 August 2015. Published on the Official Journal on 01 September 2015.

cific uniform resource locator (URL) and date of access to the content in question. The next step is to file a Police Report at the Police Station. It is also recommended that the victim preserve the evidence of the suffered damages by requesting a notarial minute, as a record of the damages endured online. This record will include the URLs indicated by the victim, the date and time the content was viewed and a description of the occurrence with print screens of images, websites and other content. In Brazil, the notarial minutes have high probative force. Article 6, III, of the Law No. 8.935/94 foresees that notaries are responsible for authenticating facts. Thus, if a certain website is taken down or if the image or video is deleted, the necessary information is still safely documented. If proving the offender's identity poses a challenge, the victim can judicially request the IP addresses used by the offender as well as some personal information, in accordance with article 22[4] of the Internet Bill of Rights.

The Internet Bill of Rights and the protection of revenge porn victims

Article 19 of the Internet Bill of Rights (Law No. 12.965/2014)[5] establishes, as a rule, that after a specific

4 Art. 22. In order to obtain evidence for use in civil or criminal proceedings, the interested party may apply to the court, as an incident to a main proceeding or in a separate proceeding, for an order compelling the party responsible for keeping Internet connection logs or Internet applications access logs to produce them. §1. In addition to other legal requirements, the application will not be admissible unless it contains the following: I – good grounds to suggest that an unlawful act was committed; II – good reason to believe that the requested logs will be useful as evidence or for purposes of investigation; and III – the period to which the records relate.

5 Also translated as: Brazilian Civil Rights Framework for the Internet ("Marco Civil da Internet").

judicial court order the internet applications provider must remove, within the scope of its technical limits and deadline, the content found harmful.[6] One of the exceptions to this rule is the case of revenge porn. Article 21 of the Internet Bill of Rights determines that if the content questioned consists of images, videos or other materials depicting nudity or sexual acts of a private nature, the internet applications provider will have to remove such content after receiving an extrajudicial notification. Because it concerns revenge porn, the internet applications provider has the duty to remove all the indicated content, after receiving the extrajudicial notice, under the penalty of liability for the violation of privacy. However, said extrajudicial notice must be sent by the victim or by his or her legal representative. The notification must specifically indicate the harmful

6 Art. 19. In order to ensure freedom of expression and prevent censorship, Internet applications providers may only be held civilly liable for damages resulting from content generated by third parties if, after specific judicial order, the provider fails to take action to make the content identified as offensive unavailable on its service by the stipulated deadline, subject to the technical limitations of its service and any legal provisions to the contrary. §1. Under the penalty of nullity, the judicial order referred to above, must specifically identify the offensive content for the unequivocal location of the material. §2. This article will apply to violations of copyright and related rights only when specific legislation to that effect is adopted; the legislation, when adopted, must respect the freedom of expression and other guarantees provided for in article 5 of the Federal Constitution. §3. Actions dealing with damage reparation resulting from content related to the claimant's honor, reputation or personality rights made available on the Internet, or with Internet applications providers' removal of such content, may be brought before small claims courts. §4. The court may grant the relief requested in the complaint on a preliminary basis, in whole or in part, if there is unmistakable proof of the facts and after considering the public's interest in making the content available on the Internet, as long as the claimant shows that his claim is prima facie good and that there is reason to believe that irreparable harm, or harm that would be difficult to repair, would occur if the relief was not granted in advance.

content used to violate the privacy of the victim to allow for clear identification of the images that should be removed from the web. The notification will also verify the legitimacy of the request.

It is important to highlight that Article 21 is applicable to cases involving revenge porn, but also extends to other related issues. This is so because the legislator makes no reference to the motive or reason that led the offender to disclose the content. It is known that the disclosure of intimate contents may occur either by an ex-partner who refuses to accept the end of a relationship or by any other person who may not even have a close relationship with the victim, such as hackers or work colleagues.[7]

With the increasing usage of mobile network and applications for delivering and sharing messages and images through mobile phones, the challenge of protecting an individual online has become even greater. Files containing harmful content can be stored not only in a company's server, but also in personal mobile phones. Therefore, any user can reinsert such content online at any given time. Thus, the power to control the potentially harmful content ends up with those who share or receive the content, rather than with companies responsi-

7 Some perpetrators are not motivated by revenge or any other negative feeling towards their victims. Thus, it is more correct to say that Article 21 of the Internet Bill of Rights protects victims of "non-consensual pornography", which is defined as the distribution of "sexually graphic images of individuals without their consent and includes both images originally obtained without consent as well as images consensually obtained within the context of an intimate relationship". (Cyber Civil Rights Initiative. Available at: https://www.cybercivilrights.org/faqs/) Revenge porn may be understood as a kind of non-consensual pornography.

ble for social networks or apps. People should be aware that exposing and sharing intimate third party related contents can result in serious harm to the exposed person. There is a need for educating people in this sense and showing them the repercussions of such actions. Bodily autonomy and sexual freedom go hand in hand. These rights must be encouraged and not repressed.