



DIGITAL RIGHTS: LATIN AMERICA AND THE CARIBBEAN

EDUARDO MAGRANI (EDITOR)

**DIGITAL RIGHTS: LATIN AMERICA
AND THE CARIBBEAN**

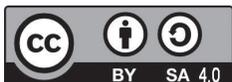
Edition produced by FGV Direito Rio
Praia de Botafogo, 190 | 13th floor
Rio de Janeiro | RJ | Brasil | Zip code: 22250-900
55 (21) 3799-5445
www.fgv.br/diretorio

**DIGITAL RIGHTS: LATIN AMERICA
AND THE CARIBBEAN**

EDUARDO MAGRANI
EDITOR

FGV Direito Rio Edition

Licensed in Creative Commons BY-SA 4.0



Printed in Brazil

1st edition finalized in May 2017.

This book was approved by the Editorial Board of FGV Direito Rio, and is in the Legal Deposit Division of the National Library.

The opinions expressed in this work are the authors' responsibility.

Coordination: Rodrigo Vianna, Sérgio França e Thaís Mesquita

Book cover: Andreza Moreira

Layout: Andreza Moreira

1st proofreading: Marcia Glenadel Gnanni

2nd proofreading: Thaís Pol

Ficha catalográfica elaborada pela Biblioteca Mario Henrique Simonsen/FGV

Digital rights: Latin America and the Caribbean / [Editor] Eduardo Magrani. - Rio de Janeiro : Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2017. 238 p.

Inclui bibliografia.

ISBN: 978-85-63265-85-2

1. Direitos humanos. 2. Direito à privacidade. 3. Proteção de dados. 4. Liberdade de expressão. 5. Internet. 6. Direitos autorais. 7. Movimentos sociais. 8. Direito e informática. 9. Crime por computador. I. Magrani, Eduardo. II. Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas.

CDD - 341.27

CONTENT

INTRODUCTION	13
---------------------------	-----------

1 PART

PRIVACY AND DATA PROTECTION	21
--	-----------

Mapping the protection of privacy	22
--	-----------

Juan Carlos Iara

Privacy and security, the Latin American way	24
---	-----------

Claudio Ruiz

Privacy and surveillance in Ecuador	26
--	-----------

Carlos Correa

The friction between transparency and personal data protection in Peru	27
---	-----------

Miguel Morachimo

Your fingerprint for a kilogram of flour: biometric and privacy in Venezuela	30
---	-----------

Marianne Díaz

Private profiles in public places	33
--	-----------

Dennys Antonialli, Francisco Brito Cruz and Mariana Giorgetti Valente

Personal data, companies and the cloud: are we ready for it?	35
---	-----------

Valeria Milanés

The dangerous ambiguity of communications encryption rules in Colombia	38
---	-----------

Juan Diego Castañeda Gómez

SECRET shakes up Guatemalan society	41
--	-----------

Renata Avila

2 PART

FREEDOM OF EXPRESSION	43
------------------------------------	-----------

An opinion in favor of freedom of expression on the Internet	44
---	-----------

Eleonora Rabinovich and Atilio Grimani

Freedom of expression violations on the online environment	46
---	-----------

Heloisa Padija, Julia Lima and Laura Tresca

Paraguay: democracy and freedom of expression in digital justice ..	48
--	-----------

Yeny Villalba and Natalia Enciso

A key tool in the struggle for a free Internet	55
---	-----------

Ramiro Álvarez Ugarte

Freedom of expression on the Internet: opportunities and challenges for Latin America	57
--	-----------

Eleonora Rabinovich

Spam elections	59
-----------------------------	-----------

Eduardo Magrani

Why obliging self-identification is wrong for freedom of information	60
---	-----------

Gregory Michener

Guidelines for freedom of expression on the Internet in Latin America	64
<i>Alexandre Henrique Saldanha</i>	
Political Internet censorship: a reality in Mexico (with a little help from the United States and GoDaddy.com)	65
<i>Luis Fernando Garcia</i>	
Documenting Internet blocking in Venezuela	68
<i>Marianne Díaz Hernández</i>	
Toward freer lands on the Internet	71
<i>Maria del Pilar Sáenz</i>	
Online censorship is latent in Chile	75
<i>Paz Peña</i>	



REGULATION

Chilean bill on personal data protection is a setback for people and businesses	78
<i>Alberto Cerda</i>	
Peru's controversial law on cybercrime	80
<i>Eduardo Alcocer Povis</i>	
The use of drones in Chile and DAN 151: innovation regulations are necessary, but insufficient	83
<i>Valentina Hernández</i>	
Personal data: awaiting a text	85
<i>Paulo Rená da Silva Santarém</i>	
Civil Rights framework for Internet use: Brazil at the peak of Internet regulation as warrantor of rights	88
<i>Marina Pita</i>	
Digital regulation challenges for the new government of Chile	91
<i>Francisco Vera</i>	
Human Rights as a bargaining chip: the case of #LeyTelecom	94
<i>Francisco Vera</i>	
“Digital Argentina”: regulation and future?	96
<i>Santiago Marino</i>	
Draft Bill 215/2015, infanticide to the newly-born digital rights in Brazil.	98
<i>Bruno Ricardo Bioni</i>	
The Internet in Mexico, two years after #ReformaTelecom	100
<i>Carlos Brito</i>	
How we learned to stop worrying and love the ban	104
<i>Miguel Morachimo</i>	
A new Internet geography for Cuba	107
<i>Eliocer Cutiño</i>	
From the cassette to ‘the package,’ or how to do streaming without Internet in Cuba	113
<i>Regina Coyula</i>	

4 PART

INTERNET GOVERNANCE **117**

Internet and statecraft: Brazil and the future of Internet governance 118

Carolina Rossini

Could Brazil become the leader in Internet governance? 121

Claudio Ruiz

Mexico discusses Internet governance 123

Israel Rosas

The region is preparing for the Internet governance forum 126

Pilar Saenz

NETmundial and the future of Internet governance 128

Marília Maciel

Argentina and progress towards multistakeholder model 132

Ramiro Alvarez Ugarte

The need for a digital agenda in Bolivia 133

Camilo Córdova

Internet governance in Colombia 135

Gloria Meneses

Civil society's role in the Internet governance debate 136

Amalia Toledo

My experience with the Internet 138

Karina Gálvez

5 PART

COPYRIGHT **141**

Copyright law reform in Brazil 142

Eduardo Magrani

Colombian constitutional court overturned copyright law 144

Carlos Cortés Castillo

Access to culture and copyright in Uruguay: #noal218, a civil society victory 146

Jorge Gemetto

The reform of collective management of music in Brazil 149

Pedro Belchior, Mariana Valente and Eduardo Magrani

Copyright in Argentina 152

Beatriz Busaniche

Copyright in Brazil 153

Marcos Wachowicz

The privatization of copyright enforcement: the Brazilian context ... 154

Pedro Nicoletti Mizukami

A discussion that could finally change copyright in Peru..... 160

Miguel Morachimo

Copyright and access to culture in the digital environment..... 162

Allan Rocha de Souza

Open educational resources..... 165

Eduardo Magrani and Pedro Belchior

**Exceptions and limitations to copyright for libraries and archives in
Colombia: update & upgrade more than necessary.....** 168

Luisa Fernanda Guzmán Mejía

Copyright in Chile..... 170

Francisco Vera

Copyright in Colombia..... 171

Carolina Botero



ACTIVISM..... 173

Activism and the Internet..... 174

Miguel Lago

Right to protest and policing in social networks..... 176

Francisco Vera and Paz Peña

Internet and democracy: the protests of June in Brazil..... 178

Eduardo Magrani and Mariana Valente

**Hacking team in Chile: does the software comply with the minimum
quality standards established by the Chilean legal system?.....** 184

Valentina Hernández

Internet Rights in Ecuador: the possible triumph of activists?..... 186

Analia Lavin and Valeria Betancourt

**The online mobilization against Jair Bolsonaro, Julien Blanc
and the rape culture.....** 188

Michael Freitas Mohallem

Technology and political participation..... 190

Eduardo Magrani

**Collaborative development in Labhacker: including the
“external element”.....** 192

Cristiano Ferri

**The Indignados movement in Central America reconfigures the
traditional class struggle.....** 195

Bernardo Gutiérrez

Hacking patriarchy: the first #femhack experience..... 199

Gema Manzanares



SURVEILLANCE AND CYBERCRIME..... 203

Limits to domestic espionage: what comes from within can also strike us 204

Francisco Brito Cruz and Denny Antonialli

Surveillance, Human Rights and the role of States: Rousseff's speech and Peña Nieto silence 207

Renata Avila

The Snowden case and the Brazilian reaction..... 210

Marília Maciel and Luiz Fernando Moncau

Chilean government to subject Chileans to American surveillance apparatus 213

Gus Hosein

Information collection, location tracking & user awareness..... 215

Ellen Marie Nadeau

What transparency standards should we demand from States using surveillance technologies? 217

Francisco Vera

FinFisher in Mexico: smile, you are still being spied 219

Pepe Flores

Surveillance balloons: how much are we willing to give up in order to feel safer? 222

Paula Jaramillo

The guardian who watches over the citizens..... 224

Fabrizio Scrollini

Computer crime: the necessary Human Rights perspective..... 226

Paz Pena Ochoa

Cybercrime in Brazil 228

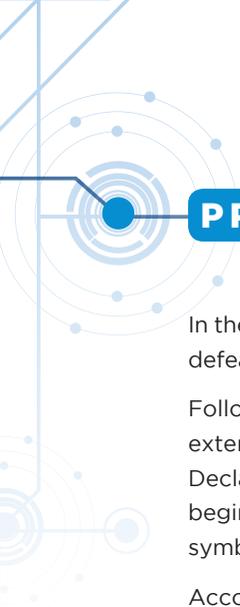
Omar Kaminski

The challenges of criminal investigations in the age of Internet..... 229

J. Carlos Lara

Cybercrime in Peru..... 232

Miguel Morachimo



PREFACE

MICHAEL MOHALLEM

In the history of Human Rights, Latin America has been oscillating between defeat and inspiring leadership.

Following World War II, the region led the creation of the world's first extensive international Human Rights instrument — the American Declaration of the Rights and Duties of Man, in April 1948 — marking the beginning of the Rights Era, months before what would become its greater symbol, the Universal Declaration of Human Rights.

According to Paolo Carozza, 'the region exhibited a dedication to international Human Rights generally at a time when the idea was still viewed with reluctance or even hostility by most other states'.¹ But such commitment to rights was soon replaced by a succession of national dictatorial regimes, state violence and backlashes against freedom and democracy.

The long absence of democracy in Latin America was finally replaced by liberal regimes. The nineties witnessed governments as concerned with free elections as they were with flexible working rights, economic globalisation and the free market.

Finally, a period of intense transformations arose from the ascension to power of governments with repressed plans of more political participation, income, gender, racial and social equality, less influence of corporations in elections and freedom of expression.

The new wave of hopes blended with the promises of digital rights. Internet and technology invited politics into its core and since then have been delivering a renewed agenda of rights and regulatory debates.

But what makes the case of Latin America so special in relation to rights protection?

In addition to the historical relevance of Human Rights, it is possible to identify five main contemporary reasons for the adoption of strong legal protective schemes. First, the region has been subject to a common ideological influence of Human Rights principles through the Catholic

¹ Paolo G. Carozza, 'From Conquest to Constitutions: Retrieving a Latin American Tradition of the Idea of Human Rights' 25 Hum Rts Q 281, 287.

doctrine and more recently through socialist thinking.² Though a global phenomenon, 'the impulse to incorporate dignity [into states constitutions] was clearly strongest in those circles which were influenced by Catholic or socialist thinking, and probably most strongly in those circles where both influences were present'.³

Secondly, the period of dictatorship regimes throughout the region encouraged the adoption of a higher level of protection of Human Rights. Although not all states in the region suffered a coup d'état, even in those where the constitutional tradition was maintained in the latter half of the twentieth century, deep social and political conflicts favoured the rise of a 'constitutional moment', as much as in the states in transition from civil-military (or just military) regimes back to democracy.

A third reason to be highlighted is the cultural and linguistic similarities, which favours not only the borrowing and coping of similar legal provisions, but also stimulate dialogues between courts and civil society movements.⁴ Thus, a legal or social action producing positive outcome in one state is easily observed by the others and frequently replicated.

A fourth particularity of Latin America is the integration process.⁵ The Mercosul was originally conceived as a regional free trade market but its motivations expanded to the political sphere resulting the Common Parliament of the South and many ambitious projects. The aspiration of

2 Christopher McCrudden, 'Human Dignity and Judicial Interpretation of Human Rights' 19 *European Journal of International Law* 655-724, 664. Also relevant to note that despite the influence of the Catholic Church in Latin America, the constitutional reforms of the past twenty years 'generally tend to overcome certain religious tendencies in the legal systems of many countries that granted important privileges to the Catholic Church. New constitutions, when they are not clearly secular, tend to recognize equality between different religions, including indigenous religions', in Rodrigo Uprimny, 'The Recent Transformation of Constitutional Law in Latin America: Trends and Challenges' 89 *Texas Law Review* 1587, p. 1589.

3 Christopher McCrudden, 'Human Dignity and Judicial Interpretation of Human Rights' 19 *European Journal of International Law* 655-724, p. 673

4 Sometimes the reciprocal use of citations in courts reflects a 'larger project of economic or social integration, or as continuation of a common history'. Christopher McCrudden, 'Human Rights and judicial use of comparative law' in Esin Örüçü (ed), *Judicial comparativism in Human Rights cases* (United Kingdom National Committee of Comparative Law 2003) 12.

5 Since the end of the colonial period, the goal of regional integration is present in political discourses, diplomatic endeavours and internal legislative indications of will. For example, the Constitution of Venezuela not only brings the intention to integrate the region in its preamble but also in article 153 where it states that the 'Republic shall promote, and encourage Latin American and Caribbean integration' and to that end it may 'transfer to supranational organizations, through treaties, the exercise of the necessary authorities to carry out these integration processes'. Similarly, Ecuadorian Constitution prohibits the adoption of treaties in which the State accepts the jurisdiction of international arbitral tribunals, except for Latin American organs. Also Argentina gives special treatment to integrationist treaties with Latin American countries, art. 75(24).

supranational integration is one further factor pushing states to give effect to international commitments, despite the recent difficulties in advancing such goals.

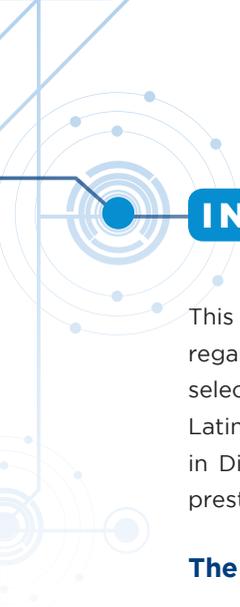
Finally, a fifth reason is the common feature of expansion of the judicial role. The recent constitutional documents innovated by including thorough charter of individual rights, social and economic rights, and a considerable level of judicial independence. Those elements together bring to the constitutional jurisdiction a large number of issues and empowers the constitutional or high courts with a broad authority to interpret and construe domestic and international law.

Although previous moments of extraordinary impulse in Latin American rights agenda can be traced to many decades in the past, the recent years were crucial – and the book “Digital Rights: Latin America and the Caribbean” highlights precisely one of these waves of fast change and encouraging innovation.

Eduardo Magrani’s selection of key articles – originally edited by him on the digitalrightslac.net website – offers a complete view of all the relevant political moments in Latin American countries regarding privacy, data protection, state surveillance, freedom of expression, online censorship, cybercrime, net neutrality, internet governance, copyright laws and online political activism.

Yet the most valuable contribution of this book is the line-up of authors. “Digital Rights” joins together a constellation of activists, government officials, political leaders and academics who were either part of the policy development in their respective states, or followed closely the critical moment of a legislative debate. Thus, nearly all 80 articles in this book have the exclusive angle and the rare vision of those who were – and continue to be – protagonists in developing digital rights in Latin America.

Michael Freitas Mohallem teaches Human Rights Law and is the head of the Justice and Society Research Centre at Fundação Getulio Vargas (FGV) Rio Law School, where he is also chair of the Editorial Council. He is PhD in Law Candidate at the University College London (UCL) and holds a LLM in Public Law and Human Rights from UCL, a Postgraduate Degree in Political Science from the University of Brasília and a LLB from the Catholic University of São Paulo. Previously worked as Campaigns Director in Brazil for Avaaz.org, legal advisor in the Brazilian Senate and in the Brazilian Ministry of Justice.



INTRODUCTION

This book is a window into the current state of Latin American society regarding technology. The present work consists in a comprehensive selection of articles that were published in the newsletter Digital Rights: Latin America & the Caribbean, a project organized in Brazil by the expert in Digital Rights, Professor and Researcher Eduardo Magrani, alongside prestigious Latin American organizations.

The Project

The monthly newsletter initiative was launched in June 2013 by the Center for Technology and Society (CTS/FGV), in Brazil, together with the NGO Derechos Digitales, from Chile; Asociación por los Derechos Civiles (ADC), from Argentina; and the Fundación Karisma, in Colombia. It has been translated each month into three languages (Portuguese, Spanish and English), encompassing 191 publications assembled in 30 volumes/editions and ended with a final, special edition, in December 2016.

The publications approach important issues related to digital rights in those regions and manage to portray a broad overview about what was currently happening in those countries, by analyzing the state of digital rights in Latin America and the Caribbean, and addressing regional news, analysis of relevant subjects, recommended research material and data regarding conferences and events.

These topics were studied deeply by The Digital Rights Newsletter, which managed to gather articles from as much as 16 countries, as it follows: Brazil, Argentina, Colombia, Chile, Mexico, Peru, Ecuador, Cuba, Uruguay, Paraguay, Panama, Bolivia, Nicaragua, Guatemala, Honduras and Venezuela. Mainly, the book delves into issues that represent contemporary topics about cutting-edge technology, the growth of interconnectivity, privacy issues, government actions and laws that try to regulate new advances on this field.

As such, this selection of papers provides an excellent opportunity to better understand current developments and changes in digital rights in Latin America, how the discussions about those ideas take place, and which way they are headed.

The background: the democratic importance of the connected public sphere

We live today in a social scene that is largely in the digital world, in which various types of spaces and devices have become vital tools for recording events, news and expression. Digital platforms are used today to share information and to specifically promote a greater degree of participation and engagement in issues of public interest.

Technology can bring us countless benefits, but it also creates difficult problems which need to be thoroughly discussed if we aim to solve them. In terms of privacy, there is a growing fear - and with just cause - that the development of new technologies might end up increasing the risk of violations in users' privacy. There is no doubt that the improvement of technological devices and the way people grow ever more dependent on those new tools will significantly modify the way we deal with and share personal information.

The concern that we may be gradually giving up a greater amount of privacy while technology advances has been reinforced by several factors. Recurring violations of data storages, the constant monitoring of users' activities online and the mapping of behavioral patterns based on data collection are some of the elements that point out the need to study new ways to keep personal information protected. Moreover, the astounding growth of social networks and connected devices greatly contributes to the expansion of the amount of information made public on the web, and generates some apprehension about its use. After all, it is no wonder that severe criticism has been made about how it may encourage a culture that takes for granted public exposure.

Such issues demonstrate how urgent it is for Latin American countries to develop comprehensive regulation regarding privacy. Many have already passed legislation that directly addresses this matter, but others - like Brazil - are falling behind and let serious violations occur by neglecting to establish the necessary degree of control over such actions.

New technological developments also create issues concerning fundamental rights, such as freedom of expression. Certainly, the Internet has occupied such a role in current society that it has become hard for people to imagine living without it. It has brought many new ways of publicizing and disseminating content, and it has also amplified our capacity to communicate. Today, anyone can disclose his thoughts, ideas or discoveries through various means: blogs, social networks, email

groups, web forums and many other digital platforms enable the open and free exchange of information throughout the globe.

This constant stream of communication further serves to develop democratic participation, especially in developing countries. The technologies and the way they are being used have transformed individuals into an important source of information, socio-political engagement and control of public power, allowing a greater empowerment of citizens, which triggers processes of social transformation and, at the same time, greater legitimacy of political power. All these factors are representative of the emergence of a connected public sphere with significant democratic potential yet to be fully explored and measured.

In this perspective, we can already begin to see more solid contours of the consideration of this space as a fundamental democratic space. In May 2011, the UN Special Rapporteur for the promotion and protection of freedom of expression, Frank La Rue, advocated the recognition of Internet access as a human right, considering it one of the main means through which individuals may exercise their right to freedom of expression, as stipulated in article 19 of the UDHR. In the conclusion of his recommendations, La Rue asserts:

(...) Unlike any other medium, the Internet enables individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an “enabler” of other Human Rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole. (...) Given that the Internet has become an indispensable tool for realizing a range of Human Rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all states. (...)

La Rue’s speech expresses that the Internet is a tool to promote development on several fronts. The deepening of democracy is one of the most remarkable of them. The combination of digital technology and Internet infrastructure results in platforms that are substantively distinguished from traditional media. By drastically reducing costs and barriers to participation in the public sphere, the Internet enables multi-directional, instantaneous responses, broadening possibilities for discourse and debate.

With the advent of new digital tools with democratic potential, the emergence of what has been called “e-democracy” or “digital democracy” appears. In promoting citizens engagement and political participation through new technologies, the doctrine has identified the impact of the Internet on the mechanisms of: (i) improving the transparency of the political process, by monitoring the actions of government officials and public resources; (ii) facilitation of direct involvement and active participation in political processes, and; (iii) improving the quality of the formation of public opinion, with the opening of new spaces for information and deliberation.

In 2013, Brazil experienced a couple of the biggest protests in its history. A R\$ 0,20 raise in bus fares was the catalyst for several national movements demanding better quality of public services, more public transparency, definitive measures for fighting corruption, among other claims. This probably would not have been possible, or at least would not have taken such magnitude, without the Internet. People used primarily social networks to manifest their discontentment, to share and convince others that there was an urgent need to press government authorities and, finally, to organize and schedule an agenda for the protests. This demonstrates how political struggles also take place online and how new technologies have the capacity to aid social movements.

However, it is clear that such mechanisms of democratic participation find limits. Factors such as the unequal distribution of access, the highly fragmented structure of channels, the polarization of discourses, and the increasing appropriation of online space by the logic of state power and market capital illustrate how the Internet ability to expand the public sphere can be constrained, hindering to a great extent its potential.

Another example of an obstacle to democratic participation is the increasing use of bots which conduct automatic messaging and posting on social networks in elections periods to promote certain political candidates, parties or ideas. This practice, known as astroturfing, tries to simulate spontaneous political movements through commentaries online, by employing bots that can operate several profiles and mask their identity. It is in direct opposition to what has been called grassroots, the truly unplanned and voluntary growth of a political trend. Clearly, astroturfing brings even more complications to the already complex dynamics of an election, with its ability to artificially influence voters.

There has also been some criticism of what has been called “couch-activism”, referring to the preponderance of support to causes by manifestations that

are restricted to the online environment. However, it must also be said that digital activism can break barriers that otherwise could inhibit political participation. Many people often have little time or energy to engage in activities after managing long working hours and many time-consuming tasks in their routine. With the Internet, citizens can participate in political discussions at any given time, from the place and platform that is most convenient and for any duration.

Overall, the digital environment can provide various mechanisms to reduce Human Rights deficits and strengthen political participation. Sadly, the instruments provided by technology to promote the capacity of citizens to influence the course of politics are still underused. Governments and other institutions could establish different methods to enable the diffusion of common ideas and opinions and the direct participation of its constituents in important decisions that will affect their lives. Mainly, the objective would be to give voice to civil society by developing digital platforms to allow people to respond to misuses of power, by using more democratic and horizontal tools, such as the ones the Internet provides.

Freedom of expression also relates to the tension between free and unrestricted disclosure of information and the protection of people's images and their wish to keep some materials private and unavailable to the public. There have been many cases, argued in judicial courts throughout Latin America, in which the main controversy revolved around maintaining or removing content from webpages or search engines online. This type of conflict usually entails a judgement that opposes public interest in that particular piece of information and the personal rights of the people involved.

Another important topic approached in this book is state regulation over digital platforms. As technology advances, the law must adapt to the new tools created, by devising efficient civil frameworks that could enable us to handle them better. As an example, the use of unmanned aircrafts, popularly known as drones, is fairly recent and it brings about many concerns, especially in regards to physical integrity and property. Not only could drones do actual damage to people or objects (for instance, when they crash), but their capability to take pictures and videos of different areas from various angles could easily give way to severe violations of privacy. These rights also need to be protected from those different types of offenses, which prompts the importance of conceiving new forms of legislation to include them.

Brazil, in particular, has applied great efforts to produce the Civil Rights Framework for Internet Use. This law was sanctioned in 2014 and it is a large step towards better regulation of digital platforms. This type of action should be encouraged and replicated by other countries in Latin America, as it provides new mechanisms for the protection of constitutional rights online.

Internet governance is another focus of this work, referring to the development and application of shared principles, rules and procedures that concern the use of the Internet, which is promoted by governments, the private sector and civil society. In this definition, each stakeholder has assured participation by performing different complementary roles, constituting the multistakeholder model.

With more than two billion users around the world, the Internet calls for a broader dialogue about its consequences. In this sense, there is a pressing need to create international bodies with multistakeholder composition to further promote and advance discussions regarding the online environment. The Internet Governance Forum (IGF) is an example of this model, as well as some other regional efforts, which have attempted to develop management strategies for this medium, by reaching decisions about its infrastructure and services.

The strong preference for a decentralized multistakeholder standard derives from the importance of the equal participation between players. Without it, the discussions could tilt in the direction of some particular group, putting at risk the balanced decision-making by favoring specific interests of sectors that boast economic power or political influence. Therefore, there must be a focus on increasing the equal involvement of governments, civil society, companies, the technical community and academics.

The development of new technologies and intensified use of the Internet has also heavily affected Copyright Law. Naturally, one of the solutions to this problem would be to formulate new legislation, in order to better balance the protection of authors and the new paradigm created by the digital environment. As it follows, we must weigh copyright against other constitutionally guaranteed rights, such as Freedom of Expression and access to information. So, clearer lines between unauthorized copying and fair use of works and a better adaptation of the current notions of property and the unavoidable flow of content online are necessary.

Another field that has been the topic of many controversies refers to surveillance and cybercrime. The scandal involving digital espionage committed by the NSA, revealed in 2013, raised a red flag about the potential

risks to privacy generated by the misuse of technology. This event has not only badly damaged the public's opinion and faith in authorities, but it has also significantly raised peoples' distrust that digital devices can keep users' information protected. Furthermore, even the relations between States have been shaken, as the case also exposed the persistent surveillance of important foreign government officials, a fact that has caused heavy strain in diplomatic relations between the countries affected.

This episode helps to stress the importance of the creation of strategies and structures that encourages transparency, especially to prevent such practices. Intelligence and counterintelligence activities should be subject to public scrutiny, at least to delineate its purpose and legal limits. In turn, the greater level of transparency would help to generate better accountability in regards to governments' actions, while also granting the population the possibility to control, if only to some extent, those activities. Those elements – transparency, accountability and the control of government's actions – are fundamental for democracy, which indicates the need to hold further debates in this area.

The knowledge that companies also track users' data to develop marketing strategies and to collect information about consumers' behavioral patterns has added to the concern about privacy. Users should be better informed about this sort of data monitoring, and companies should adopt policies that enable people to choose which types of content they might be willing to disclose. Even though it may be used for useful and legal purposes, the collection of data should not be conducted covertly or without permission.

Cybercrime is yet another well-founded concern often raised. A great deal of programs and different schemes are concocted daily by people who try to gain access to users' information and to trick them into giving away sensitive data. Computer crimes have recently grown more sophisticated and, consequently, harder to tackle. Therefore, we must develop new mechanisms to prevent those violations and pass legislation that encompasses cybercrime, in order to better deal with those occurrences.

It is clear that the topic of digital rights has been gradually gaining importance in public agendas in Latin American countries and the Caribbean, so it is vital to establish a broad participation in discussions about the Internet. Thus, the main goal of the present work is to provide information to whom it may interest (students, journalists, lawmakers, activists, academics, among others) about the debates that emerge in the region of Latin America regarding the digital sphere.

Due to the current relevance of the topic, the discussions led throughout this work are still incipient and many arguments are, to a large extent, controversial. So they depend on the maturation of the debate and a greater number of empirical researches. In order to seek a more solid foundation, many arguments are illustrated with concrete cases, which does not necessarily mean using the framework with the methodological rigor of case study. In addition, although it gives a broad panorama, it is important to inform that this work has no pretensions to exhaust the discussions and cases concerning digital rights in Latin America.



PART
1

PRIVACY AND DATA PROTECTION



Mapping the protection of privacy

*Juan Carlos Lara*⁶

For several months we have been conducting a thorough investigation, which seeks to map the protection of privacy and personal data in Chile, which later will also include South America. As the relevant rules are being closely examined, together with the opinion of some players in the system, we will eventually know how to address regulatory issues and how to address them.

The need to improve the conditions for the protection of rights related to privacy has often been included in public discussions, whether it be in terms of privacy, the privacy of communication or the processing of personal data. In almost every instance, we found a consecration of rights which, for one reason or another, turned out to be empty in face of the phenomena of widespread lack of observance. State devices that monitor citizens, corporations that profit from the unruly trade databases of people and penal prosecution entities that override privacy issues without any form of control, are the type of encumbrances which we have been reading about for a while.

Logically, this leads us to wonder about how we can guard ourselves from such a broad range of attacks on being free to control our very own lives. So far, the answers to these questions have proven to be useful and informative, raising some serious warnings. But likewise, it has shown us that the national systems often have major flaws that prevent the effective protection of privacy.

In Chile, this problem is evident just by looking at the constitutional regulation: the consecration of a right for the protection of privacy and inviolability of communication exists in such broad terms that it makes it seem as if all privacy issues could be solved through it, whereas in countless bodies of law we find an abundance of rules, yet a comprehensive, consistent and equitable regulation is needed.

Another example is the absence of observance mechanisms for dealing with personal data (an outright exception in the region as they are not subject to constitutional protection), plus the need for a control and

⁶ Lawyer, specialist in the law of new technologies, focusing on the link between the public interest and the regulation of digital forms of communication.

monitoring organism, and a lack of dissuasive sanctions, among other things. It seems that, unlike many countries in the region, Chile has plenty of rules, but lacks genuine rights.

Moreover, there are problems due to practices which border on illegality, including cases of companies that trade databases to send out unwanted commercial information, drones being used for air surveillance, and access to personal information, even in the absence of a warrant, at the mere request of the police.

How do we deal with a scenario which includes so many different forms of charges, in such important areas of each person's life? How do we reach a point of equilibrium, if for every interest at stake there are countless other threats? In the area of privacy and its many facets, it is firstly necessary to become familiar with a map of the problem.

For the above reasons, a significant effort has been made throughout several months by Derechos Digitales NGO. On one hand, through the comprehensive study of what the protection of these interests represents in Chile. On the other, a diagnosis of the situation through an analysis of this legislation in the field of penal prosecution, in order to know whether the institutional safeguards echo constitutional protection. Additionally, the actors of the multiple positions involved in penal prosecution were the subject of an inquiry to find out about their mode of interaction with the legislation, which apparently seems more based around intuition than actual knowledge.

From the closest inspection carried out so far, the findings show that the problems, both institutionally and in practice, are much greater than previously suspected. However, the purpose of the research is not to account for all the problems and rest on its diagnosis; on the contrary, the formation of competences for both civil society and government agents, as well as information on new legislative proposals and public policies which convert the respect for privacy into one of the essential pillars of their activity, are part of its objectives.

At a time when privacy seems to be at the center of global debate, Latin America has a great opportunity to stand out as a region where rights are actually respected. All of us are contributing for this to occur.

Privacy and security, the Latin American way

Claudio Ruiz⁷

Under the advancement of technology, the key question in our countries is to ask how unchecked surveillance practices continue affecting the right to privacy of our populations.

Edward Snowden's revelations have sparked a global scandal, as they have exposed how digital technology, which until recently has inspired countless utopias, has a very murky and dark side. It facilitates the job of states to monitor the world population in cooperation with private corporations. But in this global context, what is the situation of Latin America and why should it receive any particular attention? Originally, privacy was understood as the right to remain alone, originally it was an idea from an old article by Louis Brandeis and Samuel Warren, who have been very influential in setting up the right to privacy in the North American system.

In Latin America, the evolution of the concept of privacy has always had a much wider connotation, with constitutional recognition in most of the countries around the region. Additionally, the idea of privacy has evolved according to the evolution of technologies, which have increasingly defined its limits due to the automatic processing of our personal data. The development of information technology in the midtwentieth century has created powerful tools for treating and processing information, allowing the field of medicine to obtain extra health data from large segments of the population and control pandemics. However, both the state and private sectors are responsible for setting trends and behavioral profiles without the consent of the people.

Privacy, therefore, can no longer be reduced to the right of private space, but as one where everyone can take an active part in controlling the existing information of each individual; a legal manifestation of respect and protection which is guaranteed to each and every person, protecting dignity and human freedom, by recognizing within the holder, a power of control over their personal autonomy. The Inter-American system has not been immune to this construction. Without going any further, the 2013 Report of the Special Rapporteur for Freedom of Expression expresses the richness of the concept,

⁷ Claudio Ruiz is NGO Derechos Digitales' CEO.

indicating that the right to privacy was referring to that external sphere which is beyond the arbitrary interferences of the state and third parties.

In other words, it is the right of self-governing, i.e., of developing personal autonomy and individual projects, of secrecy of data and information of reserved spaces, and of the right to one's own image. Although there is a long way to go, particularly due to the aggressive advance of digital technologies and their impacts on Human Rights systems, this categorization is a good starting point for building a sophisticated doctrine for the protection of these rights, under the wing of the tradition of the American system.

The rapid evolution of digital technologies has exposed these aspects of the right to privacy to permanent threats from around the world. Worryingly, Latin America is not just an exception to this trend, but as on other occasions, it has even become a field for exploring new forms of surveillance. Thus, the 2014 report of the High Commissioner for Human Rights, Navi Pillay, deals specifically with the subject of privacy in the digital age, with a special focus on the problems arising from state surveillance and the lack of transparency: "The complexity of the challenges for the right to privacy in a digital age, of rapid and dramatic changes, will require constant scrutiny and dialogue between all key sectors, including governments, civil society, scientific and technical experts, the business sector, academics and Human Rights specialists".

Moreover, on an international level the ruling of the European Court of Justice is particularly important, as it determined that the data retention rules of Internet service providers are neither necessary nor proportionate, i.e., they do not meet the standards of respect for fundamental rights. Despite this decision, which has caused a profound reflection in Europe regarding such practices, in Latin America the data retention rules are generally an exception instead of a rule. From the perspective of the Inter-American countries of the region, they should advance in harmonizing these practices in light of the Human Rights criteria.

Unfortunately, the following are not exceptions, but different practices that can be seen throughout Latin America:

- In Mexico, the last amendment to the Telecommunications Act included explicit policies regarding the geo-location of cell phones without requiring court order.
- In Colombia, it has been revealed that a number of communication interceptions have been made under the peace process, without any judicial guarantees.

- In Argentina, through the Federal Biometric Identification System for Safety (SIBIOS), which is probably considered the most aggressive surveillance system state in the region, based on biometric identification.
- In Brazil, the emergence of protests against the organizing of the World Cup gave way to a technical reinforcement of the police and intelligence services in order to deal with them. This example is particularly important given that it shows the connection between the protection of personal information, or at least of due process and transparency, with other fundamental rights such as the right to protest. Somehow, the exercise of the right to protest in the XXI century is closely linked to the protection of privacy on the Internet.

The development of digital technologies has brought a new opportunity for the growth of surveillance practices in Latin America. Despite having suffered decades of totalitarian state repression, which included a strong monitoring component in the form of agents, so far it does not seem like a simple task for our societies to make the connection between this reality and the exercise of Human Rights through digital technologies. Edward Snowden's revelations, which also cover the close cooperation between security agencies and technology companies, should be a wake up call for the construction of a normative model that respects online Human Rights. Additional efforts are expected from public policies, but more so an effort to systematize practices and local realities in order to understand these dynamics and provide consistent and guaranteeing solutions.

Privacy and surveillance in Ecuador

*Carlos Correa*⁸

In Digital Rights LAC, we asked to different specialists in the region about their personal appraisal in digital rights issues. This is the case of Carlos Correa of Ecuador, to whom we asked what lessons for activism can be drawn from the Penal Code and the Article 474. Here is his answer.

In Ecuador, we ended 2013 with ambivalence in regards to digital rights activism and advocacy. The balance tips in favor of users when we talk about the Penal Code (#COIP), recently approved by the Legislative Assembly and yet to be sanctioned by the Executive. In early October, at the stage of a bill, the Article 474 disregarded the right to information privacy and

⁸ Carlos Correa is the Center for Interdisciplinary Studies of Industrial Property Law and Economics' director, at University of Buenos Aires.

the privacy of the citizen. Immediately, through spontaneous meetings of interested associations and around the hashtag #InternetLibre, it was suggested not only the modification of this article, but its elimination. Two months later, this was accomplished. I venture to list the conditions that were given for this achievement:

- 1 Getting out from the Internet bubble.** While the web was the common place to meet, organize and develop, the challenge was getting out from the easy e-activism and starting working closely with the decision makers: the Members of Parliament (MP).
- 2 Carrying the discussion agenda to ordinary citizens through the mass media.** Inconsistencies of Article 474 were more evident when ordinary people began to talk among them about the dangers of implementing the law. This was a result of activists' work with journalists and the specialized press that gave visibility to the problem.
- 3 Joining together.** When alarm bells rang, associations, unions and interested groups made a single front, wearing the same shirt, using the same network to be better organized, but not separately. When the news of the removal of the article was learned, the credit was for all.
- 4 Being critics and also proactive.** After being neatly documented, the tone of the discussions with MPs and their advisors passed from the complaint to the proposal.
- 5 Moving through activism.** Finally, the minimum necessary and obvious: to move! Now comes the stage to maintain consistency and make from this theoretical concept related to the "collective intelligence" something practical and tangible. 2014 awaits us.

The friction between transparency and personal data protection in Peru

Miguel Morachimo⁹

In recent months, it has been discussed in Peru how the personal data protection norms must be interpreted within the framework of transparency obligations. In cases decided by two different bodies, the limits of what can and cannot do with public databases have been discussed. The answer to these questions can impact significantly on new journalism practices and the degree of access to public information.

⁹ Miguel Morachimo is an attorney and NGO Hiperderecho's director.

Datos Perú and legal norms

In October 2014, the Personal Data Protection Authority (PDPA) resolved two claims against the Datos Perú website's administrators. The site, which operated for several years in Peru, among others, paid the access and search service for legal devices within the State Gazettes. In other words, the entire Legal Standards Bulletin published in the Official Journal, including legal and administrative acts of compulsory disclosure as appointments and sanctions, were copied and pasted. Two of these norms reproduced by Datos Perú correspond to disciplinary sanctions against the claimants. That was the origin of the claim.

In its decision, the PDPA determined that the site had failed to comply with the data protection law in failing to request the consent of such persons to include their name in a legal database and, thereafter, in ignoring their requests for cancellation. Although the same information, including the names of the claimants, was accessible from the Official Gazette website, as well as from the Ministry of Justice website, the PDPA considered that this did not authorize any third party to reproduce information containing personal data. That is, the PDPA determined that prior publication of a public document did not authorize its consecutive reproduction to the extent it contains personal data.

Equifax and the public taxpayer register

In March 2015, another case brought us back to the same question. This time the Constitutional Court (CC) ruled a habeas data claim filed by a citizen against Equifax, operator of a private credit risk bureau in Peru, for including information he did not provide, comprising also his address. In its defense, Equifax said that it has obtained the plaintiff's domicile had obtained through a routine search in the public taxpayer register available to the general public on the Peruvian tax authority website.

For the CC, Equifax was not authorized to use or incorporate into its database the information contained in the taxpayer register. By establishing the rule that the credit bureaus cannot collect information from public databases, it established the criterion that only those who are expressly authorized can do so. That is, in a similar tone to the PDPA's decision, the court stated that prior publicity of personal information in a public database does not authorize others to use such data without permission of the owners.

A response but not a solution

The rule underlying both decisions is clear: third parties cannot reproduce the documents or state databases accessible to the public as containing personal data. The exception being that these third parties have a special authorization from the owner of the data or are under an assumption of emergency (e.g., public interest). This is the reasoning given by the head of the PDPA in several occasions, including a recent interview. However, although this approach can be sustained under an interpretation of the personal data and transparency norms, it leaves a bitter taste for many reasons.

There is a serious conflict between what we seek to protect and the reality. It is idealistic protecting privacy only when private persons infringe it. Through their decisions, the CC and PDPA acknowledge that reproducing certain personal data may affect the privacy of citizens. However, instead of preventing the affectation in origin, they limited themselves to punish third parties replicating what the State did in the first place.

In both cases, it is about sanctions to private persons that tried to reproduce data published firstly by the State and, so far, available through state services. I fully understand that legally there is no consent for further processing by third parties. However, what are we really protecting by applying this criterion? Clearly, it is not the confidentiality of such personal data.

The second mismatch occurs when this rule is analyzed from the new ways to access public information. It is not whimsical that the taxpayer register is publicly available or that even includes taxpayers' address and their tax capability. Nor it is random that resolutions of appointments, disciplinary sanctions or affidavits by civil servants appear in the Official Gazette and are archived in all libraries and archives in the country. This information is distributed as public information because it is part of the national memory, a guarantee for business transactions and unalterable record of the country's life.

Before, only a person with physical access to those documents could access, read or recall them. Today, the technology allows for the consultation of databases with millions of such documents. That is, the reuse of public information made available by the State allows ordinary citizens the full exercise of their right of access to public information.

According to the reasoning of the mentioned decisions, this possibility would be closed, unless any reference to personal data is previously removed from these databases. In the case of many databases, this does not only imply

a titanic job, but the subtraction of the content itself. If the information is published with the intention that all can access it, why this right can only be exercised in the terms and on the platforms enabled by the State?

Finally, this rule only seems to support an anachronistic view of the journalistic task. According to it, it is fine for an investigative journalist accessing numerous databases individually but can only publish those data of public interest as part of his/her story or article. But what about the data journalism projects in which entire databases are also published through visualizations or tables? In Peru, for several months, it is available a website that allows to consult visitor records from various public offices, taking data directly from the records published by the institutions themselves. Under the proposed solution, this activity, which in itself is a form of investigative journalism, would be illegal for not having the consent of the persons whose names are being shown.

What is clear is that the solution proposed in these decisions need to be reconciled with reality. We need to establish clear rules that protect personal data and are applicable to the State and private persons. These rules cannot ignore how nowadays we interact with technology and how we use it to exercise both civil and economic rights. Acknowledging the existence of this problem is the first step to begin solving it.

Your fingerprint for a kilogram of flour: biometric and privacy in Venezuela

*Marianne Díaz*¹⁰

In a lot of contexts, balance between privacy and comfort is an issue of convenience. In Venezuela, where in order to buy food supplies you must slide both thumbs through a fingerprint scanner and give a big spectrum of personal information, is an issue of survival.

In Caracas or Maracaibo' supermarkets and drugstores, buying a kilogram of grain or a pack of cookies has become a complex procedure: it's required for you to deliver an ID, full name, phone number, address, date of birth and to slide both thumbs in a device: the emblematic "fingerprint scanner"; a device which usage by stores was originally voluntary, but which evolution,

¹⁰ Venezuelan lawyer and activist. She manages the NGO Free Access and writes for Global Voices.

months afterwards, is one of omnipresent machinery, kind of a necessary tool for the acquisition of a simple pack of gum in any chain store.

Advertised and imposed by the government as the blessing that would end Venezuela's food and medicine shortage, the so called Food Safety Biometric System hasn't changed reality. The long lines persists, products are still in shortage, and the black market blossoms under the complacent eye of the people in charge of control management. Nevertheless, fingerprints of millions of Venezuelans are taken every time anyone makes a basic transaction. In spite the claim that this system would only be used in purchases of "regulated" products, cash registers require fingerprints to be activated.

Hundreds of millions of bolivars were expended implementing this system. According to armando.info's investigation, the company in charge of the device's import is called HiSoft, but its directives are the same as the ones of a known company: Smartmatic, a name that has become a synonym of elections in Venezuela, because they were in charge of the implementation of the fingerprint scanner in the electoral system, used for the first time in the elections of the year 2000.

Along with biometric and personal data requested to the customers at the moment of the purchase, stores are obliged to preserve a great deal of information regarding the transaction, demanded by the government's tax collector. The extent of the databases that the Venezuelan government possesses regarding their citizens would be heaven for any big data analyst. With enough computer skills, it wouldn't be difficult to establish a detailed profile of every Venezuelan citizen, starting from data such as address, the places where he shops, how much money he expends and the products he acquires. Nevertheless, no one outside of the government possesses the capability to know if these systems are intertwined or where this huge quantity of information is stored, much less what the policy for its retention and storage is.

The implicit risk of the usage of biometric technology is the capability of governments to use it with surveillance purposes. In cases such as this, biometric data are part of a multimodal system, because they are combined with other information points such as birth date, address, and national ID number. The more data points belonging to an user exists, the easier it is to implement full surveillance. Just thinking about the whole spectrum of information hoarded by the government is overwhelming: our ID is required to acquire a telephone line; we are obliged to provide our tax registration number to any interaction with public administration.

In Venezuela, a country with a dark recent history of persecution caused by a list of citizens whose political identification was made public through the infamous “Tascón list”, the reaching capabilities of this kind of surveillance are chilling. Regarding the fingerprint scanners, we know at least one of the possible uses of this information: those marked by the system shopping in quantities superior to those of their established quotas, go to a blacklist, and are blocked completely from the system. This makes them use the (illegal) black market in order to purchase food, medicines and basic products.

With this scythe hanging over the citizens head, in a country who has lost faith in their electoral system and where technologic alphabetization leaves much to be desired, some people are aiming to a kind of subconscious connection between the possibility of provide food and being able to vote. The Venezuelan economic system, profoundly paternalistic, is builded for dependency on an almighty government who “grants” privileges and royalties in its own terms (“granting” houses, food in accessible prices, in exchange of an almost religious loyalty), and whom, like a vengeful god, takes away those privileges when mortal falls out of grace.

After Tascón’s list, a lot of people found themselves unable to access mortgage loans, scholarships or job opportunities because they supported the recall referendum against the government in turn (which period has extended for more than fifteen years). It’s not surprising, then, that a lot of people’s subconscious makes unwanted connections between the different fingerprint scanners and begins asking questions. As pointed by Luis Carlos Díaz, referring to the electoral system: “the machines are only a medium, a platform, but they are inserted into a scenario that is not neutral at all and they also become an object of diatribe in which the NEC hasn’t put a lot of effort to clarify. It seems as it is not of their interest”.

In Venezuela, there is not a personal data protection law and in spite that the law of Information Technologies establishes that the citizens are required to hand out only the absolutely necessary information to be provided with a service, the Venezuelan State, with their panoptic cravings, hoards big quantities of personal information which final destination is unknown to us.

In past weeks, it was made public that the National Superintendency of Banks is now demanding financial entities to deliver all information of electronic transactions made by their customers, including IP addresses, amounts, names, bank accounts and reason of transactions. Once again, the justification for such violation of privacy is called “economic war” which is

blamed for the deep inflation crisis present in the country. This is the excuse that has been used once and again to block websites, incarcerate users, intervene communications and restrict rights.

Even if they are not the government eyes that we fear, the security of this database is doubtful. The Venezuelan electoral and civil registry, as well as the information related to tax identity and social security, are public, they can be consulted online and mined by anyone interested in them. The online government system of the country storage passwords in plain text and send them to the users by email, and the vast majority of the government websites' security certifications are outdated. Certainly, it's not the kind of system in which I would wish to confide my biometric data, but I don't have another choice, unless I wanted to be restricted to the illegality of buying food in the black market.

Private profiles in public places

Dennys Antonialli,¹¹ Francisco Brito Cruz¹² and Mariana Giorgetti Valente¹³

Imagine a world where when you are involved in a lawsuit a judge can, before making a decision, check your profile on social networks. Who your friends are, what places you usually go to, your pictures at parties, comments on memes and pages you liked. Let's say that the judge can do it whenever he or she wants, since it would be helpful to analyze who you are, if you are telling the truth and thus make a decision based on more information.

This reality is not far away. Recently, the judge Marcus Vinícius Pereira Júnior, of the jurisdiction of Cruzeta (RN), denied a court fee exemption request (based on claim of poverty) made by a citizen, after searching and checking her profile on Facebook. Based on her pictures and posts on the social network, he concluded that she could afford the amount to be paid to the court.

According to the decision, “by making public her presence at the ‘big event of Jorge e Mateus with friends at the rodeo in Currais Novos” [...] “as well as happy AND EXPENSIVE moments, watching 2014 FIFA World Cup

¹¹ President Director at Internet Lab.

¹² Vice President Director at Internet Lab.

¹³ Research coordinator at Internet Lab.

matches”, this person would not be “concerned to support her family”. She was also convicted of bad faith – which means she was issued a penalty for her request by the judge, considering the applicant was supposedly trying to deceive the court.

At first, it may seem that the judge had a good idea. He gathered more elements and this allowed a “more fair” decision. However, there are some reasons why such practice is understood as inadmissible and objectionable. The first one is of legal nature. It is true that the law grants authority to a judge to ask on his or her own discretion that specific evidences are produced (raised and taken to the court), when they are difficult or expensive to be obtained otherwise. The judge can, either because a party to lawsuit asked or he or she considers important (by means of an official letter), determine that such evidences are produced or the judge can produce them – investigating “people or things”, for instance.

But in cases like these the request must always follow a formal procedure, ensuring both parties the right to provide clarification and make remarks they consider relevant (Art. 440 and 442 of the Civil Code of Procedures). This is a guarantee for parties to respond to such evidences and provide their interpretation before the judge makes his own judgment. Everyone has the right to present a context and give an explanation to the judges on facts that come up during a lawsuit. Those rights of providing a version and being able to refute the other party’s argument are called defense.

The second reason is related to how we use the social networks. We all know that people usually reveal only some of their aspects on their profiles. By choosing pictures and moments to be shared, we frequently hide weaknesses or difficulties. We sometimes want to show something we are not.

And there is no problem to do so. The issue is when those parts of our lives start being used as a perfect reflection of them. The worst – without having the right to even express ourselves about it. Besides, what else my profile might reveal? What if the magistrate finds an enemy in my friends list? What if he or she finds out we have different political views? What if he or she assumes I am irresponsible for the groups I belong or places I go? All this can be a bias and influence him or her against me.

But it happened before the social networks. Body language during a hearing, the way of speaking or even how someone dresses are examples of subjective aspects that might eventually impact on a decision. The difference is that in such cases we had some control over what the judge was observing. In case of social networks it works as if the judge

had checked the citizen's life outside the proceedings, out of the person's view, outside the court. This can become particularly worrying if it is done secretly – if magistrates, when checking the profiles of parties before making a decision, do not give the possibility of clarifying or at least refuting the conclusions made due to such analysis.

However, it should be reminded that judicial snooping can only be done if all our information on the Internet is publicly available to all users. The default on Facebook, for example, is that everything on our profiles are public at first. It means that if we do not change our privacy settings, anyone will be able to have access to our pictures, posts and friends list. Restricting access to such information only to our friends or friends of friends can be a way to try to be protected from a “surprise official visit” to our profiles.

Today, we know that virtual presence is an easy source of information about people. There are several cases of employees fired after disclosing on Internet that they lied about not going to work. Employers who – during selection processes – analyze the candidate's behavior by observing how the person interacts or his or her likes, according to profiles on the social networks.

Who has never searched more on the web about someone that was mentioned in a conversation? If, on one side, people could be more concerned with their own privacy and Internet companies could adopt default settings to avoid such practice, on the other side the Judiciary should also be careful when using those facilitation tools in a procedure that guarantees people's rights. Curiosity is not always helpful to the Justice.

Personal data, companies and the cloud: are we ready for it?

Valeria Milanés¹⁴

Cloud computing technology, so advanced in other parts of the globe, is incipient in Latin America in general and in Argentina in particular. Nevertheless, according to recent studies (Usuaría Research, 2013), Argentine businesses expect to see substantial growth in the adoption of

¹⁴ Lawyer with experience in litigation, graduated from the Faculty of Law and Social Sciences at Buenos Aires University (UBA) in 2002. Member of the Institute of Computer Law of the Public Bar Association of the Federal Capital. Researcher of legal aspects related to ICTs and Internet.

cloud technology in 2015, especially in the hiring of public cloud services provided by large multinational companies, including Google, Amazon, Microsoft and Rackspace, amongst others.

The greatest concerns raised over the adoption of cloud computing are in connection with privacy and data and information security, not only in relation to the company itself but especially client and user data.

What is the situation like in Argentina? The dominant legal framework is Law N° 25.326 on Personal Data, dated 30th October 2000 (based nearly word for word on the Spanish legislation), modified by Law 26.343, dated 12th December 2007, and the regulation deriving from it, including Regulatory Decree N° 1558/2001 of the same Law and all the Provisions issued by the enforcement authority, the National Personal Data Protection Department (DNPDP, as it is known in Spanish).

Also noteworthy are art. 43 of the National Constitution, as well as the international conventions that are constitutional nature in nature and applicable in accordance with art. 75 subparagraph 22 of the same body of law.

Argentine Personal Data Protection law is viewed as being the most advanced data protection legislation among all others. Firstly, it establishes the lawfulness of databases that are duly registered with the D.N.P.D.P., taking “file”, “record”, “database or databank” indistinctly to mean the organised set of personal data being treated or processed, electronically or otherwise, in any shape, form of storage, disposition or access.

The law also determines aspects of data quality, security and confidentiality, data holder consent, applicable conditions for assigning and transferring data internationally (including in both cases shared responsibility between the person responsible for the data and the contracting third party), data holder rights (regarding information, access, rectification, updating, suspension), habeas data, requirements and procedures concerning Database registration and criminal sanctions, amongst other provisions. In respect of chapters I, II, III, IV and art. 32, it also establishes the nature of public order, which is not a minor issue as public order legislation is not negotiable or renounceable and this means that any obligation assumed to the contrary goes against the law.

On the other hand, with regard to the cloud, large multinational public cloud service providers are known for using adhesion contracts, which generally do not contain specifications established by Law 25.326 and in which the applicable law and predetermined jurisdiction are that of the country where these companies are legally domiciled, mainly US cities. Furthermore, even the servers that store the information are sometimes not in Argentina.

It is important to notice that since there isn't a Personal Data Protection legislation, the US is viewed as a country with inadequate protection by international and national standards. This is also not a lesser issue, because Argentine law requires that special administrative authority be granted in case of international data transfers (cfr. art. 12 Decr. Reglam. 1558/2001).

In addition, the Personal Data law is of limited application and compliance. For example, in 2012, after twelve years in service, the D.N.P.D.P. had registered 20,000 databases, compared with 1,600,000 databases registered by that date and within the same period with the Spanish Data Protection Agency.

Equally Argentine businesses are not renowned for their adoption of international data protection standards. There are very few local companies that have obtained ISO 27001 and other related standard certification, not to mention the recent ISO/IEC 27018, which specifically concerns cloud security standards and that is only now falling under the scrutiny of specialists in the field.

Thus, we may conclude that Argentina still has a long path to tread in terms of data protection and that, in order to implement cloud technology beneficially, joint and responsible public and private sector growth are necessary, with a view to bringing commercial practices in line with the current legal framework.

This also holds true for the region, which to a lesser or greater extent consists of countries with personal data protection regulations. The issue continues to challenge the State, the business sector and users, who provide their data, with the need for actions towards effective implementation and compliance of current laws and adoption of responsible and sound business practices to allow, in as far as possible, for personal data privacy and security guarantees to be preserved.

The dangerous ambiguity of communications encryption rules in Colombia

Juan Diego Castañeda Gómez¹⁵

In Colombia, the discussion about the legitimacy of using encrypted communications must start from the fact that there is already legislation on the matter.

It is not unusual that, with attacks such as those in Paris against the satirical magazine 'Charlie Hebdo,' governments react by promising legislation that would increase the powers of the police and intelligence services. On this occasion, the Minister of the Interior of the French Government, Manuel Valls, said that new measures against terrorism are necessary. On the other hand, the Prime Minister of the United Kingdom, David Cameron, has proposed measures against private communications encryption, so that "blocked areas" for security agencies should not exist.

Of course, such proposals have been criticized because, among others, the privacy of communications strengthened by encryption is an essential guarantee for the realization of the rights to privacy and freedom of expression. Interestingly, the latter was the right that occupied the media coverage of the attack on the French magazine.

In Colombia, the discussion about the legitimacy of using encrypted communications must start from the fact that there is already legislation on the matter.

In the case of encrypted cell phone communications, the legislation has two areas. On the one hand, operators can only provide encryption service to certain government officials. On the other, sending encrypted and encoded messages are banned. Let's take a look.

The Intelligence and Counterintelligence Act (Law No. 1621 of 2013) provides that telecommunications services providers must offer encrypted voice call service to high government and intelligence officials. This means that a very small segment of the population can acquire the encryption service, leaving out, for example, journalists and Human Rights activists.

Moreover, since 1997, users of "communications equipment that use the electromagnetic spectrum", besides needing a "subscription card" by

¹⁵ Lawyer and researcher on subjects of right to privacy and surveillance in digital environments.

the operator, have limited the use of these for personal purposes and banned sending “encrypted messages or in unintelligible language” (Article 1, Law No. 1738 of 2014 in which Article 102 of Law No. 418 of 1997 is extended).

The text of this statute was approved for the first time in 1993 and was revived four years later. In addition, it has been continuously renewed until today (in 2014, its validity was established until 2018). In addition to this norm, others were approved in the same way, that is, without proper democratic debate or without revising the powers granted to an entity such as the National Police, which may request subscriber data, seize equipment and restrict the use of interceptors, scanners and open broadband receivers.

Some criticisms

■ **The sum of all powers:**

First, these powers are in addition to others that have the Colombian government to fulfill its constitutional duties to pursue the prosecution and protection of citizens and public order.

Telecommunications service providers must inform the Prosecutor about the type of technology they used in order to facilitate interception of their networks. They must follow the guidelines issued by the Ministry of ICT to carry out the interception. They must also report to the Prosecutor about identification data of subscribers and keep them for five years. Finally, if required, operators must provide the information they have in their databases to geographically locate cell phone devices in “real time” (Articles 1, 4 and 5, Decree No. 1704 of 2012).

Since 2013, the intelligence agencies have the power to monitor the electromagnetic spectrum and to obtain from telecommunications service providers the “communication history” of subscribers, their identification data and, in general, any information needed to pinpoint the location of equipment. Like the Prosecution, the intelligence authorities may request the mentioned information for a period of five years.

Taken together, the power of the Prosecutor and State intelligence agencies seem sufficient to fulfill its mission. In that sense, banning the use of encryption or sending coded messages is neither necessary nor proportionate in regard to fundamental rights.

■ **Lack of clarity:**

A big problem with these standards is that we are unclear about technologies and information included. For instance, the statute does

not define what is meant by “communications equipment that use the electromagnetic spectrum” (it can range from cell phones and radios to wireless routers). Such a broad definition does not allow to know if it is banned encrypting messages in a device, regardless of the transmission channel used (voice and/or data). In any case, beyond the precise interpretation of the notions, a statute allowing such intrusion into the privacy of communications should be much more specific.

■ **Measures that go unchecked:**

In our analysis, we find that the proscription of encryption in Colombia exists since 1993 and has been renovated in laws passed in 1997, 1999, 2002, 2006, 2010 and 2014. This shows an almost routinely extension of the period of validity and, what is worse, without any discussion of its necessity and proportionality, despite the profound technological changes that have occurred since it was first approved. Any extensions should serve, for instance, to clarify the ambiguity in the above-mentioned notions.

In a 1995 lawsuit, it was alleged that the statute infringed the right of freedom of expression. However, the Constitutional Court ruled that the State can (1) impose rules on use of spectrum, (2) limit fundamental rights to preserve public order, and (3) that the measure does not affect privacy because it is not an authorization to conduct wiretapping without legal and constitutional requirements. Of course, at the time, technological developments were not the same and the possibility of massive and illegal state surveillance was not recognized, which facilitates the ubiquity of digital technology. Therefore, although the topic is reviewed formally, it would be worth to be re-evaluated.

As for the electromagnetic spectrum monitoring authorized in the Intelligence Law, the Constitutional Court found that the wording of the statute did not permit the interception of communications, as monitoring is an impersonal activity not targeted to specific subjects. In any case, it is unclear, for example, how can “monitored” cell phone calls in an area without intersecting it. However, for the Court this action does not require judicial authorization (Corte Constitucional de Colombia. Sentencia C-540 de 2012).

In conclusion, in Colombia it is still not clear what communications cannot be encrypted nor in what sense the monitoring of the electromagnetic spectrum is not interception. 2014 will be remembered as the year of surveillance due the many scandals. But what It seems to be clear is that governments do not know how to regulate the powers we have given them.

SECRET shakes up Guatemalan society

*Renata Avila*¹⁶

Authorities in Guatemala flirt with the idea of regulating social networks and applications, because presumably many of them have the potential of promoting abuse. Does the country need such measures?

Guatemala has long enjoyed a relative calm in terms of censorship and control of its Internet usage, despite having other regulatory issues related to radio spectrum distribution and media diversity. This is without considering an incident in which a Twitter user was arrested for “inciting financial panic” and sent to jail in what truly became a political scandal. The man’s sentence was later overturned.

Although connectivity is low and its broadband access is considered the worst on the continent (less than 4%), Guatemala enjoys a high level of mobile connectivity. To this day, there is only a single draft law on the protection of personal data, which has been abandoned since 2009, plus a few other scattered laws on social networks.

Nevertheless, there are two laws, which somehow go unnoticed for most of the authorities, which actually govern online activities. The Protection of Children and Young Persons Act (PINA), which has the traits of a public order law, stating that children have a right to be protected from harmful information, together with the Mobile Terminal Equipment Act, which imposes a registry of cell phone users, creating databases of phones associated with personal identification documents. The latter can also be applied without a warrant in order for the authorities to obtain information about the location and identity of users and calls. This law also establishes the crime of conspiracy through the use of electronic devices, even if the crime has not been committed, opening the possibility for electronic surveillance of all kinds.

In early September, after an increase of activity in Guatemala surrounding the application known as SECRET, the Vice President of the nation, Roxana Baldetti, announced the urgent need to take action on this matter in order to “protect” children from the dangers of this application, which she branded as a tool for spreading “sexual violence, child pornography and bullying”.

The vice president then delegated the head of the Telecommunications Authority (SIT), who acts as the regulator of companies providing mobile services and Internet telephony, with the task of addressing this issue and

¹⁶ Renata is the global campaigns manager for the Web We Want initiative of the World Wide Web Foundation.

requested the acquisition of equipment to carry out a comprehensive program which would identify the users of the SECRET application, including their geographical location and personal identity. More than a month after these statements, nothing appears to have been registered on the SIT transparency website regarding the acquisition of such equipment.

A government coalition was established, consisting of the Attorney General, the Attorney-General's Office, the Presidential Commissioner for Transparency, e-government and the Superintendent of Telecommunications. Its mission was to request that, through a court order, the distribution of the application would be suspended in Guatemala.

This joint action was followed by an unfortunate announcement made by the Executive on the regulation of social networks in Guatemala, through the inclusion of amendments in the Bill of Computer Crimes, which had been pending for further discussion and approval, by adding the Moral and Integrity Law for Computer Based Communications. The text has not yet been published by the Congress of Guatemala and in a country where the use of social networks increases by the day, it poses a great risk of censorship and control, particularly as we approach 2015, when the country will have its next general election.

However, there is still no injunction prohibiting SECRET. The threat of application regulations could possibly be requested by the Executive agency or through a court order via a new law.

Supporters of the measure, such as the Nomada newspaper, consider that banning the application is a correct measure, due to its use in Guatemala to denigrate and destroy the reputation of women in a country where levels of violence and the murder of women are among the highest in the world.

However, the general view among journalists and lawyers is that the regulation of social networks could erode citizens' privacy during critical times, both politically and socially. The legal framework of Guatemala, which generally includes regulating libel and slander, child abuse and verbal violence against women, make it unnecessary to administrate such specific topics given that illegal conducts are already criminalized regardless of the means used to perpetrate them.

It also opens the opportunity for those in power to pursue and monitor opponents and critical voices. Moreover, it is questionable whether this type of regulation on social networks will substantially modify violent and demeaning social behavior, which are not exclusive to the use of an application, but seen every day as part of general social behavior.



PART
2

**FREEDOM OF
EXPRESSION**

An opinion in favor of freedom of expression on the Internet

*Eleonora Rabinovich*¹⁷ and *Atilio Grimani*¹⁸

The opinion of the National Attorney General in the *Da Cunha* case regarding the responsibility of Internet intermediaries could be the first step towards a Supreme Court case which will impact the entire region.

In Argentina, the issue of responsibility of Internet intermediaries became visible as a result of a number of legal actions against Internet search engines, actions which have collectively created a jurisprudence which is very problematic for freedom of expression.

Judicial cases from recent years have generally involved celebrities complaining about the unauthorized use of their images by third parties or the linking of their names with webpages with reprehensible content. More than 150 cases of this nature have been filed. In these cases, plaintiffs have generally requested the elimination of the link between their name or image and the webpages which supposedly harm them. In some cases, plaintiffs have sought economic compensation for damage. These demands have occurred in various procedural stages.

Until now, there have only been two decisions involving the liability of search engines. Most cases until now have addressed protective measures which erase the results of searches that actors consider violations of their rights.

The first, and probably most emblematic, case to arrive to the Supreme Court was *Da Cunha*. In *Da Cunha*, actress, singer and conductor Virginia Da Cunha filed lawsuit against search engines Google and Yahoo! alleging they had damaged her image by linking her name and image and webpages with sexual, pornographic, and prostitution content.

The lower court ruled in favor of Da Cunha, arguing that even though they function automatically, search engines know and select the shown data, thus “participating in content selection”. The judge held that the liability of the search engines was based on the fact of *facilitating* access to offensive content. The judge, however, overruled the issues of liberty of expression and

¹⁷ Public policy professional specialized in Internet policy, media regulation, Human Rights and freedom of expression.

¹⁸ Assistant program manager at Google.

the right to information, arguing that they do not constitute an absolute right and allow for restrictions upon abusive exercise. The decision was repealed in the Chamber of Appeals, which found that it was impossible to fault the search engine and consequently reverted the order to compensate Da Cunha.

On August 22nd of this year, the National Attorney General delivered an opinion of the *Da Cunha* case ([here](#)). Deputy Attorney General Laura Monti delivered a comprehensive opinion in which she considered the multiple facets of the case, stating that search engines were not liable, subjectively or objectively, for the content published by third parties.

After reviewing the regulations which apply to the case, the manner in which search engines technically operate, and the form in which they recompile information on the Web, Monti considered that the Argentine legal doctrine of “Campillay” applied. The “Campillay” doctrine, which the Argentine Court established several decades ago to protect the press when it acts as a *mere intermediary* of information generated by third parties, establishes that the press is not liable for the information it reproduces as long as it does so accurately and properly attributes it to the pertinent source.

Monti’s opinion maintains, in line with the “Campillay” doctrine, that these search engines are not liable for controlling the content. She also acknowledges the undeniable role they play in the organization of information and its consequent accessibility. To the contrary, the dictamen affirms that holding intermediaries responsible for content generated by third parties would inhibit freedom of expression and public debate, providing more incentives for self-censorship. Two years ago, the Association for Civil Rights (ADC) presented an *amicus curiae* in the case which referred to the aforementioned arguments.

The National Attorney General aligns its opinion with the UN Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression ([here](#)), the joint declaration of various freedom of expression rapporteurs ([here](#)), and local civil society agencies.

While the opinion could represent an important step towards the protection of Human Rights and liberty of expression in particular, it is not legally binding, and, thus, cannot guarantee that the Court will adhere to it. Expectations are high: the Court’s decision will be crucial to modifying a problematic civil jurisprudence and clarifying the constitutional principles at stake. This case will ultimately be an important milestone in legal discussions of freedom of expression not only in Argentina but also in other countries in the region.

Freedom of expression violations on the online environment

Heloisa Padija,¹⁹ Julia Lima²⁰ and Laura Tresca²¹

On the online environment, freedom of expression violations can be defined out of the wide range of variables which are commonly linked to the web, such as web neutrality violations, surveillance practices, restrictions to file sharing, among others. Besides the specific violations, serious Internet-related crimes, such as homicides, attempted murders, death threats, kidnaps and disappearances, are also frequent.

What has been traditionally associated to journalism is now extended to people that elected the Internet as their main tool of expression, for instance, bloggers, owners or editors of websites and Internet users. There are notable signs which indicate that those violations have the potential of getting more and more intense against these communicators, who are generally individuals acting autonomously, without any support from the big companies of the communications sector. This reality is not an exclusive trace of a single country; it certainly corresponds to a regional panorama. Thus, bloggers' and users' rights to protect themselves and to fully assure their right to freedom of expression on the Internet become an emergent theme concerning web governance in the region.^[1]

In 2012, Article 19 did the entire registration of the gravest cases of freedom of expression violations on the online environment in Brazil and produced a report called "Threats on the web" ("Ameaças na rede"). The report aimed to characterize and to dimension the challenges of online freedom of expression in Brazil through the victim's perspective and accounts. Unfortunately, the threats exceed the scope of judicial censorship. Journalists and bloggers are victims of frequent physical aggression, death threats and murders because of what they say on the Internet.

Article 19's research found sixteen cases of serious threats to freedom of expression in 2012. It is important to notice that it was performed an investigation in which the cases made available to the media or

¹⁹ Works in Article 19.

²⁰ Works in the area of research and analysis of the Freedom of Expression Program of Article 19. Graduated in Public Relations at University of São Paulo.

²¹ Master in Social Communications and Journalism at Universidade Metodista de São Paulo (UMESP). Social scientist at University of São Paulo (USP).

communicated directly to the research team were monitored and posthumously analyzed. Hence, despite all the efforts, the “threats on the web” report is not exhaustive: there may be cases which weren’t spotted or communicated to the organization.

The sixteen registered cases of serious threats correspond to three homicides, three attempted murders and ten death threats against communicators that disseminated information, ideas and opinions on the web. The case analysis pointed out some important quantitative and qualitative aspects in order to clarify some vulnerability patterns which are favorable to the occurrence of freedom of expression violations.

About the regional aspect, the research demonstrated that the Center-West region leads the violation’s ranking, representing 43.45% of the total amount of grave offences to online freedom of expression. There were seven cases of serious violations in the region, followed up by four cases in the Southeast region and three cases in the Northeast. The North, Northeast and South regions presented fewer occurrences. However, it is important to remind that the North and the Northeast are the Brazilian regions in which it is more difficult to find households with access to the Internet and this fact can influence directly on the low quantity of violations in these regions.^[2]

Other important aspects that were perceived during the case analysis are the gender, the motivations and the profile of the offenders. Concerning the gender of the victims threatened in 2012, 81.25% of the violations were performed against men. The quantity of violations made against women - which were three throughout the year - occurred through death threats.

A relevant fact that can help us understand why there are less freedom of expression violations against the female gender is possibly the minor quantity of women that possess sites and blogs or express themselves professionally on the Internet (comparing to the quantity of men that do so). Moreover, the female gender suffers from other types of hostilities that culminate in self-censorship and inhibit expression in a more preoccupant way, since they are not occurrences that resonate inside society in an equally impacting manner, mainly if we compare them to the serious violations inserted in the report.

On the motivations, the complaints were the major type of content that led to retaliations against the victims, presenting themselves as an element

of motivation in 11 cases. Other contents that provoked violations against bloggers and journalists were criticism, opinions and information reproduction.

At last, we can also remark that the State is involved in the majority of the analyzed cases, through the hands of politicians that occupy official positions in different spheres of power, mainly in more local and policed levels. Together, these two actors represent 62% of the serious cases of freedom of expression violations. The offenders that are not related to the State are linked to other functions, such as entrepreneurship and organized crime, each representing 19% of the cases.

The identification and the deep analysis of a problem are preliminary phases in the adoption of measures which can be able to solve it. The report cited in this text expects to give the necessary visibility to a very serious problem in order to incite authorities' actions, preventing future problematic cases and giving a solution to the old ones. Besides the non-violation of Human Rights, the State is also obliged to take positive measures to prevent any kind of attack that aims to silence people on the web, even if the violent actions are performed by other actors. Therefore, we do believe that this theme is becoming an emergent topic on web governance in the region.

[1] The topic will be discussed in a workshop organized by UNESCO, CELE and Article 19 during the IGF 2013.

[2] The data were taken from a research made by Cetic.br, a CGI organization responsible to the analysis of the web behavior in Brazil, concerning the year of 2012. The research can be accessed at the following link: <http://www.cetic.br/usuarios/tic/2012/A4.html>.

Paraguay: democracy and freedom of expression in digital justice

Yeny Villalba²² and Natalia Enciso²³

The fragile protection of freedom of expression in Paraguay and its limited development on the Internet is just another indication of how slow the consolidation process is in the transition toward a democracy that is respectful of Human Rights and a State that guarantees digital justice among its residents.

²² Legal consultant at Centro de Estudios Judiciales del Paraguay.

²³ Attorney at Law and Public Notary at Facultad de Derecho y Ciencias Sociales, Universidad Nacional de Asunción.

In other words, while this premise is not new, the more the Internet and potential social infrastructures develop for the full enjoyment and exercise of freedom of expression without discrimination – together with other recognized rights –, the greater the possibility of a social rule of law; of a country founded on democratic values that extend beyond dogma and propaganda and where obstacles are prevented – including those arising from “indirect means” for violating rights, such as a lack of infrastructure for a free and neutral internet, and any element that reveals or “blocks” the quality of the democratic model being sought.

Transition toward democracy with a transition toward digital justice?

Paraguay has been undergoing a long transition toward democracy (1989-2014) that has extended almost as long as its prior dictatorship (Alfredo Stroessner 1954-1989), in a scenario in which the internal debate focuses on other priorities (such as current levels of social inequality, poverty, extreme poverty and tributary injustice, among other things), and the issue of digital justice is relegated to a small corner in the shadows of Paraguayan democracy.

This is not only because Paraguay still lacks specific legislation for protecting digital justice and opening its channels for exercising the right to access public information, but also because of the permanent criminalization of activists that mobilize freedom of expression and public interest on issues that supplement the digital agenda. In this context, digital law is practically excluded from reality and public debate. Paraguay is the country with the lowest alternation of government in the region and whose standards are so minimal that it differentiates itself from all other Latin American countries. Another differentiating factor is its limited number of actors, which hinders a mature discussion on Internet rights or the digital agenda in government programs, without losing sight of the comprehensive nature of the Human Rights that make up the fragile social reality of Paraguay.

In order to speak of a digital transition in the Paraguayan scenario from a digital rights-centered point of view, it is convenient to first relate and contextualize the last elections that took place in April 2013, which were characterized by cases of criminalization and tension revolving around lack of transparency. Meanwhile, the public interest debate occurred through limited tools that are available online. The fact is that citizens who are using technology are openly expressing their views online and are demanding transparency and effective management of public assets, while focusing their criticism – as can be expected during electoral campaigns –

on candidate profiles. In a participative and plural democracy, all this should simply be part of ordinary life, people should be able to express their thoughts without drawing attention to themselves or taking risks or extraordinary measures, but that is not the case in Paraguay.

The country's weakened democracy has created a hostile scenario for an angry public, where electoral candidates have generated negative precedents when trying to "make examples" out of certain cases and preach the importance of "keeping quiet", turning anything that is said against them into a case of "defamation and libel" through a weak legal interpretation that is particularly dangerous in electoral times.

There were no "politicians" in the April 2013 elections in Paraguay whose proposed government programs focused on the debate or the insertion of standards for accessibility, technical development, diversity and increasing capacities for the exercise of all rights, nor focusing on respecting freedom of expression, privacy or other issues in the global digital rights agenda. That is why I am using this election, the importance of which exceeds the change in government administration, as a segment in the history of Paraguay that illustrates and links freedom of expression to the digital agenda; as it has even led the Inter-American Court of Human Rights to sanction Paraguay for criminalizing activists and subtly "blocking" their liberties.

In the electoral context, third-party accusations should have led candidates to seek transparency and clarity and to expose the truth in the public arena, taking advantage of the political game to bring out the best in each candidate; however, the possibility of pressing criminal charges for libel and defamation proved to be too strong a temptation and, in addition to serving as a form of intimidation, this recourse to judicial remedies exposes and reveals the harsh reality perceived in the collective imagination: that one must be afraid to speak up, write notes, post or tweet without "sufficient proof".

Long before the last general elections in Paraguay, in the 1993 elections - when candidates included the future first president since the dictatorship, representing the usual political party (*i.e. Asociación Nacional Republicana - Partido Colorado*) versus Civil Engineer Juan Carlos Wasmosy (now lifetime senator) - the first case was filed before the Inter-American Court of Human Rights against Paraguay for allowing a candidate to undergo criminal charges after the elections for his statements regarding public interest issues. This case was preliminarily analyzed in relation to freedom of expression and, once accusations were confirmed, the Court decided against Paraguay on the basis of proven violations to the American Convention on Human Rights; this

decision issued on August 31st, 2004 in “*Ricardo Canese vs. Paraguay*”, marks the first international precedent focusing on transparency in the electoral race, the right to freedom of expression and truth as a public interest.

However, throughout 2013, there have been situations that affected freedom of expression and Paraguay is still at risk of new sanctions like those in the Canese Case. Lower profile precedents than those in the Canese case reveal that the defense of the legitimacy of internet rights and liberties urgently needs to find its way into the social agenda.

Leaked reports that serve as “examples”

With lack of specific norms constituting the perfect excuse to limit access to public information that could result in “evidence” and information that is almost always followed by denouncements and the full exercise of the right to freedom of expression, and given that what is at stake are public interest issues based on general principles of civil and criminal law that are more evident during elections, local media have leaked information on congressional candidates who indirectly hinted that they will take the time and trouble to identify individuals that leave messages in public interaction forums. A controversial example of this is the complaint filed against a politician from an opposing party in an electoral area of the interior of the country who was ultimately subject to conviction.

According to reports leaked by the local media.

“... senator Juan Darío Monges (ANR) filed a complaint against the liberal lawmaker, and former mayoral candidate, Jacinta Barreto, of Sapucái, Monges’s birth city. In his complaint, the senator claimed that Barreto had allegedly accused him of “being a petty thief” [abigeo] on Facebook during a political campaign where she was running for mayor of Sapucái in February of that year.

Barreto denies having ever made such an accusation against him. In fact, she issued a public apology – also via Facebook – claiming that “someone else” (such as a hacker, for example) had used her profile to make the accusation.

She also stated that everyone knows she comes from humble beginnings and does not have the necessary financial means to “clear the senator’s image” by paying the fine in question.

On February 16, Héctor Ovidio Cáceres, Darío Monges's protégé, won the electoral race in Sapucaí. Liberal candidate Jacinta Barreto lost by nearly 500 votes..."

Another eloquent case is described in the newspaper ULTIMA HORA DIGITAL "[...]

Representative Oscar Tuma requested, via Facebook, information on a person that had published his personal phone number via Twitter last Saturday, sparking controversy throughout social networks. The person who published Tuma's personal phone number was Male Bogado (Twitter handle @fanquifungus). Below is an excerpt of the article:

Among other things, this former Oveidist tweeted: "Look at public TV... so f*** funny, hahaha, so many clowns talking." "Now there's a ridiculous woman on the air. It's like a sitcom." "These fools still have no clue what's going on. Someone should tell them the country has a new administration. They should flee to Cuba." In addition, he referred to Cristina Fernández de Kirchner, President of Argentina and Dilma Rousseff, President of Brazil, as "hysterical women."

Male Bogado told ULTIMAHORA.COM that what the Representative said via Twitter was disrespectful. "He expressed himself in a very derogatory way," he stated.

He questioned whether a public figure and government representative like Tuma could express himself in that way toward his political rivals. When he heard that the senator was trying to find him online via Facebook, Bogado claimed that if they really wanted to reach him, they should have done it privately. "The fact that he's making it public indicates that he's not serious," he stated. Following the strife, Male Bogado made his Twitter profile private so that only his followers can read his tweets. He explained that the reason for this was that Tuma sympathizers would probably follow him, since there were already Facebook users who were expressing ideas in favor and against him. Bogado's tweet via @fanquifungus was retweeted several times. This proved, according to him, that there are people

out there who “dislike” him. “Many joined the public flogging,” he added. The power of social networks should never be underestimated. However, he claimed it makes him sad to see that Tuma sympathizers “publish inappropriate posts.” He believes that if people wished to behave violently, they would have done so already or found out his address. Tuma was ultimately able to find @fanquifungus, but has not yet contacted him to date.

For his part, Óscar Tuma believed any kind of argument would be in vain. “No criminal charges have been pressed, but I forwarded the statements that were circulating in social networks to the Ministry of the Interior,” he said to ULTIMAHORA.COM.

Similarly, cases of “content blocking” and “site redirecting” transcended because of their social impact and because they constituted a negative precedent; for example, victorbogado.com and partidocolorado.org were taken down by the governmental communications department known as COPACO and later abc.me users were blocked by the ISPs TIGO and PERSONAL.

Another widely broadcasted case in local Paraguayan media was that involving members of the Association of Internet Users who run the sites victorbogado.com and partidocolorado.org, which are public interest sites that published information on inconsistencies in the Representative’s administration and history during the elections. The day after publishing their posts, the site administrators realized their site had been blocked and users were being redirected. Users noticed it was COPACO that was redirecting them and, after confirming the event, denounced the censorship in every available media.

Similarly, another situation that startled users was when phone companies and ISPs blocked www.abcolor.me; as was pointed out at the time, this violated administrative norms pertaining to concessions for operating internet services established by the State agency Conatel. Both phone companies later issued an apology and stated that they had unblocked the site due to online pressure from users; however, information was later leaked that a third party had filed a complaint against the individuals who had published the post in question.

In Paraguay, the Joint Declaration on Freedom of Expression and the Internet, in relation to filtering and blocking, has not been widely diffused nor

referenced by users; however, it has been resorted to for making defenses and filing complaints in some cases, although surrounded by the pressure that is usually implied in expected reactions and by the absolute partiality of ISPs. Let us review section 3 on filtering and blocking; as applicable to the cases mentioned above: “a. *Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse*”. And “b. *Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression*”.

Incorporating the need for recognizing technology as an unlimited resource for social justice through digital rights, as well as the existence of a directly proportional relationship between that need and “letting people do” with minimal standards, constitutes a pillar of digital justice that enables citizens to exercise their freedom of expression. The traditional view “to each his own” must be ensured, but not in a context of hostility between citizens and the authorities.

Open internet and freedom of expression in a framework of digital justice for all without distinction ultimately plays a key role in the political agenda; when absent, democracy is weakened because civil society cannot interact with the State or overcome inertia, thus rendering it impossible to have a dialog with the authorities.

Would demanding a clear agenda and dialog enable us to overcome the precariousness of the current debate and post-dictatorial fear and authoritarianism? How do we overcome the authoritarian and extremely paternalistic tradition, remnant of the dictatorship, while coming out of the darkness and bringing digital justice with us?

There is hope for promoting the digital agenda and strengthening Paraguay’s civil society on public interest issues. To that effect, a Chapter of ISOC was recently created in Paraguay, and there are other organizations that are embracing political ideas aimed at promoting digital rights, digital justice and freedom of expression. However, there is still a long path ahead in terms of negotiations and consolidation, particularly in achieving the technical support and cooperation that is needed to grow in par with other States and to finally overcome Paraguay’s internet “*neo feudalism*”.

A key tool in the struggle for a free Internet

Ramiro Álvarez Ugarte²⁴

The Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR) has published the report *Freedom of Expression and the Internet*. This report probably constitutes the main legal and constitutional tool to advance the struggle for a free and open Internet in the Americas.

The report is neither an international treaty nor directly binding on States. However, it is an official interpretation of the American Convention on Human Rights issued by one of the system's bodies. What it does is extend to the digital world the generous standards on freedom of expression developed by the Inter-American system throughout decades.

The report is extensive and comprehensive and includes standards and principles of Human Rights and good practices. It draws on what exists and points to possible and, on occasion, necessary directions to protect the right to freedom of expression on the Internet. It covers issues such as net neutrality, access, privacy, cybersecurity and responsibility of intermediaries. And in each of those issues, it explains what the system's current Human Rights standards have to say.

These kinds of IACHR reports have historically been useful in the defense of Human Rights. In several countries, international treaties are directly applicable and, in many cases, have constitutional status. Some even argue - at a constitutional, statutory or case law level - that the interpretations issued by international treaty-making bodies require attention. That is why this report is relevant: it is a kind of soft law that has proven very effective in the past.

Civil society organizations need to bear in mind what we do to be able to fully comprehend the importance of this report. In fact, activists interested in making the Internet a free and open space generally act outside the formal structures of the State. We have no political affiliation

²⁴ Ramiro Álvarez Ugarte is the Areas of Access to Information and Privacy in the Association for Civil Right's director (ADC).

nor run for elections. Our political action takes a different form: we seek to persuade our public officials that the principles we hold are true and that they, in turn, must lead judicial decisions as well as political and regulatory options that take these issues seriously.

This persuasion policy is how we have been making our rights-based claims for decades: movements for civil rights, indigenous rights, women's rights and LGBTI rights are proof of that. We have limited resources and combine them in different ways: while some are engaged in organizing the public and launching public communication campaigns aimed at our representatives, others prefer direct lobbying; while the rest of us use the courts as a platform for submitting our demands to the State. The rights invoked in our agendas are **one of the most valuable resources we have**. And in democratic societies they tend to be powerful arguments in our task of persuasion. The Commission's report significantly strengthens this resource for at least two reasons.

First, it allows us to unify the discussion at the regional level. Principles that were once scattered are now contained in a single document that articulates them in light of Inter-American standards. Issues that once posed questions or dissimilar criteria are clearer now. The report is an essential first step in generating a genuine regional discussion about the future of Internet; one that could – and should – have an impact on the broader discussion that is currently taking place in global forums.

Second, it opens an additional advocacy space. The Commission usually follows-up on its own reports, which means that it and – ultimately – the Inter-American Court will constitute arenas in which to continue to advance the Internet freedom agenda. The Inter-American system creates a great incentive for the coordination of tasks at the regional level: it invites us to cross borders and take a broad perspective that includes other countries.

The Inter-American system has been a space for strengthening the struggle for Human Rights, especially in Latin America. We celebrate the fact that the struggle for a free and open Internet has been welcomed into that space.

Freedom of expression on the Internet: opportunities and challenges for Latin America

Eleonora Rabinovich²⁵

The right to freedom of expression has been defined as “the fundamental pillar” of the democratic system. It has been subject to generous interpretations issued by the organs of the Inter-American Human Rights System (IAHRS). As a result, high standards for the protection of such right have been created.

Such standards offer an appropriate regional framework when thinking about the exercise of freedom of expression in the digital area. The “dual dimension” - individual and collective - of the freedom of expression allows its scope to be reinstated in order to deal with current situations in different countries of Latin America arising as a consequence of cases of inequality in the access to technologies and cases of policy decisions, legal regulations and judicial decisions which tend to limit the expression on the Internet. On the other hand, the wide recognition of the freedom of expression, in all its forms and manifestations, also becomes useful to assess the forms to exercise expression which are specific to an interactive and multidirectional media such as the Internet.

The Special Rapporteurship for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR) addressed, in the past years, several of the different aspects of this phenomenon. It did so through Joint Declarations - with the UN Rapporteurship, OSCE and the African Commission on Human Rights - and through a specific chapter in its last Annual Report.

In such report, the Rapporteurship develops valuable principles to protect the right to freedom of expression in the digital area, including topics such as net neutrality, intermediaries' liability, the locking and filtering of contents, the relation between privacy and surveillance of communications, and the access to the Internet, among others. The Rapporteurship emphasizes that Section 13 of the American Convention on Human Rights - which proclaims the right to freedom of expression - is “fully applicable to communications, ideas and information one can spread and have access to via the Internet”. Likewise, the Rapporteurship highlights that the online environment does

²⁵ Deputy Director, Asociación por los Derechos Civiles (ADC).

not only make it easier to exercise such right, but it also provides the best conditions for the exercise of other fundamental rights, such as education and freedom of association.

During the hearing held in the IACHR the past October 28th – where a group of organizations expressed our opinions regarding the impact of the Internet in the exercise of Human Rights – from ADC we talked about the main challenges and opportunities which arise within the region regarding the validity of the principles developed by the Inter-American Human Rights System with respect to freedom of expression.

These are some of the risks we highlighted:

- 1** Within the region, the extent of Internet intermediaries' liability regarding the user generated content is being discussed. In some countries' case-law, intermediaries were held liable. The penalties have ranged from precautionary measures which ordered the elimination of certain search results to compensations for damages of different amounts.
- 2** Legislative or judicial discussion regarding the elimination of contents any individual may consider inappropriate is also a concerning trend within the region. In Colombia, for example, the Constitutional Court analyzes a case in which a court of appeal ordered the newspaper El Tiempo to remove an article which showed a judicial investigation.
- 3** There are judicial and administrative decisions which represent a clear step backwards the Inter-American standards. One example is seen in the excessive use of criminal law and civil law to silence critical opinions regarding public interest topics; another example is seen in the excessive use of copyright. Likewise, there are legislative discussions that do not take into account the principles of the IAHRs properly. In Ecuador, for example, the Communication Law limits anonymous speech. In Argentina, a bill intended for the protection of sexual exploitation victims may allow the elimination of legal contents.
- 4** There are examples of countries in Latin America where governments have blocked public interest content on the Internet. Positive trends showing us the opportunities regarding legislation and public policy within the region can also be found. The Brazilian Civil Rights Framework for the Internet is one of them. The recent ruling of the Argentine Supreme Court regarding intermediaries' liability is another.

In the next years, these and other discussions will have to be solved. The Inter-American Human Rights System provides us with powerful tools to achieve an outcome in terms of regulations and policies which respect freedom of expression.

Spam elections

Eduardo Magrani²⁶

The Internet can and must play a more significant part in the electoral period. In order for this to happen, the democratic potential and communicative effect of digital platforms, as a result of their own characteristics, must be recognized by both the State and its citizens.

Recently, Jeferson Monteiro, who created the ‘Dilma Bolada’ profile on different social networks, temporarily took down its Twitter and Facebook pages in fear of being made liable for influencing voters during the current election period. At the same time, the different parties began to implement such tools as spam text messages and automatic posts on social networks, paving the way for a strategic, digital guerilla dispute.

Both of these movements demonstrate, on one hand, how digital environments have been flooded with pre-programmed robotic expressions, aimed at convincing the voters; and, on the other hand, how their true potential to be an arena for public debate is not being realized. Peoples’ fear of being liable for any comment and the lack of a solid culture of freedom of expression, have a cooling effect on the debate, which hinders the maturing of online discussion and deters the free manifestation of opinions in digital environments.

The Internet can and should play a more significant part during the electoral period. But this depends on the recognition of the democratic potential and the communicative effect of digital platforms, as a result of their own features, for the State as well as for its citizens.

The lack of comprehension of this potential becomes evident when searching for any existing regulation of such spaces. For example, electoral legislation, when dealing with the right of reply on the Internet, limits the response to an offensive comment to the same size and the same time. This makes sense if we think in terms of TV and Radio, but it makes very little sense when we think of social networks. One of the main characteristics of the Internet is precisely the flow of information it allows for, with fewer limitations and a lot more freedom to argue and counter-argue. The right

²⁶ Professor of Law and Technology and Intellectual Property at School of Law at Fundação Getulio Vargas (FGV). Researcher at the Center for Technology and Society (CTS-FGV). Project leader on E-democracy and Internet of Things. Brazilian Coordinator of Creative Commons and the Digital Rights: Latin America and the Caribbean project.

of reply is already embedded in the very logic of social networks and the Internet, without restrictions of size or time.

If this arena continues to be incorrectly regulated during electoral periods, reducing its communication potential, dominated by pre-programmed spam and by citizens' – and candidates' – auto-censure, it's society who will lose by unnecessarily limiting its own right to access information and freely express its opinions.

Why obliging self-identification is wrong for freedom of information

Gregory Michener²⁷

Let's assume you are a citizen of a Latin American country that has recently enacted a freedom of information (FOI) law. This is a likely situation; all but three Latin American countries have implemented some type of FOI measure over the last decade (with the exception of Costa Rica, Venezuela, and Paraguay). If your law is any good (which most are), it should empower you with the right to ask and receive information from government on most everything, barring certain standard exceptions. If it's a good law, it also obliges your government to put certain important types of information online. If you happen to be in Brazil, like me, you can ask for your information in machine-readable open formats. According to the Center for Law and Democracy's Right-to-Information Rating, Brazil's law is among the fifteen most rigorous in the world.

Endangerment and discrimination

Let's also assume that you, citizen, know about serious corruption going on inside your city government and you want to do something about it. The problem is that whatever information you ask for using the law – the sort of information that may prompt an investigation by higher authorities, for example – you must provide your name and social security number (CPF) to the (dangerous) local authorities. This information can cost you your personal safety or that of your family. What do you do? You probably do not make the request in the first place.

²⁷ Greg Michener is an assistant professor at the Brazilian School of Public and Business Administration (EBAPE) at Fundação Getulio Vargas (FGV), in Rio de Janeiro, Brazil.

The need to provide a veridical name and identity number is required by only five of Latin America's 14 freedom of information measures: those of Brazil, Ecuador, Nicaragua, Panama and Peru. Of these laws, only two appear to be actually operating with minimal functionality – those of Brazil and Peru. Given the challenges of making FOI laws work in the first place, why impose obstacles such as the necessity to self-identify?

Let's assume a milder hypothetical situation. The water your building receives from the city is dirty. You file a FOI request with the local water authorities and the relevant regulator. The information officers in these agencies receive your request and Google your name – out of innocent or calculated curiosity. Based on your Facebook profile and the fact that there is nothing else about you on the internet, they guess you are a 'nobody,' and answer with only basic, incomplete information that requires little effort on their part. Now let's assume you're a journalist from a powerful news organization. After the information officers receive your request and Google your name, they provide detailed information because they fear that lesser information will prompt you to launch an appeal and make the agency look bad.

What type of fundamental right requires self-identification?

If at all possible, government officials should not be able to discriminate based on a citizen's identity, as illustrated above, nor should they be given the opportunity to intimidate a citizen. In effect, the obligation to provide one's identity to exercise a fundamental right – the right to information – strikes a dissonant chord with international norms and national constitutions. In most countries with better practice laws, using your own identity is optional. You can provide an email like mickeymouse@hotmail.com and that is all you need. Why is a social security number necessary to exercise a fundamental right? This obligation is legally equivalent to having to register your social security number before assembling a group of friends in a public place or writing an editorial for a newspaper. These rights – the right to assemble and the right of freedom of expression – do not require social security numbers, so why does the right to information?

The need to eliminate the need to self-identify is urgent, particularly so in Latin America and other developing regions. Unprofessional administrators, patrimonial governments, and administrations infiltrated by criminal organizations present serious risks to the practicability of freedom of information rights. It is ironic that the obligation to self-identify renders the governments most in need of public scrutiny – such as those involved in illegal activities – the least likely to be brought into the light of day.

Googling requesters and intimidation tactics

All of the above claims, about intimidation, Googling requesters, and differentiated responses based on identity, come from my experience in Brazil or my research abroad. In the case of Brazil, it is a well-known fact that many municipal governments – particularly outside of the larger cities – are associated with paramilitary organizations that run protection rackets or drug trafficking businesses. Similar situations occur in parts of Colombia, Guatemala, Honduras, and Mexico, among other countries in the hemisphere. In a conversation with the former Director of the Regional Alliance for Freedom of Information and Expression, Karina Banfi, it became clear that the need to self-identify is not an isolated problem; it is a generalized intimidating mechanism that is retarding the use of laws throughout the region.

A member of a Rio de Janeiro-based nongovernmental organization told me a sad story. The organization was conducting transparency evaluations of a town on the outskirts of Rio de Janeiro, but the initiative had one major flaw: citizens refused to participate. Citizens knew that those in government were crooked and dangerous, and the need to self-identify dissuaded them from collaborating in the transparency audit.

FOI often meets with hostility from public administrators, even in the most advanced democracies. The antagonistic relationship between public servants and requesters is as unfortunate as it is well documented – I even wrote a white paper that briefly examined this dilemma, before the Brazilian law was enacted in 2011. The important question to ask is why we design laws that give public servants a target for their antagonism. My students – many of them public administrators – tell me that Googling requesters is common practice before processing a FOI request. They also tell me that they try to provide requesters with as little information as possible, which depends on their identity.

Many public administrators have strongly negative feelings about FOI laws. In some instances, this negativity appears to be the result of a culture where the state historically reigned supreme and is now supposed to be at the service of citizens. The obligation to self-identify implies the following question: “if you’re going to question the state, then the state has the right to question you. Who are you, and what is your grievance, anyway?”.

In the case of Rio de Janeiro state, this sort of “state regarding” attitude (as opposed to ‘public regarding’) is taken to the extreme. Not only does a requester have to self-identify, but s/he cannot send out an official request electronically. The requester must fill out a request form and present it in person, then s/he must sign a disclosure form that warns against the misuse of information at the risk of criminal proceedings. This is not just irritating officiousness, it is downright intimidation. If taken to extremes, the misuse of any information – whether it be governmental or not – can always lead to criminal proceedings in Brazil. This fact begs the question of why government should warn citizens about ‘misusing information’ only when they want to scrutinize government. If misuse of information is a generalized concern, why not conduct public awareness campaigns? Clearly, these are intimidation tactics.

Intimidation is not restricted to official procedures, however. A fellow researcher – who focuses on one particular federal policy area – was told by officials in his policy research area that he would have access to leading policymakers so long as s/he did not make any FOI requests. The antagonism public servants may feel towards requesters is perhaps inevitable, but it is not inevitable that this antagonism be directed and targeted. The obligation to self-identify makes targeted antagonism possible.

In conclusion

As far as I know, there is no movement to reform or remove the obligation to self-identify from statute. Ironically, Panama’s law just underwent a serious reform in 2013 (it was previously ranked among the worst laws in Latin America – it is now ostensibly among the five best), but the obligation to self-identify was not taken out of the law. The key to making FOI laws work, and to improving accountability in government, is to instill in citizens the habit of questioning government policy. If FOI laws intimidate citizens, we will never get to this point. The use of FOI laws is not only critical to fostering accountability in general, but it is also critical to pressuring governments to perfect access rights. No law is born perfect, and efforts to improve laws are especially critical in regions where political cultures are not necessarily amenable to political freedoms in the first place. At least not yet.



Guidelines for freedom of expression on the Internet in Latin America

*Alexandre Henrique Saldanha*²⁸

Recent discussions of the constitutional law analyze the existence of a new constitutional thought that emerged in Latin American countries. This new constitutionalism in Latin America arises from social movements that seek more democratic spaces to resize social participation in public management.

Recent experiences in Venezuela, Colombia, Ecuador, and Bolivia have led to such discussions, since their constitutions include forecasting tools for popular consultation and democratization of areas previously reserved to the government.

While it may be possible to argue about the emergence of a new model of constitutional movement based on recent experiences and from a few countries on the continent, it is noteworthy that such discussions are quite valid since they analyze the legitimacy of constitutional norms, using the theory of democracy as a parameter. Therefore, it is necessary to add the issue of freedoms on the Internet and the democratization brought about by cyberculture to this discussion. Regardless of a new constitutional thought in the Latin American continent, freedom of expression on the Internet in this region has been the object of analysis, including the Inter-American Commission on Human Rights, which, through its special rapporteur for freedom of expression, creates reports containing guidelines for American countries to adopt as informative principles for Internet regulation and its uses.

Through these guidelines, the committee suggests that each country adopts such principles as a benchmark in its legal treatment to the digital environment. Thus contributing to the greater expectations about democratic density typical of the discussions of the mentioned new constitutional thought in the region. Network access, Plurality, Non-Discrimination, and Neutrality are some principles suggested by the InterAmerican Commission on Human Rights for freedom of expression on the Internet, and each alone represents a proposal to guarantee democracy and social participation.

²⁸ PhD in Law from UFPE. Coordinator of the Law Course at Faculdades Integradas Barros Melo/Olinda. Professor and lawyer.

Access as an information principle represents a kind of obligation of each state to promote public policies to ensure digital inclusion, so that every citizen has access to information in cyberspace. Plurality in turn argues that the more voices that can interact by means of expression through the internet, the more democratic will be the discussions and information accessible through the World Wide Web. Nondiscrimination, on the other hand, aspires to be a guarantee that there will be no different treatment to citizens who access the Internet, since the most vulnerable will have the same access and interaction opportunity than the less vulnerable. Finally, neutrality at first ensures that there won't be censorship regarding the content to be transmitted and informed in cyberspace, as an access provider may not have such type of control.

One realizes how strong each of these informative principles of the inter-American committee are in terms democratic aspirations, with the purpose of enhancing dialogue and participation of various sectors of society, which coincides with the intentions of those who reflect on the mentioned new Latin American constitutionalism. Therefore, this article is only as a provocation, in the sense that any current issue involving constitutional rights and Human Rights should include the Internet and the rules that regulate it in the discussion, since there will not be enough democracy if fundamental freedoms are not guaranteed in the digital environment.

Political Internet censorship: a reality in Mexico (with a little help from the United States and GoDaddy.com)

*Luis Fernando Garcia*²⁹

The 1DMX website was censored for three months, without explanation and with the cooperation of the Mexican and American government, along with the complicity of one of the largest domain name companies in the world. What are the implications of political censorship on the Internet for the rest of the countries in our region?

On November 25th, 2013, the coordinator of National Digital Strategy announced the Mexican government's commitment to "fully respecting

²⁹ Luis Fernando Garcia is the lawyer of 1DMX and a specialist in digital rights.

freedom of expression on the Internet". A week later, on December 2nd, 2013, the government censored the 1dmx.org website.

This website was created a year before, on December 2nd 2012, a day after Enrique Peña Nieto was sworn in as president, a moment which was marked by police violence, arbitrary arrests and even a death involving the Federal Police. 1dmx.org was launched on December 1st 2012 as a portal for receiving, sorting and publishing videos, photographs and testimonies about Human Rights violations committed by the security forces.

A year later, the right to protest continued being systematically attacked in Mexico from the government and other sectors, so in the run up to the anniversary of the protests 1dmx.org decided to raise awareness on the erosion of civil liberties that have been occurring since December 1st 2012. They prepared themselves once again to document any likely abuses that could happen during the protests scheduled for December 1st, 2013.

However, on December 2nd, 2013, an email from GoDaddy.com (provider of the 1dmx.org domain registration) informed its board that the domain had been suspended for an alleged violation of the terms of use.

When requesting details about the alleged violation, GoDaddy.com reported in a second email that the suspension was actually part of an "ongoing police investigation" and stated that for further details they would have to contact a special agent of the Department of Homeland Security of the U.S. embassy in Mexico. When contacted, the embassy refused to provide any information.

Due to the participation of the U.S. embassy in Mexico, it was presumed that the request to suspend the domain came from a Mexican agency, therefore 1dmx.org requested a defense to fight this censorship in court, as it clearly violates the right to freedom of expression and they pointed the finger towards ten authorities as the likely suspects behind the order.

The lawsuit was then supported by a federal judge so the authorities were obliged to submit a report, either accepting or denying that they ordered the censorship, and from their personal case, justifying whether it was constitutional. To date, more than a month after the deadline for the authorities to send their reports, eight authorities have denied ordering the censorship of 1dmx.org. However, the Ministry of Interior and National Security Commission (technically part of the Interior Ministry) have refused to submit the report.

At the same time, an employee of GoDaddy revealed that the agency that requested the censorship was the Specialized Technology Response Center (CERT), an agency that is part of the National Security Commission. On March 4th, 2014, 1dmx.org decided to make the case public by conducting a press conference denouncing censorship, through the op1d.mx website.

Less than 24 hours later, the 1dmx.org domain was reactivated without GoDaddy.com reporting any official reasons. The authorities of Mexico and the United States have not made any public statement about this situation. The impunity of the perpetrators is being hidden and maintained behind the silence of those involved. One thing is incontrovertible: 1dmx.org was banned for three months. Internet censorship in Mexico is not a hypothesis but a reality.

This case in turn raises several issues that are worth thinking about, especially in face of the discussions on Internet governance, where it is becoming more and more frequent to use or invoke words associated to the legal language of Human Rights.

On one hand, this case clearly shows a real intention of the government of Mexico to restrict freedom of expression and undermine the right to privacy on the Internet. This intention continues materializing in the way of legislative reforms, such as the Code of Criminal Procedure, that increases surveillance powers without adequate safeguards; the project of modifications concerning copyright, which decreases the exceptions and limitations of copyright on the Internet, criminalizes users and establishes a system of censorship for alleged copyright infringements on the Internet; the upcoming Telecommunications Act, which in a filtered version reveals the intentions of further expanding the surveillance powers of the state, enabling Internet censorship and seriously compromising net neutrality. It is clear that the language of the Mexican government over its alleged commitment to Human Rights on the Internet does not have credibility.

It must also be noted that 1dmx.org censorship would not have been possible without the cooperation of the government of the United States and GoDaddy.com. This fact makes it clear that beyond the usual speeches on “Internet freedom” and public relations statements, it is essential for governments and businesses to establish transparent processes, based on Human Rights principles in order to manage government requests that compromise freedom of expression and privacy on the Internet.

Repeatedly, it has been suggested that the power of both the United States and the major Internet companies, based within its territory, are actually a boon for free speech on the Internet. With the approval of many, it is often referred to as “imperialism of the first amendment”. Maybe it’s time to revisit those claims, because in cases like that of 1dmx.org, it is precisely the extraterritorial element that has led to the possibility of there being an act of censorship (openly violating the prohibition of prior censorship unequivocally embodied in the Constitution of Mexico and the American Convention on Human Rights) and worse still, it has greatly hindered the possibilities of defense and punishment of those responsible.

The implications of this phenomenon should form an important part of the discussions on Internet governance which, until now, have been monopolized by voices and interests far removed from the reality of Latin America. If nothing is done, then events like the censorship of 1dmx.org will carry on affecting us and the erosion of freedoms that we have experienced on the streets of Mexico, will continue throughout the Internet in Latin America.

Documenting Internet blocking in Venezuela

*Marianne Díaz Hernández*³⁰

Although Venezuela does not appear in global Internet censorship reports, the country has a history of questionable practices regarding content filtering and user persecution for their online activities. Despite what you may think, the history of Internet filtering practices in Venezuela are not anything recent: it dates from at least 2007, when the first blocking of webpages were held by CANTV, the leading telecommunication company in the country, which was re-nationalized that year by President Hugo Chávez, who had just begun his third term.

From that year on, a series of practices (social media user detentions, blocking webpages by CANTV, controversial statements about social media influence in national politic and stability) began to be commonly used. Two people (with very few followers and almost no influence) were

³⁰ Marianne Díaz Hernández. Venezuelan attorney and storyteller, activist of accesolibre and legal leader of Creative Commons in Venezuela.

arrested in 2010 for writing on Twitter about the banking system, after a wave of interventions to financial entities on charges of “destabilizing the banking system” in the country. After the 2011 parliamentary elections (when the Minister of Telecommunications shut down the Internet throughout the country for about thirty minutes, claiming that the action was taken “to avoid the hacking of the National Electoral Council website”), a citizen was arrested for allegedly posting a photo on Facebook of electoral material burnt (corresponding to a previous election), despite it was clear that the user had not been the source of the circulation of the photo – already massively shared in social media. Websites like Noticiero Digital and La Patilla were temporarily blocked several times by posting certain content, such as reporting on fighting in La Planta prison. In 2013, after President Chávez’s death, all.co domains (related to link shorteners such Twitter) were blocked for two days, in an attempt to prevent the online propagation of an alleged recording of Chávez.

However, the current president’s administration, Nicolás Maduro, Chávez’ successor, has brought his own policy on digital media, in all appearance a previous and redoubled version. Since November 2013, when Maduro announced on live national television his decision to block any website containing information on the price of the parallel dollar (leading to block of between 500 and 900 webpages by CONATEL), his policy regarding this issue was clear. While blocking websites on the so-called “black dollar” goes back many years (with exchange controls going back from 2003), Chávez had simply limited himself to ban two or three emblematic websites, but he never carried out such a massive content filtering campaign.

In 2014, it was the turn of the protests. Since mid-February, when protests kicked off in the state of Táchira, and in March and April, when protests had their high points in major cities, the web was used to document, organize and report on them. In this way, the Internet had become one of the objectives to be controlled by the government through subtle practices, such as suspected bandwidth throttling (in which Internet connections were terribly slow during evening hours, when the repression of protests was increased and people resorted to the web for information due to the absent of media coverage in over-the-air television channel), and much more drastic measures. For instance, in Táchira, where protests were more intense, Internet was completely shut down for two days without any plausible explanation by authorities. The government also announced

deliberately interfering communications of Zello application, claiming that it was being used to plan protests and, immediately after, it was blocked. VPN applications as TunnelBear or anonymization apps as Anonymouse were also inaccessible.

Between February 14th and April 8th, 2014, the NGO Acceso Libre collected, through Herdict and with the support from users around the country, website blocking reports showing around 25 blocked webpages. From 2.155 individual reports collected, it was noted, among other things, that while sites such as those informing on the parallel dollar remained blocked at all operators, other websites were evidently inaccessible only through CANTV (e.g. Pastebin, PasteHTML and others). Something similar occurred with tools of VPN and anonymization such TunnelBear and Anonymouse that showed to be almost completely blocked in CANTV, as opposed to other operators.

While the government claims that these blocking are based on the Social Responsibility in Radio, Television and Digital Media Act (RESORTE-ME, in Spanish), the fact is that it contradicts international standards on Human Rights by granting content filtering powers to an administrative body under the Executive (CONATEL). According to RESORTE-ME law, legislation passed in 2011, ISPs are obliged to block all content that fits a series of vague situations such as “no recognition of the authorities” or “promoting breakdown”. Moreover, the norm does not comply with the principle of proportionality. It is worth mentioning that the OAS Joint Declaration on Freedom of Expression on the Internet states that filtering entire webpages is an extreme measure, which is justified only in serious cases, and that content filtering not controlled by end user is a form of prior censorship (a practice prohibited by the Venezuelan Constitution). In the same manner, the Joint Declaration establishes that “[c]utting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can never be justified, including on public order or national security grounds”. This also applies to measures such as throttling, which, as practices undertaken by the Executive during the 2011 elections, constitute a frontal violation of freedom of expression on the Internet.

Culminating 2014, protests have been almost totally exhausted, despite the circumstances that gave rise to them remain the same and no agreement was reached with the government. However, everything seems to indicate that Venezuelan online communication policies continue imperturbable: last week, for instance, two people were arrested for posting in Twitter

some messages related with the murder of the Socialist Party deputy, Robert Serra, and the news portal Infobae was blocked, in this occasion in a publicly and openly manner as stated by the President CONATEL.

The absolute lack of transparency regarding these procedures, and the tone in which the authorities express themselves in regard to digital media and social media (accusing them of contributing to the “psychological warfare”), coupled with measures such as the creation of the Strategic Center for Security and Homeland Protection (CESPPA, in Spanish), a security agency whose mission is to “neutralize destabilization plans against the nation”. Among other powers, the Center can declare any information as classified, including Internet content. This demonstrates a clear desire to continue limiting the free flow of information on the web.

Toward freer lands on the Internet

Maria del Pilar Sáenz³¹

Internet Service Providers in Latin America are increasing data plans that include free access to certain popular applications or not involving consumption of data plan. The “zero rating” arrived in the region and not all are happy.

Zero rating is a practice widely criticized for entering into conflict with the net neutrality principle, which is part of the guarantees to maintain free and open Internet. Overall, the offers are intended to increase the number of Internet users with promotions that appeal to a very specific market segment: one that does not have much experience with technology and therefore, knows only the most popular services and uses them to interact in “social media” at the lowest possible cost.

In practice, when access to the Internet on equal terms to all is not guaranteed, problems begin to appear as the creation of “walled gardens” or virtual spaces where companies have control over applications or content available and the ability to restrict them. The “walled gardens” make it impossible for users to access all available information, creating a bias in their ability to make decisions.

³¹ Maria del Pilar Sáenz works at the Fundacion Karisma and is part of the collective RedPaTodos and Hackbo.

Competition problems also arise. If someone makes decisions about which programs, applications and/or resources are available, many other fall outside, including direct competitors and new proposals that have no way to reach potential users.

A third problem is the cultural involvement. In the past 30 years, a number of cultures around the net have emerged, which have fought to keep it free and open. An example is the hacker culture that is based on the principles of the hacker ethic: a set of values, which include the free access to knowledge and accessibility. The work of these communities is at the core of the Internet and all large companies who thrive in this ecosystem. Without free Internet access, this cycle runs the risk of being torn to pieces and, instead of curious and active individuals able to innovate, we will see more and more passive consumers that do not distinguish between Facebook and the Internet.

One of the first countries for which we have information on the impact of zero rating is Paraguay, where Tigo, in partnership with Facebook, offers a free Facebook plan since a year ago. In February 2014, Mark Zuckerberg spoke about this cooperation at Mobile World Congress 2014 in Barcelona: “In Paraguay, we are working with Tigo, and they have also seen that the number of people using data plans grew by 50% during the time of the association”.

In 2015, the iconic case for the region is Colombia, where Facebook, in partnership with the government of president Juan Manuel Santos and, again, through an agreement with Tigo, established the first implementation in the region of the Internet.org program. According to the information on its website, Internet.org is a Facebook-driven initiative that “brings together technology leaders, nonprofit organizations and local communities to connect two thirds of the world’s population that lack access to Internet”.

In Colombia, Internet.org offers free access to 16 websites: 1doc3, 24 Symbols, AccuWeather, Agronet, BabyCenter & MAMA, Facebook, Girl Effect, Instituto Colombiano para la Evaluación de la Educación, Messenger, Mitula, Para la Vida, Su Dinero, Tambero.com, UNICEF, Wikipedia, and YoAprendo. The creator of Facebook attended the project launch. Although this program only provides access to few applications, the government’s press releases and mass media announced this initiative as one that seeks to provide access to Internet.

Weeks later, at Mobile World Congress 2015 in Barcelona, Zuckerberg stated: “50 percent of data users in Colombia have benefited from Internet.org”. There is no official figures that allow us to test this statement. If so, it would mean that half of data users in Colombia are not accessing the Internet, but to a limited and blurred version of the web through Internet.org.

We do not know which countries in the region will host Internet.org as part of state policy. However, in September 2014, Zuckerberg was negotiating with the government of Mexico, but an official announcement has not been made yet. However, in March this year, it was said that by 2015 two new countries in Latin America will launch Internet.org.

What does exist is a proliferation of schemes and offers that include free access to some services. In Peru, Claro is offering free WhatsApp. In Mexico, Telcel had a free WhatsApp promotion from August to December 2014 and is now Movistar who offers a plan that distinguish the access to social networks (Facebook, Twitter, WhatsApp) and mail from the Internet. In Paraguay, Tigo keeps promoting Facebook and WhatsApp for free. In Colombia, in addition to Internet.org, operators also offer WhatsApp for free.

As already stated, these plans, developments and implementations based on “zero rating” practices generate clashes with the net neutrality. Therefore, for advocates of these models, the development of regulations and policies around the web could represent an obstacle.

In the region, Chile is the only one who has spoken loud and clear on the subject. The Department of Telecommunications warned telecommunications companies, in their interpretation of the neutrality law, that those commercial offers that ensure the free use of specific social networking applications (or other) as WhatsApp, Facebook, Twitter, were highly discriminatory as they benefit a specific application to the detriment of their competitive nature. So, the only way the Chilean operators can offer “zero rating” plans is if the gratuity applies to all offerors of the same class of content. This would mean that if an operator in Chile wants to offer free WhatsApp, it also must offer Telegram, Line, Viper and any other application.

Other countries have not yet spoken. In Colombia, the net neutrality has defined supports market segmentation. In the interpretation taken by the controlling body – the Regulatory Commission of Communications –, operators can offer plans provided that they make available to their users an alternative or rate plan that does not require any limitation regarding

services, content or applications to which the user can access. An interpretation of net neutrality quite different from the one in Chile. As a result, in Colombia, we find free “WhatsApp” or “Internet.org” or economic tariff plans for “chat” or “social networks”, where the operator defined which services are included.

In Brazil, the regulation of Civil Marco of Internet is yet under discussion. It is expected that the issue of zero rating will become part of the debate on net neutrality.

While discussions and determinations of the countries take shape and international discussions on the subject are kept in the various related Internet forums, protests coming from the same Internet users are not left behind. We have heard some voices in the region that disagree with the zero rating.

In Colombia, Carolina Botero, from the Karisma Foundation, said: “Internet.org is not Internet”. In the Mexican case, the issue of market segmentation was seen with concern, when the net neutrality was discussed as part of the reform of the Telecom Act. There are doubts in Brazil about the appropriateness of such implementations. In this sense, they warn about the creation of “caste” on the Internet and what it means in terms of ruptures facing a process of digital inclusion.

In my point of view, one of the most curious reactions is the Paraguayan. In the absence of a legal framework that limits this, the response has been technological. A Paraguayan developer, exploiting vulnerability in Facebook’s chat application, has created a program that establishes a tunnel from Facebook allowing users to browse the entire Internet. In the words of the developer: “We all know that the Internet is about accessing many places, etc. So I feel this campaign [internet.org] as a serious limitation”. That is, in the spirit of those who created the web, the developer shows a practical solution to ensure that Internet.org does not restrict access to Internet.

Basically, we know that the goal of companies led by Facebook with Internet.org is not altruistic. Zuckerberg made it pretty clear this year in Barcelona when he said: “At the end, we want to make more money and connect more people in the process”. It may backfire them. And, following the Paraguayan path, connecting more people could allow those most in need getting out of the “walled garden” created by Internet.org and “zero rating” toward freer lands on the Internet.

Online censorship is latent in Chile

Paz Peña³²

The latest draft amendments to the Press Law in Chile (known as Digital Media Act) caused quite a bit of controversy over how it would affect the expression of Internet users. The problem is that in a country that has had its fair share of censorship issues on the net, the defense of our freedom of expression becomes an urgent necessity.

The latest controversy over freedom of expression online in Chile erupted with the discussion of the so-called “Digital Media Law” – two newsletters (9460-19 and 9461-19) that seek to reform the Press Law (19.733). On one hand, we had the creators defending it by appealing to the so called “spirit” of the law, which only intended to regulate traditional online media. On the other, there were organizations, which after the denunciation by Derechos Digitales, noted the potential dangers of a bill that was poorly written, with negative effects towards online freedom of expression.

The big problem with these projects is the vagueness of their concepts, which come along and worsen the already unclear definition of communication mediums in the current Press Law. The latter says:

“Communication mediums are those which are apt for transmitting, disseminating, broadcasting or propagating texts, sounds or images intended for the public, in a stable and regular manner, regardless of the medium or the instrument”.

The idea of the amendment is to define what an electronic communication medium actually is. According to its definition, it means that any publication, whether it is printed or digital, which is published at least four days each week and meets the other requirements of law, will be considered a newspaper.

But if the definition of newspaper, as we see in the press law, is applicable to virtually all websites on the Internet, including social networks, the new distinction of “publishing at least four days a week” does not really help to differentiate an electronic newspaper from other sites that store and distribute content online.

³² Advocacy director in Derechos Digitales.

Ignoring the vagueness of this modification is dangerous, because it leaves the door open for it to be used as an excuse for applying all the obligations of an electronic communications medium, which as NIC Chile once pointed out, are rather absurd, to any type of website. This implies fines and, indeed, the obligation of identifying the legal representative of the web, clearly putting the right of anonymity at risk.

Reporting these possible effects on freedom of expression in Chile is not a trivial matter. Often, the public ignores or forgets many cases of censorship on the web that have occurred in the country. Reminding ourselves about them helps us to understand a fundamental fact, that is, the political context in which the Digital Media Act is made possible: the existence of authorities and powerful figures who are willing to clamp down on any critical discourses against them.

Among the most emblematic cases, is that of ElMercurioMiente.cl, a satire website aimed at the traditional conservative newspaper El Mercurio, which lost its domain name after being sued by lawyers of the owner, Agustín Edwards. They argued their case on the grounds of there being an abuse of intellectual property rights. Unfortunately, this is not an isolated case in Chile.

Another case was “Free Rod”, where a Twitter user was confronted by the powerful businessman Andrónico Luksic, who personally went to the prosecutors to denounce the satirical Twitter account (@losluksic) as an alleged act of identity theft.

Neither can we forget the case of the current governor of Santiago and former presidential candidate, Claudio Orrego, who sued a satirical Twitter user for dubiously stealing his identity, which resulted in punishment for the accused user, in the form of 80 hours of volunteer work.

Bearing in mind these different situations, and looking beyond the future of the Digital Media Law, it is an obligation for both civil societies, as well as the democratically elected authorities, to shut down the possibility of there being any infringements on Internet freedom of expression.

Sometimes we forget that censorship is not something that only happens tens of thousands of miles away, as was the case of the bloggers law in Russia which, moreover, also sought to regulate digital media. Unfortunately, it is a sad fact which is a lot closer to home than we care to admit, in a country that prides itself of being one of the most stable nations in Latin America.

PART

3

REGULATION

Chilean bill on personal data protection is a setback for people and businesses

*Alberto Cerda*³³

The bill attempts to solve deficient protection for the right to privacy, to remove barriers for international transference of data and to harmonize domestic law with international standards. But the bill fails each of its purposes.

In 1999, Chile became the first Latin American country having a comprehensive law on personal data protection. Through time, the law proved inefficient at protecting people, facilitating international transference of data and adjusting to international standards. This led to new bills on the matter, like the one introduced in Congress in January 2011 by the Executive, after an opaque process of public consultation.

The bill remained frozen for two years because of criticism by experts and lawmakers, until last January, when the Executive achieved an agreement with the Congress. This agreement will allow advancing the bill through the legislative process, by limiting the effects of the law to just a few years, after which the Executive will evaluate achievements and allow Congress to discuss new legislative steps. In fact, however, this bill will delay adopting an actual solution and, meanwhile, it will diminish people's rights and put in jeopardy competitiveness of local businesses.

In spite of its negative effects, the bill gets some points right. For instance, the bill sets forth that the purpose of the law is protecting people's information that is being used by private and public entities in order to safeguard their right to privacy. The bill explicitly includes internationally recommended principles on the matter and improves the right to information and requirements of people's consent in order to allow personal data processing. Additionally, the bill resolves legal issues related to personal information about deceased persons and establishes responsibility of entities that process personal data by themselves and those that process data on behalf of someone else.

There are several issues in the bill that raise concern, however, because of its ambiguity, which may diminish people's rights and create legal uncertainty. For example, the concept of "personal data" differs from both international instruments on the matter and foreign laws, which prevents

³³ Alberto Cerda Silva is director of International Affairs for the NGO Derechos Digitales.

international harmonization of Chilean law, erodes protection to people and risks increasing barriers for international transferences of personal data to Chile. The same problem happens with an ambiguous concept of “public accessible source”, that allows processing personal data without knowledge or consent by people.

The bill assures compensation in favor of people affected by illegal processing of their personal data, but requires them to prove illegality, which is beyond actual capabilities for most people and ignores information asymmetries between companies that process personal data and data subjects. This makes compensation of damages almost impossible. It would be better setting forth strict liability on companies or, at the very least, reversing the burden of proof by requiring entities that process personal data to prove they act diligently.

The bill adopts a system of “Do Not Call” lists that allow people to inform they don’t want to receive information through their phone, email or other means. But there is not empirical evidence that this kind of system works and, on the contrary, it has been a failure in countries it has been implemented. There is no reason to believe this system will work properly in Chile.

The two main problems with the bill, however, are, on one side, that it will aggravate barriers for international transference of data into Chile and, on the other side, that it lacks actual enforcement regarding to the private sector.

A serious inconvenience for Chilean companies providing online services is they cannot do so with the European Union, which demands clear rules on how and where to export personal data. Other countries within the region have adopted that kind of rules, such as Argentina (2000), Uruguay (2008), Mexico and Colombia (2010), Peru and Costa Rica (2011). Meanwhile, Brazil has a similar bill under discussion in its Congress. In other terms, if Chile does not adopt a legal framework that provides an adequate level of protection, local companies will face more obstacles for doing businesses not only with Europe but also with other economies in Latin America.

The bill tries to solve the problem of international flow of data through an expensive and complex contractual mechanism. Other countries have tried that solution, with limited and questionable outcomes. To make things even worse, the bill creates unnecessary costs for local innovation and business. Achieving adequacy requires a proper institutional enforcement, but, unfortunately, the bill lacks it. Adequacy supposes recognizing rights of data subjects, imposing obligations on those who process data, and the

existence of mechanism of enforcement. The latter is the most deficient point in the bill.

The bill proposes an inadequate system for supervising the private sector. According to the bill, enforcement against private entities that process personal data would take three forms. First, through civil actions, a mechanism that is insufficient and does not guarantee adequate enforcement. Second, through reclamations before the local consumer protection agency, a toothless institution that does not have power to supervise, neither to sanction nor to prosecute infringers. And, third, through mechanisms of self-regulation and certification that have failed in the United States and in Mexico. They also failed in Chile, where both the National Chamber of Commerce and the Chamber of Commerce of Santiago attempted for over eight years similar mechanisms among their members, with poor results.

Most countries have adopted an independent, public enforcement authority, which has broad powers for supervising, sanctioning and prosecuting infringement. Unfortunately, all those powers are absent in the bill or they are absolutely diminished. As a result, the bill will neither improve protection of people for processing of their data, nor remove obstacles for free flow of information in order to encourage investment and to promote providing services of personal data processing from Chile to the world.

Far from 1999, having the experience of other countries on data protection and with several bills under legislative discussion for improving our legal framework, today we face a bill that does not make any progress on the matter, but, on the contrary, presents a serious setback that will diminish people's rights and put in jeopardy the competitiveness of local businesses.

Peru's controversial law on cybercrime

Eduardo Alcocer Povis³⁴

Why has this initiative, informally known as the “Beingolea law”, raised many critical voices in Peru? In a brief analysis, Professor Eduardo Alcocer dissects the law (which is now in possession of the Executive after being approved by Congress) and shows how some of its provisions are not only misguided, but can also affect fundamental rights such as freedom of expression.

³⁴ Eduardo Alcocer is a professor of Criminal Law at the Pontifical Catholic University of Peru. He is also lawyer and member of Estudio Oré Guardia.

On September 12th 2013, the full Congress of the Republic approved the bill on cybercrime, the same one that is currently in the office of the president of the Republic, as it may end up being promulgated*. The text that has been approved by Congress has been the subject of a lot of questioning, not only because of the surreptitiousness of the procedure carried out for its approval (which included other proposed bills that were not previously discussed in the congressional justice committee nor put to the attention of the legal community), but also due to its clear violations of criminal law principles.

Indeed, one of the core principles of criminal law is its minimal level of intervention, in the sense that the application of punitive power can only be legitimate if the regulated conduct is “harmful” or exposes legal goods, of particular social relevance, to some form of “concrete danger”. Contrary to this, the project plans to incorporate in our Penal Code the crime of “illegal access” (art. 2), which aims to punish those who enter computer systems by breaching security measures that are put in place to prevent such actions. In other words, it seeks to sanction “white hackers”, i.e., those who access systems without the intention of obtaining secret information, violating the privacy of others or causing any form of damage. This is very different to what is currently provided for in section 207 – A of the Penal Code, which requires for its configuration a “special intent” to obtain information or alter databases, for example.

If we consider the security of information contained in systems as a legal good to be protected, then the conduct displayed by the agent, who is intended to be punished through this bill, will be harmful. However, not all detrimental acts towards legal goods deserve to be sanctioned by penal law, as this effect has to be especially relevant to society, taking into consideration the actual interests being protected and the degree of danger of the agent. In the case of political “intrusiveness”, in criminal terms the security of information is protected because what is at stake is the legitimate interest of protecting the privacy and property of the people. However, in face of these legal goods, the project does not even contemplate the exposure to concrete danger and, subjectively, the intentions of the author or perpetrator are not deemed relevant. Therefore, I believe that criminal law should not punish these conducts, devoid of any real offense.

In relation to the principle of proportionality, the proposed sanction is questionable, as it foresees four years of imprisonment as the maximum penalty, punishment which is greater than that given for detrimental action

towards property (petty theft has a maximum custodial sentence of three years) or offenses against dignity and honor (imprisonment in cases of defamation is for a maximum of one year in simple cases and three years in more extreme ones – for example, defamation through the press).

Another approved proposal is to incorporate a new type of offense: sexual propositions towards under-aged people via technological means (art. 5). It intends to criminally punish those who “contact” minors in order to “request or obtain pornographic material” or “perform sexual activities with them”. It is reprehensible that in order to describe the main verb of the offense, the ambiguous term “contact” is used. When does a person actually make “contact” with someone? By simply greeting somebody by writing an email? By adding a person as a “friend” on Facebook? These acts should not be typical ones. I believe that the existing criminal offenses for child pornography, seduction or rape of children are already sufficient for punishing such harmful behaviors (e.g., when contact is already made with a minor to obtain pornographic material or for having intercourse), which are understood as attempted crimes.

Furthermore, there is the intention of punishing the offense of “discrimination on the Internet” (art. 323 CP), comparing it (in terms of punishment, from two to four years of imprisonment) to acts of discrimination such as those made through physical violence or threats. From the level of proportionality, it seems inadequate. On the other hand, it affects the principle of legality because the offense is arguably broad, as it is included as a manifestation of discrimination – on Internet – conducted for “political” reasons. Therefore, there is the danger of punishing political comments posted on social networks, for the mere fact that a person may consider themselves “aggrieved”. This puts at risk the legitimate exercise of freedom of expression. If the law is enacted, the prosecutor and the judge must perform a correct delineation of facts for criminal law to distinguish those that are relevant.

Likewise, a modification of art. CP 162 is being proposed, by which the punishment of acts of wiretapping will be included as an aggravating circumstance if the information obtained is classified as secret or confidential. It also aims to increase the penalty (eight to ten years of imprisonment) if the information obtained via interception compromises defense, security and national sovereignty. The legislator, arguably, did not take into account that our law already punishes anyone who gets hold of and or disseminates information which has been “kept secret in the interest of national defense” with a penalty of up to 15 years of imprisonment (art. 331 CP).

On the other hand, the fact that obtaining information (e.g., classified as secret or confidential) for motives of “public interest” has not been indicated as being exempt of liability is not, in my point of view, an obvious limitation of freedom of information. First, because it expressly prohibits dissemination and, secondly, because the legitimate exercise of a right (art. 20 inc. 8 CP) justifies the conduct of every citizen, as it is irrelevant – when declaring innocence – for each offense to expressly state that the agent must act “rightly” or in “public interest”.

It is true that criminal law must adapt to “modern times”, however this process should be performed according to its very own underlying principles and with respect for fundamental rights. Therefore, I believe that the bill should be observed by the president.

* Surprisingly, despite of the strong opposition from civil society and an important part of the industry, the president of Peru, Ollanta Humala, approved today, October 22nd, the Cybercrime Act.

The use of drones in Chile and DAN 151: innovation regulations are necessary, but insufficient

Valentina Hernández³⁵

The use of drones is becoming more widespread. They are available to those who can buy them and are becoming a common sight at football matches, concerts and other events and mass gatherings of people. Depending on how they are used, these devices may violate some of our rights, regarding our lives, property and privacy. In Chile their use has just been regulated, but are these norms enough?

The International Civil Aviation Organization (OACI) recently estimated that by 2018 there could be an international law regulating the use of drones or unmanned aircraft. As this kind of technology is on the rise and poses a number of risks, The Directorate General of Civil Aviation of Chile (DGAC) wisely decided that it was necessary to draw up its own rules as soon as possible. Thus, on April 2nd, 2015, the first law was presented, the aeronautics regulation (DAN) 151.

³⁵ Valentina Hernández holds a law degree from the Faculty of Law at University of Chile. She is a researcher for the NGO Derechos Digitales.

As we said before, the use of remotely piloted aircraft could lead to serious damage of the fundamental rights of the population, especially those related to life, property and privacy. For the authorities, the most palpable threat is more linked to physical integrity and properties: some of these crafts can weigh several kilos and fly at high altitudes, so if they fall or crash, they could easily cause serious damage or even death.

However, there is another big risk. Since these devices can take pictures and videos of our more intimate spaces from the air, it is not hard to picture how their use could easily become invasive, especially with the difficulties of pursuing any legal responsibilities.

Regarding the protection of our rights to life, physical integrity and property, we have a series of measures within DAN 151 that are intended for our protection, such as the flexibility of the propellers, the existence of an emergency parachute, compulsory insurance payments and an affidavit of responsibility, among other things. Similarly, a list of restrictions listed for using a “drone”, including the general prohibition of putting people’s lives at risk.

Furthermore, other requirements are considered, such as needing special permission to handle heavy drones, the registration of the craft, being certified after receiving theoretical and practical instruction, and having to pass an exam.

In contrast, the regulation regarding the right to privacy is very meager. We were only able to find a general prohibition, stipulating “to not violate the rights of people in their intimacy and privacy”, without establishing any specific measures.

Excluding the most obvious cases of transgression (photos and videos), carried out by individuals, there are much more complex aspects to take into account, such as state surveillance through the use of drones.

For the last two years, the Chilean government has been buying drones for law enforcement and surveillance, without being transparent to the public or about the acquisition and use of these devices. This aspect of the problem is not addressed in DAN 151, despite its importance.

Drones can be used to record small details that, viewed without context, might seem irrelevant; for example a photo of a person walking down a street. But analyzing photograph details such as the time, the street, the direction in which the person walked and adding data from other similar

images, make it possible to predict possible behaviors and habits to discover more about our general behavior. This type of threat must also be dealt with by a new legislation regulating the use of technologies that can be used for invasive purposes.

With just a small squad of drones, you can monitor entire regions. The technical specifications available on the more advanced models include several types of cameras along with laser, thermal and ultrasound sensors, plus other technologies which could gather as much information. This would not only make the right to privacy illusory, but other matters as well, such as the right to due process. The potential threat to the rights of life, privacy and property, posed by the government use of drones is much higher than that of the private sector. The picture is even far more complex if we consider that for the moment we have no way of identifying the state use of drones.

The use of drones is not a particularly bad thing in itself. Like with any form of technology, they can have a number of legitimate uses and there are those who perform legal economic activities through the use of these crafts. But given their potential risk, there is definitely a need for minimum conditions, governing their use.

The problem exists when the use of technologies infringe the fundamental rights and freedoms of individuals. That is why we expect a definitive law that can guarantee and protect them.

Personal data: awaiting a text

*Paulo Rená da Silva Santarém*³⁶

Very few people remember this, but in 2010 Brazil began the process of creating a specific law for the protection of personal data. Part of this lack of awareness can be attributed to the federal government itself, which for a long time stalled the initiative to create a new legal text, but it can also be due to the fact that our culture is permissive of the evasion of personal information. But the maturing of the Marco Civil da Internet (Civil Rights Framework for Internet Use) into a law opens the door for privacy to occupy a central role in the country's digital politics agenda.

³⁶ Paulo Rená da Silva Santarém has a master's degree in Law, State and Constitution, from University of Brasília. He is also professor at the Faculty of Law at UniCEUB (Centro Universitário de Brasília).

Between November 2010 and April 2011, a partnership between the Ministry of Justice and the Fundação Getúlio Vargas in Rio de Janeiro generated a public debate on privacy and the protection of personal data. In five months, 14 thousand visits and 795 comments were received. However, all of this discussion was not enough to guarantee the presentation of a draft of a law by the Executive Branch.

The federal government only readdressed the issue in 2013, when Edward Snowden reported the mass surveillance on the Internet by the American National Security Agency in association with similar agencies from four other countries (Australia, Canada, New Zealand, and the United Kingdom). In spite of this, this new approach merely proposed changes to be made to the Marco Civil text, as this was being analysed by parliament since August 2011. Even the proposed alterations – such as the initial demand of data centres in the country and the enforced obligation of retention of data and access to the protection of privacy – were not proven to be exactly adequate for the protection of privacy.

Certainly the Brazilian government's disinterest in continuing this discussion is related to the lack of public sensitivity to the issue of preserving personal data. It's surprising to consider the vast amount of information, which is supplied in order to access any service, public or private, or even to acquire products. From the Natural Persons Register number (CPF) presented by shoppers in for tax exemptions, to giving your personal address to participate in a promotional television campaign, in Brazil personal information is easily obtained by any company.

This context generates a series of risks, exacerbated by the growing demand for the supply of an ever-greater amount of data. From a public security perspective, retention as a rule and the State's access to data are deemed necessary to enable criminal investigations, specifically in the digital field; in the market's logic, consumer profiles are real assets which can easily be converted into money by way of directed marketing; in the logic of the entertainment world, *big data* allows consumers the comfort of a more personalized experience. This leaves little room to consider the issue of the right to a private life.

Without a public political debate, open to participation and subject to broad social scrutiny, currently the decisions concerning the protection of privacy are made according to private interests. This is very problematic,

as oftentimes the market's priorities do not align themselves with the protection of rights. The government itself, unless legal limits to its activity are established, can play the role of a tyrant when it comes to the treatment of personal information of its internal and external adversaries.

It's always important to emphasize that we are not just discussing the Internet. Firstly, we must also consider credit cards, cell phones, MP3 players, movement-controlled video games and even cars and smart-TVs: any personal device which contains digital information. Secondly, surveillance cameras, electronic turnstiles, biometric identification and records tied to the Natural Persons Register. There is a growing number of means of building a complete map of anyone's life.

Privacy, in broader terms, can be seen as the right to determine, for oneself, the line that separates the public from the private part of our lives. This is a free and individual choice, in accordance with one's personal convictions and way of seeing the world. A guarantee that each person can have a private life, in terms of what each person wants. Furthermore: without any tax on this choice and with the assurance that it will not be disrespected.

But of course real life does not follow the logic of the law. Individually, only a few violations of privacy are worth the effort, time and money required to seek a judicial solution and restitution. In the public sector, the existing international web surveillance is a good example of a very strong political component. However, in a complex society, which involves politics, economics, religion, science, entertainment and even convenience, the time will come in which the need to determine limits of right and wrong, in terms of what's legal and illegal, will become necessary.

The creation process of the Marco Civil and its maturing broadened the concept of what is necessary to assure peoples' privacy, within the Internet and outside of it. This context has proven to be ideal for the federal government to resume the debate on privacy, ultimately seeking to achieve an objective implementation of an express command from the Federal Constitution, which in turn reflects existing North-American and international rules. Even though it's late for the debate, Brazil can still arguably assume a protagonist role in this. Or at least reach the level of its Latin-American neighbours, who already have a set of rules assuring the minimum provision of personal data.

Civil Rights framework for Internet use: Brazil at the peak of Internet regulation as warrantor of rights

Marina Pita³⁷

The last two years will be remembered in the history of the internet as those when disputes over its future surfaced. This comes as no surprise, since these are the years that preceded the maturity of the World Wide Web: in 2014 we celebrate its 25th anniversary.

Although the internet was born and grew faster in North America, it seems that South American countries are the most enthusiastic to defend principles to keep it at the same path during its adulthood". Brazil, in particular, continues at a prominent position with the approval in April of the Law 12.965 – the Civil Rights Framework for Internet Use.

The World Conference on International Telecommunications (WCIT), in December 2012, raised the controversy over who should regulate the network. And, at that time, the director of the UN agency pointed out the lack of balance between the investment made by companies operating mostly in the infrastructure layer, Internet Service Providers (ISPs) and companies that profit from it, the so-called over-the-top companies. As a word to the wise, it was clear that there was an opening to think of a model in which large online Internet platforms and content producers had to pay for network users to reach them. This decision would severely affect the potential of the Internet to make knowledge, freedom of expression and innovation more democratic.

From that point forward, the debate on the need to maintain the principle of network neutrality increased rapidly and, in Brazil, it was combined to the effort that many civil society organizations and hacktivists have been already making to prevent the creation of internet laws from a perspective of criminalization of illegal acts and violations.

Also in 2007, in opposition to the Cybercrimes Bill (84/99), which established network vigilantism, the idea of promoting a legislation to regulate the Internet in Brazil that derived from the guarantee of rights emerged as a concept. Such determination found solid foundation to yield

³⁷ Reporter specialized in corporate coverage, market, economic policy and regulation of telecommunications, information technology and electronic devices.

good results when, in 2009, the Brazilian Internet Steering Committee (CGI.br) – tripartite organization with members representing civil society, business, and government – approved a resolution with the ten principles for Internet governance and use in Brazil.

They are freedom, privacy and rights; democratic and collaborative governance; universality; diversity; innovation; network neutrality; unaccountability of the network; functionality, security and stability; standardization and interoperability, and legal and regulatory environment.

Under the responsibility of the Ministry of Justice, the draft bill has received more than two thousand contributions from all sectors of society, with the broad participation of entities in defense of online rights and hacktivists, already mobilized to prevent the passage of the bill criminalizing online activities and electronic vigilantism. From 2011, when the first version of the bill came to the Chamber of Deputies, the Civil Rights Framework for Internet Use underwent a new round of consultations. The text was improved through public hearings that heard more than 60 representatives from various sectors, in four of the five regions of the country. The text also went through an online consultation and, for the first time in the history of the Brazilian Chamber of Deputies, a bill received contributions through Twitter. The rapporteur of the bill, Alessandro Molon (PT/RJ), accepted one of them, which was incorporated into the final text. That is, the Civil Rights Framework for Internet Use innovated not only in its set of topics, but showed new possibilities for the Brazilian legislative process and wider popular participation with the Internet as a medium.

Upon reaching the Chamber of Deputies, however, the text faced stiff resistance in the Brazilian Congress. The theme was technically too complicated for legislators with little technical knowledge about network operation. Besides, the telecom giants launched a strong lobby to prevent its approval using biased arguments. For giants Telefônica, América Móvil and Telemóvil, each with its subsidiary in Brazil, the Civil Rights Framework for Internet Use would prevent them from creating new business models based on the ability to collect data from users, manage the network to create plans for services and charge content companies and online platforms for the differentiated traffic.

For the civil society around the world facing this strong lobby within its borders, it must be noted that in Brazil, for the first time, the monopoly in broadcasting – so difficult to local political developments – weighed in favor of the interests of civil society. Feeling threatened by the telecoms

advancements in content distribution and afraid of having to start paying for internet users to access its portals, the family business Rede Globo de Televisão, which concentrates 70% of TV advertising in the country, placed its political weight and editorial line in favor of the Civil Rights Framework for Internet Use.

It was then, amid pressure from both sides, that the first reports were published in *The Washington Post* and *The Guardian* about state surveillance in the United Nations and that would be backed up by big internet corporations. This fact was essential for the tug of war that was established around the Civil Rights Framework for Internet Use to start tilting to the side of civil society organizations. The issue of personal data privacy, often neglected in Brazil – the country of friendly people – came to light. Obviously, at this point, much of the Brazilian government was already convinced of the importance of net neutrality, the guarantee of freedom of expression and access to information, the tripod concerning the importance of guarantees for the right to privacy was completed.

The text of the Civil Rights Framework for Internet Use is extremely important to enforce neutrality as a principle. Network neutrality ensures that the Internet will remain open so that dissenting voices may express themselves at the cost of the connection and gain relevance from the interest of netizens and not by their economic power. The production of independent online content is gaining ground in Brazil to address the broadcasting oligopoly and media concentration in the hands of conservative families. For the June demonstrations against the rising prices of bus tariffs, online videos were essential to oppose the position of the military police, which arrested several activists and acted with violence against peaceful protesters.

The Civil Rights Framework for Internet Use also ensures that requests for removal of content from the net should only be imposed when there is a court order. This regulation creates a secure legal environment so that content platforms are not coerced into removing material from the net under threats. Brazilian civil society understands that this fact is of great importance because without the mediation of justice, the definition of content withdrawal weighs on economic and political power capacity, with great prejudice to freedom of expression and diversity and plurality of ideas. This regulation has proved to be relevant in the case of the 2014 elections. Some politicians have invested heavily against information disclosure, satires and online critiques, but now they need to pass the

scrutiny of Justice. At this point; however, it must be noted that civil society failed to reverse the exception to the notice and take down in the case of copyright content.

In the case of privacy, the text states that private communication is inviolable and operators of telecommunications networks are not allowed to monitor the content accessed by their clients, since they cannot change service provider the same way they change browser or application. In the case of online applications, access and copying of personal data requires express consent from the user, after he has been clearly and comprehensively informed about the collection of such data, and should be deleted if the user terminates his contract with the company.

For Brazil and the entities that strive to guarantee the right to freedom of expression, access to information and privacy, the Civil Rights Framework for Internet Use is a victory that has not been seen in a very long time in the field of communications. However, the law only establishes the rules for the game; now it is up to each of the players to play it so that the regulations provided are actually being implemented.

Digital regulation challenges for the new government of Chile

*Francisco Vera*³⁸

In March of this year a new government will take office in Chile. Any digital development policy that it implements must necessarily consider legal variables, by designing regulations that enable sustainable development, beyond buzzwords such as “digital government”, “smart cities”, entrepreneurship, innovation or disruption.

Digital development in a country is not separate from the regulation that supports it. It is not limited to climbing a few positions in the access to technology or e-government charts, but refers more to a holistic approach, where digital technologies are a tool to enable people to maximize their welfare and respect for their rights.

The mere assertion from some sectors that their interests are what best interpret the country (oh, what a coincidence!), cannot be accepted without first making

³⁸ Francisco Vera is Derechos Digitales' public policy director.

a critical reflection on their implications for the development of our rights. Thus, the new government will have to make several regulation decisions on digital issues that will directly affect public interest in various areas.

Privacy and personal data

Chile has a personal data law which from the beginning has been labeled as “tailor made for big companies”. In practice, this means that our personal data is currently in “no man’s land”, due to a weak set of rights and paltry enforcement mechanisms, forcing those who are affected to go to court to gain any effective sanctions for abuses in this area.

Today a reform to this law is being discussed, but so far the project does not include the creation of an agency for the protection of personal data, which would give citizens effective tools to protect themselves from the constant abuses that exist today. However, numerous groups with corporate interests seek to maintain the status quo, on the grounds that they defend the free flow of information and knowledge, and are against all obstacles that a more effective system would create for digital entrepreneurship, along with other justifications that seek to maintain and uphold the current system of abuse.

Copyright and intellectual property

After the reform of 2010, there are still many challenges to be solved. The first and most serious being the Trans-Pacific Partnership negotiations, which would force the country to succumb to the greed of the entertainment industry, which for the protection of its business models, wishes to gain control of the entire content of the network.

On the other hand, there are many problems to be solved in relation to the copyright regulation: the ability to use and reuse public information, especially when obtained via transparency, revising the cumbersome system of registration and transfer of copyright which is in force today, along with creating a system that allows works to be used when the owner of the copyright cannot be found (also known as orphan works), among other things.

In particular, while anticipating the education reforms that the new government intends to implement, it makes sense to directly propose the adoption of a new IP policy regarding textbooks and educational materials, by pointing towards open resources and employing content licenses that allow free use (and reuse) of publicly funded content.

Internet governance

On international issues, Chile noticeably lacks participation in key discussions on digital rights, which today can mostly be found in multiple forums such as the ICANN, which governs domain names internationally, the IGF (Internet Governance Forum) and similar spaces, whose distinctive features are the participation of multistakeholder or stakeholders, which nowadays is a key for adopting sustainable, informed and effective public policies in this area.

Chile can no longer afford to miss out on participating or only attending the ICANN meetings when the implementation of a new domain name, with the extension “.patagonia”, was being discussed. The country has the mission of developing an integral strategy in this area, seeing it as a problem that transcends the technical and encompasses the political by clearly defining, with the participation of all national stakeholders, what role Chile should play in these forums.

As soon as the new Chilean government takes office it will face many challenges, such as deciding whether it attends the summit of Internet regulation that Brazil is holding in April this year or defining national participation in forums such as the ICANN and the IGF, taking into account that Internet regulation is becoming an increasingly strategic issue for countries, especially in light of the NSA surveillance scandals.

Other relevant aspects

Another issue that is likely to form part of the public agenda this year is the discussion on reforms to the cybercrime legislation which is currently in progress, which should ensure a reasonable balance between the prosecution of these crimes and respect for Human Rights such as privacy and freedom of expression.

In e-government, there have been ongoing discussions on how to implement a software licensing system to prevent reliance on certain suppliers and maximize positive externalities in technology investments, allowing other state (and non-state) bodies to benefit from these advances. The answer to this has always existed, in the form of adopting free software licenses, but it is time to implement this in a more serious and consistent manner.

Finally, to systematize all these efforts, it is necessary to work on a digital rights strategy that transcends public relations and rigorously evaluates the results of previous strategies, seriously considering the interests of the private sector and civil society, in order to create a roadmap that allows us to face the digital future in a joint and sustainable manner.

Human Rights as a bargaining chip: the case of #LeyTelecom

*Francisco Vera*³⁹

The recent approval of a new Telecommunications Law in Mexico uncovers an outrageous reality where the political process behind the transactions have converted Human Rights into a bargaining chip.

After an exhausting and prolonged battle by Human Rights activists from Mexican civil society, the draft of the Telecommunications Law of that country was finally passed and published in the Official Gazette and is ready to come into force.

The concerns regarding this law are amply justified. While one of its initial hazards, related to rules affecting the principle of net neutrality, could have been solved, the other provisions which seriously impact the Human Rights of those living in Mexico have remained unchanged. We are specifically referring to those that are upheld in the name of public safety, such as the disproportionate capacity to control areas and populations, giving a “competent authority” the power to order the suspension of telephone services arbitrarily, in order to “prevent crimes from being committed”. This measure is completely unjustified and contrary to the right of freedom of expression, information and communication.

In fact, after the law was passed, the Human Rights Commission of the Federal District (CDHDF) stated that this was not only a law concern, it was also worrying for providing real-time geolocations and the broad and disproportionate obligation for the telecommunication companies to retain the data of their users.

However, beyond the specific problem areas of the Telecommunications Law, there is a bitter feeling about the political processes underlying these decisions. First, because of the low participation and transparency of the project and, second, its general tone and the concepts of public interest and Human Rights that appear within it.

A major reason for this sentiment stems from the disastrous idea that Human Rights are somehow negotiable in the name of market efficiency,

³⁹ Francisco Vera is Derechos Digitales' public policy director.

social inclusion, digital penetration or, like in this case, an overloaded notion of public safety, which does not even provide real security for citizens. Under this approach, if a bill sacrifices some rights, it will not be a problem as Human Rights defenders will appear, along with other relevant actors, and provide all the relevant dots and wording to make it a “settled issue”.

However, deciding on respect for Human Rights, whether it be on the Internet or on another platform or place, does not equate to defining a simple public policy nor a subsidy for a particular industry, neither does it compete in importance with innovation or the market. Respect for Human Rights is an essential part of a democratic system and the rule of law; they guarantee all of our minimum rights as human beings, and they serve as the foundation for us to grow and develop in a society where we can enjoy other rights.

In fact, in most Western constitutions respect for these rights is not only recognized as a right, but also as a limitation on state power and that of other private actors, it is considered an essential duty, not a power for negotiating or making deals. It also applies in the case of the Mexican Constitution, which clearly and unequivocally defines this point in its first article:

Article 1, first paragraph: In the United States of Mexico all persons shall enjoy the rights recognized by the Constitution and the international treaties which the Mexican State has subscribed to, including guarantees for their protection, whose exercise may not be restricted or suspended, except in the cases and conditions that are established by this Constitution.

However, after reading the new Telecommunications Law and observing other behaviors of the Mexican government (like the censorship of the Tdmx website), it is clear to see that its focus is not on these matters. In the recently passed law, it is easy to note that the language is designed from the powers of a governing body, from the obligation to cooperate with law enforcement or from the exceptions that make some rules become useless. In sum, from the need to limit Human Rights, when who should limit power is them. This is clear in the wording of Articles 189 and 190 of the new law, which merely refers to the needs of the government, without any reference to the Human Rights that are being affected.

It is true that politics is based on negotiating and discussing various positions that can lead to results that leave everyone satisfied. But when the mechanisms and the language for designing public policy stem from the needs of a government or certain private actors, instead of focusing on Human Rights and public interest, the base of these deliberations and/or trading processes are biased and poorly designed.

Unfortunately, in this scenario, the role of civil society will be one of putting out fires and fixing bugs, rather than allowing our rights to flourish and develop in society.

“Digital Argentina”: regulation and future?

*Santiago Marino*⁴⁰

In Argentina, the year 2014 ended with a highly relevant news for policies, for regulation as well as for convergent and communications market. The National Congress passed the Digital Argentina bill in extraordinary sessions

The executive branch’s initiative was sent to the Congress unexpectedly, without previous debate and with the possibility to generate impacts on economic, regulatory and sociocultural terms within the extended audiovisual space (that is, the set of supports and windows which, as a result of a series of technological advances, generate different spaces, business models and types of links between supply and demand of contents and audiovisual media means).

The convergence between telecommunications and the audiovisual space has a long technical record and has been installed in social usage. Its exclusion from the Law 26522 on Audiovisual Communication Services – LSCA (passed in Argentina on October 2009 after a long debate and a wide participation of citizens) – meant missing an important opportunity to manage the process, to establish competitive conditions for a dynamic market and to limit the levels of property concentration, which has negative effects (economic and symbolic) only for citizens, users, consumers.

⁴⁰ Phd in Social Sciences, director of the Master in Cultural Industries (National University of Quilmes-UNQ), professor on Policies and Planification of Communication at the Faculty of Social Sciences at Buenos Aires University (FSOC-UBA), undergraduate and graduate professor at the Universities of Quilmes, Buenos Aires and El Salvador (UNQ-UBA-USAL).

As regards specific content, the new law has positive aspects, such as: updating regulation for a very dynamic market and distinguishing between contents and continents. With regard to digital rights, the declaration of “net neutrality” is a mechanism which may result in an advanced international regulation, once it is clearly defined concerning its scope and aspect. On the other hand, the declaration of infrastructure as “public service” and the last mile or “local loop” unbundling of fixed telephone networks (telecommunications’ central support in Argentina) are relevant decisions. The challenge will be based on defining clearly the possibility of setting fees for the renting of such infrastructure on the part of the State and the way in which this possibility is carried out in the future. It is important to highlight that the law should be enforced by the future government, which raises another question on the matter.

Another central element is the possibility that telecommunication operators may provide for audiovisual services. Such companies are already part of the audiovisual system. Their economic capacity – taking into account the size of the concentrated market and of the wide scale market in which they provide services – may result in unequal competition for agents from the market of traditional media means. Accordingly, the role of the State with the ability to control cross-transactions and levels of competence will be vital to prevent large “telecommunication” operators from gobbling them up.

The debate in Congress enabled the creation of conditions to improve central issues that the bill had left outstanding. On one hand, regarding the enforcement authority, the dispositions of the LSCA (and as a result of the pressure imposed by a group of experts, researchers and organizations involved in the topic, which were invited to participate in the meetings of the Commission where the text of the draft was discussed) were finally followed and the creation of a representative and legitimate body was approved: the Federal Authority of Information Technologies and Communications (Autoridad Federal de Tecnologías de la Información y las Comunicaciones: AFTIC). Moreover, the Federal Council on Information Technologies and Communications (Consejo Federal de las Tecnologías de la Información y las Comunicaciones) will be created with action frameworks supposedly defined. On the other hand, the debate adjusted – without solving – certain aspects related to the issue of regulation of competence, leading and “significant market” position, which shall be defined clearer when regulating the law.

At the same time, another issue that was not clearly addressed was the one concerning the “Protection of users’ privacy”, since – as stated by the Association for Civil Rights, ADC, during debate – any communication supported by TIC shall be inviolable but may be intercepted (without clearly defining in detail what this implied) “upon the request of a competent judge”. These topics must be taken into account when regulating the law.

Argentina ended the year 2014 with news regarding the audiovisual space, its regulation and the market. This situation has been going on in this intense country for more than 6 years. The news were related to the LSCA and its biased enforcement for a large number of reasons, the tendering for 3G and 4G spaces for the expected improvements on mobile telephone networks and data transmission. The news were also related to the new law which raises, at least for now, more questions than certainties with regard to the future of convergence.

Draft Bill 215/2015, infanticide to the newly-born digital rights in Brazil

Bruno Ricardo Bioni⁴¹

Still fresh in the memory of all Brazilians as well as all the internet governance community, is the scene where president Dilma Rousseff signed the Law 12.965/2014 on April 23rd, 2014, at the stage of NetMundial. Most commonly known as Marco Civil/MCI (Civil Rights Framework), the law was a reactionary move against Internet-regulation proposals based on a criminal perspective and gained strength in 2007.

Instead of betting in a regulatory dynamic that would slow social participation in the net through punishment-based lenses grounded on criminal law, upholding users’ rights and guarantees as an incentive were the chosen path.

Beyond its normative content, the MCI was also singular due to its formulation process. Engaging with the society culminated in its famous collaborative process – the elaboration of an online platform, widely accessed and diffused throughout society. It took seven years between the articulation and elaboration of the MCI and its approval at the national congress; now with more than one year, this successful and internationally applauded experience of the Internet Bill of Rights faces a great threat.

⁴¹ Lawyer and researcher at the Public Politics Group for Information Access, University of São Paulo (Surveillance and Privacy Research Project).

An agenda revoking the important chapter on national democracy is now circulating within the Congress. Already approved in the Chamber of Deputies' Commission on Constitution, Justice and Citizenship, the Draft Bill 215/2015 meets/goes against with the history of the MCI and its regulatory pillars by proposing changes in some of its apparatuses.

First, the punitive discourse is reclaimed as a regulatory strategy. This legislative initiative supports a questionable criminal policy for crimes/offenses against honor and seeks to make it stricter by increasing punishments for such crimes (when practiced through/on the Internet). In practice, this punitive regulatory framework could collaterally damage freedom of expression, provoking hindering critical opinions that could attract those types of crimes against honor, whose penalties oscillations are an unstimulating additional factor for the free manifestation of this nature. International documents and recommendations point that illicit acts such as these should be transferred to civil affairs.

Second, the bill draft foresees a limited reading of the "right to be forgotten" - it is stretched/widened in comparison to the original conception of the term. With that being so, it does not provide the disindexation of contents, only its total escheat/unavailability, and most importantly, it disregards criteria for its well-balanced enforcement.

The right to be forgotten always involved a case-by-case examination regarding information so it would not suppress the right to information. Nonetheless, this legal initiative runs over this debate when it establishes a criteria for the assumed offense against honor. Therefore, it does not include other standards, such as the historical and public values of information as an exception to the right to be forgotten.

Due to such individualistic and simplistic rationality, a corrupt politician could claim that honor-offensive information against him/her should be "forgotten", inarguably influenced by his/her public interest. Protecting honor is, once more, overstretched in view of the lack of criteria capable of emulating the protection honor vis à vis the freedom of expression and access to information, what could ultimately determine the maintenance/availability of a certain content on the Internet.

Third, and last, the draft bill extends the definition of data required for registration foreseen in the MCI - what stands as an exception to the rule that prescribes a compulsory court order to access such data. Besides personal qualification, address and affiliation, such hypothesis overreaches phone numbers, national registration number and email, demanding that

all application Internet service providers collect such data. In practice, registration becomes a necessary condition for users to surf on the Internet. Such intrusion was, within other motives, the reason for this draft bill to be nicknamed “PL Espião” (Spy Draft Bill).

The most troubling part is that it does not consider the pending regulation of the MCI, through presidential decree, that will detail this regime of exception to access personal data without court order. Similarly to the process of elaboration, the regulation of MCI has been submitted to public consultations. Its contributions aimed – antagonistically to what was proposed by “PL Espião” – in bringing greater guarantees to users’ privacy, therefore defining the limits to additional measures for requiring and holding data. Most worrisome is noting that the MCI is only in its first year, pending a presidential decree to produce all of its regulatory impact.

Even so, the Brazilian legislative arm intends to modify this judicial architecture, proposing in contradiction to its regulatory pillars, such as the liberty of expression, access to information and privacy. The civic product of the Brazilian society that was cultivated for seven years and recently completed its first anniversary could have its history shortened. Civil society, academia and CGI (Comitê Gestor da Internet) have already mobilized themselves against this infanticide. Past, present and future of Internet regulation get mixed up, putting at risk the new-born digital right in Brazil.

The Internet in Mexico, two years after #ReformaTelecom

*Carlos Brito*⁴²

Mainly by convergence effects, but above all, by its nature as enabler of rights, the destiny of the Internet is key in any analysis of telecommunications reform (#ReformaTelecom) in Mexico, which included constitutional changes, as well as a regulatory law that will outline the guidelines of the regulator. Although there were those who dismissed them as “minor issues”, when discussion was intended to bring issues related to this matter, international trends have been dragging their associated problems closer to Mexicans, to a point where it is impossible to escape them.

⁴² Carlos Brito is advocacy director at R3D, Red en Defensa de los Derechos Digitales.

The first point to discuss is, of course, the access. While AMIPCI reports that 51% of the population is connected, there is also an uneven concentration across states and regions (in years 2013-2014, the growth rate was 13%, while in 2014-2015 was 5%). These gaps, according to the reform, should be fought through elements linked to the generation of more competition and through various policy instruments that would increase the basis of infrastructure, such as the shared network of 700 Mhz band and the extension of State backbone network for the exploitation of new and existing operators (which theoretically could increase the coverage).

Both projects are not only delayed by several months in compliance; the shared network has decreased in capacity adjustments and has made itself less attractive by other bids, while the backbone network project should have started in December 2014 and should be operating in 2018. In addition, there have also been indications that there are attempts to propose a counter-reform in order to finish them completely. Finally, concessions of social, community and indigenous type are not restricted for broadcasting, as, according to the constitutional reform, they can be extended to provide telecommunications services.

Successful civil society efforts, such as Rhizomatica in Talea de Castro and other locations in Oaxaca, are an example that could be replicated in different parts of the country, where operators have refused to provide Internet access and where the regulator have failed to uphold these rights: the population installing and operating networks on their own and in their own terms.

Although constitutional reform contemplated that telecommunications are understood as a public service of general interest and that, among others, are to be provided under competitive conditions and free access without arbitrary interference (Article 6), the Federal Government was openly opposed to the net neutrality, despite the narrative of the National Digital Strategy (which ambiguously is or not an Executive's spokesperson in public policy on the matter). This institutional schizophrenia showed especially when the Federal Government was accused in early 2013 of having censored the 1dmx.org site in collaboration with the US Embassy in Mexico to pressure the GoDaddy domain provider. The director of the EDN refused to comment, leaving that task to the Federal Police.

According to the former undersecretary of communications Ignacio Peralta, articles 145 and 146 of the law established a scenario in which ISPs could charge differently to application providers, content or services (APCS) on the Internet in order to make them "contributing" to investment

of infrastructure. This is the central argument of telcos against the net neutrality worldwide. Furthermore, Article 146 permitted a number of interpretations, which could pass different types of tiering including prioritization (fast lanes/slowlanes). Article 145 included obligations on ISPs for blocking APCS by arbitrary request of unspecified authorities and liability of intermediaries for discretionary censoring by imposing the obligation to interpret possible violations of the law: private censorship.

As a result of social pressure, articulated in demonstrations on the web and also on the streets, these provisions had to be discarded, resulting in two articles on net neutrality, which, in a comprehensive reading, provides an appropriate framework for an open and free Internet... This matter, however, still needs to be handled by the Federal Communications Institute. And at this last point, things do not look good.

Mexico has gained a certain streak in creating autonomous constitutional bodies (outside the scope of the executive, legislative and judicial branches) for key policy issues. Two particularly important themes are the regulator, the Federal Communications Institute (IFT, in Spanish) and the National Institute for Transparency, Access to Information and Personal Data Protection (INAI, in Spanish).

The latter approved earlier this year a resolution that introduced in Mexico a version of the “right to be forgotten”, even more harmful to freedom of expression and access to information than the one in Europe with the Costeja case. The resolution provides a simple and without any rights weighting formula: the name of a person is a personal data, therefore, at the request of the owner, Internet search engines should de-index sites required.

This resolution began directly affecting media that in their notes denounced alleged acts of corruption by Mexican politicians linked to the family of former president Vicente Fox. For now, both Google (the first affected search engine) and Fortune Magazine (through R3D) are challenging this resolution in a litigious process, hoping to push back this form of censorship. In its argument, Google claims that Mexican laws are not applicable to the search engine service, because its operation is based in the United States, while in R3D we defend a point of view that the company is itself bound to respect provision on data protection, while we fight back the implementation of this resolution by violating freedom of expression.

Eliminialia law office, headed by Dídac Sánchez (hopefully, he will not request to de-indexing this article from search engines) and the leading advocate of the so-called “right to be forgotten”, says that 80% of their

clients are politicians and former officials in a country that is known for high levels of corruption and collusion with the organized crime and civil servants. Legal threats do not always take the form of a direct request to Google, as some media outlets yield to pressure by removing the contents of their servers. This is perhaps one of the best examples of a larger problem showing the shortcomings of the Mexican regulatory system just months after the reform, which claims to revolve around convergence.

While the IFT is prepared for the process of issuing rules on net neutrality, operators have rushed to normalize different practices contrary to this principle. One is the deliberate degradation of APCS, a practice that is tangible but invisible to end users (there is no way of knowing if an operator reduces the quality of service as a deliberate practice or if it is an incidental event); in relation to Netflix, in its annual report on the quality of their service in different operators worldwide, the Mexican ISPs are ranked among the worst ones.

At the same time, all fixed and mobile operators have generated commercial package offers of free social networks, zero rating, in clear breaching the provisions on net neutrality of the Federal Telecommunications and Broadcasting Act, and taking advantage of the momentary vacuum of rules. However, it is so advanced and organized this violation to net neutrality that the IFT itself, in its operation comparison chart (a chart done to help users choose better), shows offers of zero rating as an advantage to be considered by consumers, even before issuing rules on the matter.

In addition, since September 2014, Enrique Peña Nieto began talks with Mark Zuckerberg to introduce Internet.org in Mexico, an even more aggressive form of zero rating. Although it has been delayed due to disagreements to operate under the Telcel network (Facebook is making a bet for its proximity to Carlos Slim) or Telefónica Movistar, the IFT simply remains passive, quiet, despite being a regulator particularly equipped with tools.

Besides the argument that “the OTTs must also pay for the infrastructure”, ISPs have begun to handle a discourse that positions the net neutrality as a selective principle to access policies. In that way, they make viable the business model of APCS discrimination, bypassing the innovation system on the Internet, freedom of expression and the users themselves. When Mexicans are struggling to break free from a pattern of TV and radio concentration, they could soon find a new, larger and more complex form on the Internet. If there were legislation with clear principles that prevented directly to the INAI imposing the “right to be forgotten”, would it abide it? The IFT experience leaves doubt.

Issues that seemed distant to Mexico a few years ago – liability of intermediaries, content blocking, legislation and regulation on net neutrality, “right to be forgotten” – are now part of the digital agenda in this country, added to the domestic discussion on Internet access policies. There is an agenda that has been aggravated in recent years for Internet reforms on the mass surveillance of communications, but this is a subject for another article.

The articulation of the civil society is essential to generate a counterbalance to the visions of government and industry that emphasizes Human Rights and democracy over the profit and political control. Many stories have been opened this year, demanding participation and involvement of all social sectors. Internet has meant a front of democratic opening when formal institutions of the Mexican State have gone back in their powers; more than ever, it is worth defending it, that is, we have to defend ourselves.

How we learned to stop worrying and love the ban

Miguel Morachimo⁴³

A group of bills recently introduced in the Peruvian Congress address various issues related to Internet use. However, its take on technologies and potential is biased and pessimistic resulting in formulas which propose banning all that cannot be controlled.

A bill introduced by Congressman Omar Chegade bases itself on the concern of how easy it is to get access to pornography through the Internet. It considers that it is becoming increasingly difficult for parents to monitor what their children are doing online, due to the current variety of mediums and devices that allow people to connect. He therefore proposes the creation of a state commission dedicated to identifying and ordering the blocking of all content deemed unsuitable for minors on the Internet. This filtering would be the default setting for all Internet connections in the country and would only be deactivated for users who demand it from their Internet providers.

The proposal suffers from profound legal and practical problems, as we have already pointed out at Hiperderecho, because, in principle, it would

⁴³ Miguel Morachimo is Hiperderecho NGO's director.

implement a state system of prior censorship on content that is actually legal, such as is the case with pornography. The project does not seek to regulate access to child pornography, but to pornography in general.

In addition, the requirement of explicitly having to ask your Internet provider to enable the pornographic content would create a national registry of pornography consumers which nobody would want to join.

If put into practice, the project would also be very difficult to implement and receive proper maintenance. The volume of sites that would be added daily, to a state black list, would lead to errors and grey areas, together with cases where the state authorities may use this for censorship of a political nature. The intensive use of this power would lead to the blocking of services such as Tumblr and Pinterest or of all other peer-to-peer traffic in Peru. Therefore, accepting these solutions would open the door in the near future for the implementation of similar filtering systems for infringements of copyright or defamation.

Furthermore, after a troubled first attempt to extend the range of existing computer crimes in Peru, a new bill signed by the Executive wants to incorporate a set of new offences related to computer systems. The proposal is partly based on the Budapest Convention on Cybercrime as it proposes to incorporate crimes such as illegal access, the violation of data integrity or computer systems and the misuse of devices, among others. However, in some cases it fails to mention some of the exceptions that appear within the international text articles, while in others it incorporates entirely new ones.

This applies in the cases of grooming offences, discrimination and wiretapping. In the first, as a clear example of our national tradition of following continental trends, penalization is proposed for those who “through information technology or communications” contact children under the age of fourteen to take part in any form of pornographic or sexual activities. For discrimination offences, they propose to extend the current wording of the Criminal Code to include cases in which the crime is committed “through information technologies and communication”. In other words, it proposes up to three years of imprisonment for anyone who, by means of an article, comment or video broadcast on the Internet, discriminates or encourages discrimination. Finally, the bill also seeks to increase penalties for the crime of wiretapping, raising it to six years, and proposes aggravating factors for classified information or that which compromises national defence and sovereignty.

Although both bills have been drafted by different teams and address different problems, it is possible to identify some commonalities. First and foremost, they share a bleak view on the meaning and uses of technology and the role of the state.

Society has embraced the development of technology as an opportunity to innovate and improve our quality of life, which obviously has its risks, but its benefits cannot be ignored. In stark contrast, within these projects, our state seems to see technology as a profound threat to society which must be suppressed, and from which we will never be sufficiently protected.

For the above reasons, these projects strive to cover all possible scenarios, which in practical terms will never be verified nor will we have the appropriate means to detect them. That's why they would much prefer for the assumptions to be as broad as possible, as opposed to being too specific. This "precautionary" approach towards the uses of technology can ultimately affect not only the users but also companies, creators and entrepreneurs who experiment with new mediums.

The other common trait to be found within both bills is their detachment from the nation's reality and the institutional capacity of the state. They always start with an international document, a foreign initiative which aims to be imitated or the need to take political advantage of certain situations.

Worse still, the rush to adapt the Budapest Convention is to prevent the approval of a bill that is worse than the one proposed by the Justice Committee last year, which still has not been withdrawn. However, nobody ever points out the number of criminals who have slipped away from the state because of a loophole, the success that these measures have had in other countries or the impact that the proposed measures will have on the freedom of expression, protection of personal data and the development of scientific research.

This detachment from reality leads to proposals which are as crazy as a national anti porn filter or populist and dangerous as extending discrimination offences to areas such as the Internet. Prohibitions like these are odd because they are so ambitious that clearly they will never be effectively enforced or only selectively against those things that the State cannot keep quiet by other means. These broad and principled prohibitions are very dangerous to a free society and the technophobia of some of our politicians is leading us to take them for innocent.

A new Internet geography for Cuba

Eliocer Cutiño⁴⁴

Many Cubans yearn to discover the possibilities opened by the Internet every chance they have to go online. Youths delve deep into the world of personal relationships and use it mostly to meet new friends or to find relatives or old schoolmates who are no longer in Cuba and have profiles in social media sites such as Facebook.

For them, they point out, it is a wondrous experience. Moreover, they remark that it is more comfortable than writing a regular letter and sending it via regular mail. Older folks often don't see it as a tool that solves many problems, but they still see it as a necessity. This is why young and old alike find ways to make strong connections within the net of networks, without the slightest idea of how it would equally facilitate everyone's social lives.

Quite recently I attended what is known as a Telepunto, part of the Cuban Telecommunications Company (ETECSA, for its acronym in Spanish), the only company on the island that offers Internet service. I had been waiting for two hours to be able to use one of the working computers at the center and a lady who was waiting as well – and who seemed to be eager to talk in order to pass the time – told me that she found the Internet useful to communicate with family and friends, but that otherwise she had no interest in it.

I said that I disagreed, that if she allowed me I could explain other reasons and that I could base them on what she had done that day, if she agreed to tell me. She accepted the challenge and told me she had woken up early in the morning to go to the bank to collect her pension. That errand took her half the morning. Later she went to the bus terminal to try to find a ticket to go on a trip, but she gave up due to fatigue. From there, she decided to go to the ETECSA telecenter to send some pictures to her son, who lives abroad, which is impossible from her Nauta email.

I suggested that I could shorten her errands, based on my experience in other places where the Internet is an everyday feature of people's lives. "Madam, – I replied –, if you had this service in your home, you could have checked online whether your money was already transferred or deposited

⁴⁴ Eliocer Cutiño is an independent attorney and a member of the Camagüey delegation at the Centro de Información Legal Cubalex.

to your account and to know, anytime, whether you have it at your disposal. Moreover, you could have bought your ticket online to travel, and to know which days were available.

Finally, you couldn't just have sent photos to your son, but you could also have talked and even seen your darling, who you may have not seen for years". Her expression changed and the smile of someone who has discovered a new life said it all. She placed her hand on my head, like a grateful mother and told me: "You're very kind, thank you. You're right in everything you tell me".

This brief but true anecdote warns us that there may be many things that we may still be unaware of and that regardless of our age or our interests, any person, one way or another, may be the protagonist of a similar tale.

Some guiding principles for the Internet in Cuba

Recently I've had the opportunity to travel outside of Cuba to participate in some events about internet governance, a topic that is new to me and, though apparently simple, is full of unknowns for any person, regardless of nationality. From what I have learned in these activities, I'd like to highlight two topics that show the peculiarities of the context in which I live: access to the Internet and privacy.

Since the year 1996, the Cuban Ministry of Information Technology and Communications, by means of Resolution 49 of 1996, established that telephony and information signal transmission were the exclusive concession of ETECSA, meaning that this state body controls all policy regarding access to receiving, searching, and sharing information, regardless of the medium.

According to the Inter-American standards, the right to access information must be guaranteed for all persons, and it cannot be restricted except for those cases provided by law to pursue legitimate ends such as national security or the protection of other rights, provided this measure is necessary and proportional. However, and although this issue isn't precisely the point of this text, I think it's relevant to mention that in Cuba, due to an old and outdated legal provision, Law Decree 99 of 1977, the State established, with some exceptions, that most information produced by either the State apparatus or in private and social contexts is a matter of national security.

After becoming familiar with this issue, and notwithstanding the fact that this is a controversial question in other parts of the world, I find it curious how in Cuba, all actions related to accessing the Internet are registered.

This is so common that it goes unnoticed by people, to whom it seems like simple bureaucracy that we still haven't gotten over. This idea isn't so naive, but it's also the way in which, somehow, the right to information online is restricted, as is the technology that allows access to it. It is, de facto, a way to prevent the effective enjoyment of this right for people and communities, effectively resulting in discrimination due to place of residence, that is, to geographic fatalism.

I will try to describe briefly how we connect in Cuba. First, you have to get to one of those small and crowded offices called Telepunto, request a browsing card that costs one to two convertible pesos (1 to 2 dollars), for 30 minutes or one hour online, respectively. To get the card you must present your identity card, which is immediately registered by the government.

If you look closely, there is a bar code and a unique number in the bottom left corner of these cards, which is recorded in a digital registry enabled by ETECSA, in addition to the personal data from the person who purchased the coupon. Completing the form is a requirement to be able to go online, after which one can browse easily, except for the low bandwidth of the service, the possibility that an unseen observer is following all of our searches and the fact that some websites are restricted. In other words, it is as if we were fenced inside an impassable border, even if we feel immersed in a vast sea of information.

I'm talking of nothing other than privacy, a right that recognizes that nobody can be subject to arbitrary or abusive intrusion into their private and family life that causes harm to their life or reputation, or from excessive control over the use of technology, among others. States have the obligation not only to respect it, but to prevent others from unduly infringing upon this right. Insofar as Cuba continues to connect to the world of the Internet, it will be of paramount importance for the government to commit to respect international and Inter-American regulations and standards that pertain this issue. It will also be imperative for the citizenry to become aware of the protection of this right.

Can there be a different vision of the Internet in the Cuban context?

Cuba officially connected to the Internet in 1996. Since then, the net of network is conceived as a public telecommunication service, centrally

managed by ETECSA and exploited by state institutions expressly authorized by the Ministry of Information Technology and Communications.

Decree 209/1996 titled “Access from the Republic of Cuba to Information Technology Networks with Global Reach” sets out the policy that guarantees “full access to the Internet” in a regulated manner, first to legal persons and institutions most relevant for the life and development of the country. Recently, very slow attempts have been made to extend this service to private individuals, although it is still claimed that the technical conditions don’t yet permit this development. However, I believe there are many avenues that can be explored without the need for large investments.

Experiences in other Latin American countries demonstrate that limitations in access to information sometimes are overcome by ingenuity rather than access to resources. For example, in Cuba there are some schools that are connected to the Internet that, despite its low bandwidth connection, could be able to extend the signal using Wi-Fi antennas to the communities surrounding the school building. This has been already done in small countries in the region with great success.

Would a similar policy be possible in Cuba? Just in the province of Camagüey, where more than 120,000 students attend elementary and middle school, and there are more than 670 rural and urban schools throughout the region, implementing an initiative like this one would revolutionize access significantly.

It is also striking how the design of educational programs doesn’t contemplate or even conceive of teaching topics related to the Internet. However, in a nation that has fulfilled the United Nations Millennium Development Goals with respect to education, this pending subject openly contradicts the true interests of students who long for this service and who have made it their own by sharing educational information systems using mobile and tablet apps with the sole purpose of connecting among themselves. This is a partial beginning of digital literacy.

This proposal is far from simple, but I wouldn’t discard the possibility that our vision would open a door to the world of the Internet to Cuban. This vision isn’t at all contradictory with existing rules and regulations, but is an idea that would allow us to further develop our communities, which would play a vital role in the performance and the effectiveness of Human Rights.

The private sector in Cuba and the Internet

This issue isn't just suggestive of what I'm proposing in this writing, but also relevant to the endless possibilities that could be realized if the Internet could reach small startups in Cuba, allowing these subtle alternative economies that are alive today on the island to grow and develop.

In the modern world, this means of connection won't only allow us to communicate with faraway friends and relatives; we can also put it to work for our interests. The Internet provides us the possibility of knowing information about any particular activity not just from Cuba, but also proposals from the entire world.

To better illustrate this idea, think of a person who works repairing PCs, DVDs, recorders, printers, etc. Faced with not being able to immediately fix the device, either because there is a lack of skills or necessary parts, he or she can quickly order a part online or find how to solve the problem through videos and charts, and to do things he or she never thought possible.

If a person operates one of the so-called Paladares, places that sell typical food, or a cafeteria, the Internet is the perfect medium to make your business known in your country and for foreign visitors to read about it ahead of time and learn what it has to offer. These spaces can also provide Internet connection, which will almost certainly increase sales and reservations, and provide better conditions for growing the business. It is an incomparable advertising medium, more efficient and responsive than traditional advertising.

This is one of the details we can focus on to understand this complex scenario. For Cubans this is also a novel medium that helps us break through some of the limitations we have today. Finding a way to connect and develop with just one click is very enticing for these times of dire need to open up economically to the world.

It wouldn't be harebrained to think that what are now known as Non-Agricultural Cooperatives could request this service from the Ministry of Information Technology and Communications. Existing regulations allow legal persons to file such request and, although the matter is surrounded by certain formalism, it is reasonable to try to shift toward providing services and selling goods online, beyond simply sharing information and advertising through this medium. If Internet access is expanded to legal persons such as Non-Agricultural Cooperatives, the circulation of information will not only be seen by Cuban citizens via the so-called "weekly packages", but it would have a broader impact that can even transcend our Caribbean borders.

This is a call to see and recognize our own existing potential from a different perspective in order to be able to develop and expand them. As our options grow, this will allow our capital to increase and to be more successful in our trade relations.

Are there still many people in Cuba who haven't connected to the Internet?

There is still much to do regarding the Internet... It is true that actions have been undertaken to reduce the digital gap, but we should think of this as a right and it is our right to have timely access to this technology. This is why I'd like to share two aspects: one referring to people still lacking access and the second to the obligation of the State.

Access to the Internet means access to receiving, searching and sharing information and ideas without restrictions of any kind. It is, moreover, conceived as a human right, as part of the right to freedom of thought and expression, embodied and supported by the Cuban Constitution in articles 54 and 55.

To cite an example of how many people still lack Internet connection, in statistical terms, I shall use as a reference Nuevitas (Camagüey, Cuba), an industrial city with a significant population and where internet access remains an embarrassment. This town, or villa, as it was formerly known, has more than 61,625 inhabitants according to the last population census. There is one ETECSA telecenter, with four computers connected to a company server where, as I mentioned, one must sign in with a personal ID number in order to have access to the service.

A quick mathematical calculation makes it clear that there is one PC with access for every 15,406.25 inhabitants, representing only 0.0065% PCs per person. Added to the lack of computers, think about the bureaucratic paperwork required to connect, long lines to simply purchase the coupon and also to use a computer. There is no doubt that, to reduce the existing digital gaps, these calculations give us an idea of how much there is yet to do.

Regarding the State, it has the obligation to remove the obstacles that keep the citizenry, or a given sector, from sharing their opinions and information. In the digital realm, this means adopting measures aimed at guaranteeing this service for all people, especially to vulnerable groups. It also means having access under equal conditions, without discriminatory treatment.

In principle, it is the Cuban State, in this case, who must guarantee the free enjoyment of these rights, as established by Article 9 of our Constitution, since all communication media are the property of the State. Besides, it is essential that a plurality of opinions is guaranteed, as well as maximizing openness in the public sphere.

Finally, I conclude with the idea that access to the Internet must be universal in nature and also inclusive. For this, it is necessary to strengthen training and education in all sectors. We shouldn't be content with an Internet that lacks global features. This must be our objective if we wish to guarantee effective Internet access in the future that I aspire to for Cuba.

From the cassette to 'the package,' or how to do streaming without Internet in Cuba

Regina Coyula⁴⁵

In 2008, MySpace was losing the social media race to Facebook, which only reached 200 million people, and had just launched its platform in Spanish. That same year, Cubans were finally able to have a legally registered cell-phone line, the first desktop computers appeared in stores and DVD players were the latest craze. We were so removed from technological novelties that nothing seemed to happen, but in 2008 this disconnected country incubated one of the most innovative (and controversial) ideas for accessing audiovisual entertainment: El Paquete (The Package).

The weekly Package is a terabyte of material in a portable disk drive that covers a broad spectrum of topics. This diversity has guaranteed its current popularity, since it is hard to find enough content to satisfy for an entire week from the most cultured to the most popular entertainment, from the most demanding to the most banal. Since the legal expansion of private employment categories in 2010,^[1] The Package includes advertising about these businesses, in addition to serving as a platform

⁴⁵ Regina Coyula, Havana, 1956. Graduate in History. Discovered the Internet in 2009 and has tried to compensate for so many years of ignorance and disconnection. Editor and webmaster of the Cuban Legal Association (ajudicuba.wordpress.com and derechosclubanos.com). She has contributed to various online publications such as ddcuba.com, 14ymedio.com and BBCmundo.com.

for new music and video clips, which was its initial purpose according to one of its founders.

For this illegal, yet tolerated business, whose magnitude is impossible to calculate, those who distribute The Package adopted a mechanism born from the illicit rental of Betamax, and then VHS tapes, namely home delivery. It is also distributed in pirate sales points (an activity officially registered as “disk purchase and sale”, approved in 2010) or through a broad wired network, also illegal, known as street net or snet. Originally conceived by gamers, today it also supports The Package, chats and as much traffic as it can support in bidirectional and multidirectional communication.

The price of The Package varies. Freshly made, “wholesale” distributors buy it for 10 CUC^[2] and sell it to retailers for 2 CUC, who in turn re-sell it for this same price to their own network. Some folks have a stock of USB drives or they use the drives their customers bring and fill them “a la carte”, generally with high demand programs such as TV series, game shows, reality shows, soap operas or action films. The price of this modality fluctuates, depending on the capacity of the drive, between 10 and 40 CUP. Downloading The Package from the snet is free, as it is all traffic in this network. The proliferation of USB drives has “democratized” the way free content is shared and the notion of a final user becomes a long and untraceable chain.

Many theories are woven around The Package, but the lack of answers leads to speculation: who makes it? How do you compile such a large volume of information in a country where the few household connections average the prehistoric speed of 56 kbps? Some say that The Package is the largest employer in the private sector and that it moves millions. Although this is a reasonable assumption, there is no way to prove it, since those who work in the sector are generally hesitant to answer questions and shy away from interviews.

Against the package

Given its decentralized and practically uncontrollable nature, cultural institutions, the press and the police, have tried to discourage its use. In 2014, La Mochila (The Backpack) appeared as a counter proposal: an audiovisual product with content focused on combating “vulgarity and

banality” attributed to The Package and, incidentally, any criticism of the government. It’s worth pointing out that The Package doesn’t compile controversial, religious or pornographic content; it excludes political content and, recently, it has even deleted humorous content critical of the Cuban government.

La Mochila oscillates between 300 and 350 Gb and it is free to download at the Youth Computer Clubs^[3], but it hasn’t come close to competing with its informal contender. Those who defend La Mochila didn’t seem to understand that education and entertainment don’t always follow the same storyline and the success of The Package lies in entertainment that allows people to unwind.

The Package has been accused of violating artistic and intellectual property; and it has been accused of false freedom of choice, since one has to choose from 1Tb that was previously selected. These are the minor accusations. There are those who see in The Package an enemy plan (internal, external, both?) to “destabilize” the country and impose a mass culture foreign to “our cultural values”.

In favor of the package

It allows one to flee the dreadful national television programming; each one decides what schedule to enjoy and within its contents one can find high quality (and high definition) material, according to one’s own taste.

Despite the criticisms, not even those who oppose it can deny that TV programming contains content whose defects equal or exceed those attributed to The Package and are often equally pirated. On the other hand, most people who sit in front of the TV to unwind prefer to see pretty faces and trivial topics, rather than the ideology of national TV.

The future

The Package has some life left in it. As long as the embargo remains in effect, US companies will be in no condition to file legal claims on their intellectual property. As long as the quality of Cuban television remains erratic and excessively politicized, and as long as a Netflix subscription (which is legal in Cuba) is almost symbolic and the cost of downloading contents remains astronomical,^[4] The Package will endure.

With a more open country, intellectual property laws will be applied and people will resent the withdrawal of many copyright protected content. Will this be the end of The Package? At least it will be its reinvention, if those who manage it remain aware of audiovisual needs and trends.

-
- [1] Small private property, the only kind in the country after the nationalizations of 1959 and 1960, was abolished in 1968. It reappeared in 1995 during the deep economic crisis known as the Special Period, with shy openings that were ended abruptly after Hugo Chávez' electoral victory in Venezuela, and picked up strength again in 2010 with the drop in oil prices, Hugo Chávez' illness and the country's economic crisis.
 - [2] Official convertible Cuban currency, together with the Cuban Peso or CUP: 1 CUC = 24 CUP.
 - [3] Youth Computer and Electronics Clubs are computer rooms opened in 1987 for learning and promoting these disciplines. Currently, they exist in all municipalities and, in addition to La Mochila, which is free, they offer courses, antivirus, games, free software, and mobile applications. Notably they don't offer Internet connection.
 - [4] A 50 minute chapter from a TV series in HD weighs about 600MB and it downloads at 1Mbps speed. The maximum speed offered by ETECSA at public Wi-Fi spots can take 90 minutes, for which one has to pay 3CUC. The average salary oscillates between 20 and 25 CUC per month.

PART

4

INTERNET GOVERNANCE



Internet and statecraft: Brazil and the future of Internet governance

*Carolina Rossini*⁴⁶

After cancelling her October visit to DC, Brazilian president Dilma Rousseff addressed the United Nations General Assembly on September 24th during the High Level Meeting for the Rule of Law. The UNGA is the main deliberative, policymaking, and representative organ of the United Nations and comprises all 193 members of the United Nations. Brazilians welcomed their president's decision to cancel her October trip and address US Internet surveillance in a public, global forum.

President Rousseff noted that illegally intercepting communications, information, and data cannot be sustained among friendly nations. In saying this, she was not simply speaking in the manufactured outrage so typical of politics. She was instead speaking from a very different experience fighting against the dictatorship in Brazil in her youth. In dictatorships, surveillance is an essential tool that protects the regime. This is what makes the right to privacy a pillar for freedom of expression, freedom of opinion, and fundamental to democracy. That's the sad irony of the US government's relentless push to monitor the Internet, including domestic metadata. It's the kind of thing that dictatorships do. The only thing different is the intent.

I'm well aware that nation-states spy on each other.^[1] Most of us who have spent time in international relations know this. But it's usually a matter of spying on each other's governments (or in some cases, businesses) and not on ordinary citizens. (I am a Brazilian citizen living in the US, so I can only assume the NSA monitors my Skype calls home – and, for that matter, my Amazon purchases). We may have simply been naive in believing this was because of principle, when instead it was merely a matter of cost. Now that the transaction costs are low enough, however, anyone may become fair game.

However, Brazil is not a small country and Rousseff is not a fearful president. She looked directly at president Obama while affirming, categorically, that without respect, there is no basis for the relationship among nations. She was also very specific in her stance, demanding a multilateral mechanism to ensure core principles for the World Wide Web. In an act that may invite

⁴⁶ Carolina Rossini is part of the Internet Freedom and Human Rights Project, where she is project director for the Latin America Resource Center.

deeper governance influence for Brazil at the UN and its International Telecommunication Union (ITU) – the international organization that is trying to extend its authority over digital networks – Rousseff called out five essential affirmations for Human Rights on the Internet:

- 1** “Freedom of expression, privacy of the individual and respect for Human Rights.”
- 2** “Open, multilateral and democratic governance, carried out with transparency by stimulating collective creativity and the participation of society, Governments, and the private sector.”
- 3** “Universality that ensures the social and human development and the construction of inclusive and non-discriminatory societies.”
- 4** “Cultural diversity, without the imposition of beliefs, customs and values.”
- 5** “Neutrality of the network, guided only by technical and ethical criteria, rendering it inadmissible to restrict it for political, commercial, religious or any other purposes.”

These principles were applauded by international civil society and mirror the national debate of the Brazilian Constitution for the Internet, locally known as the Marco Civil. The Marco Civil (Civil Rights Framework) would be a domestic groundbreaker, guaranteeing civil rights in the use of the Internet. Internationally, Marco Civil would be for the highest benchmark for “open” Internet legislation ever to be enacted. Rousseff recently expressed her support for Marco Civil and has ordered it to be processed in the Congress under a 90-day fast track review (45 days in the House and 45 days in the Senate).

In thinking that national sovereignty includes the right to live a private life within one’s own borders, Rousseff is not alone. But Brazil is uniquely able to push back at the infrastructure level to encode this principle into the network itself. The country first connected to the Internet in 1990, and connectivity is now available in most areas through a variety of technologies. We constitute more than 94 million of Internet users, and are second worldwide in number of Facebook users. Brazil now wants to provide Internet connection beyond its borders and build more Internet exchange points in an effort to have more control over its communication infrastructure, a core economic element that also allows for better control over what happens to the privacy of its nationals.

As reported by Bill Woodcock for Aljazeera America last Tuesday, Rousseff also announced measures to increase domestic Internet bandwidth production, increase international Internet connectivity, encourage

domestic content production and encourage use of domestically produced network equipment. However, some of these measures are not new nor an immediate response to Snowden's revelations. Brazil has been investing in ICTs for some time, including massive government investments on broadband connectivity with the Brazilian 2010 Broadband Plan – which is late on its deliverables but still is underway. Ultimately, this move suggests that rather than relying on US cables, US companies and US state policy, Brazil aims to achieve a leading role on Internet governance by providing core Internet infrastructure to the country and by connecting the country with other countries in the Global South.

That is to say that Brazilian government may take one of the classic principles of the Internet and apply it to statecraft: interpret the surveillance as damage and route around it. Brazil is one of the few countries that can simply lay new cables over which the US has no control and impose privacy by default in those systems. See for instance, the BRICS cable. By the time it is completed, the BRICS Cable will be the third longest undersea telecommunications cable in the world, covering a distance of 34,000km.

For all the rhetoric of a stateless cyberspace, the raw physicality of the network makes it vulnerable to statecraft. Until now, that statecraft has been dominated by a state that places a prime on certain priorities at the expense of civil liberties. But there is nothing in the network that prevents a state with other priorities from joining the fray.

Does this mean that by creating its own infrastructure, Brazil wants to have more control over the Internet? This is the question we all should have in the back of our minds while the infrastructure is being laid. Brazilian civil society should also demand a series of checks and balances, so we are not surprised later with intelligence programs that the Brazilian government might impose. This need for transparency and accountability is even more pressing now with the 2014 World Cup approaching – Brazil has deployed a massive technology infrastructure to surveil the games and proximal events in the name of security. It will be interesting to see if, how, and when this setup is dismantled. This ICT infrastructure may be able to help or hurt the open Internet depending on its design and its use. Again, we all should watch and see if the distributed design is the mode of this enterprise and if Brazil is really part of the group of countries that support in action, not just in words, the future of an open and free Internet.

[1] For instance, it has been published that the United States used information collected by the NSA to influence the votes of the UN Security Council members on the Iranian nuclear issue in 2010.

Could Brazil become the leader in Internet governance?

Claudio Ruiz⁴⁷

One of the surprises of the last Internet Governance Forum (IGF) was the emergence of Brazil as a country that could potentially overshadow U.S. dominance in these issues. However, the doubts of making concrete changes to the model persist.

As expected, no representative of the government of Chile attended the 8th version of the Internet Governance Forum (IGF) held in October on the island of Bali, Indonesia. This was to be expected not only because of the poor, or rather nonexistent, digital strategy of president Piñera, but more so because, strictly speaking, a representative of Chile has never attended this meeting organized by the United Nations, where government emissaries hold discussions on equal terms with the private sector and civil society about the issues and challenges of the regulation of Internet governance.

As was also to be expected, the agenda for this year was intense and mainly focused on aspects related to security, privacy and Human Rights. The first, a ‘classic’ topic for those who have been following this forum since the beginning, acquired greater importance after the revelations made this year by Edward Snowden, who unveiled the dubious activities of online surveillance on behalf of the U.S. government, putting in check much of the infrastructure on which the Internet rests or at least as we know it.

With regard to privacy and Human Rights, both were analyzed with reference to Snowden’s revelations, although they have also been key elements of the discussion on Internet governance in the past. Unlike previous years, this was the first time that the discussion of Human Rights in the digital environment was treated with particular relevance, as part of an entire section of the program, and having, for the first time, a plenary session specially dedicated to the subject.

Nevertheless, there were two large “elephants in the room” present throughout many of the IGF discussions.

First, the tension between those who argue that the best form of Internet governance is one that seeks to maintain, with some variation, its current

⁴⁷ Claudio Ruiz is Derechos Digitales NGO’ executive director.

state, focusing on ICANN (Internet Corporation for Assigned Names and Numbers): a model known as multistakeholder, which is controlled in a way that is usually considered benevolent by the more naive analysts of the U.S. Government. On the other hand, there is increasing pressure from a number of countries – some with questionable Human Rights records such as China and Russia – to deliver more democratic legitimacy to this governance, using existing structures of the United Nations like the ITU and thus avoid U.S. control of the critical infrastructure.

This tension has become increasingly present after the latest revelations about the NSA and also due to pressure from Brazil, a top-flight actor when it comes to diplomatic relations, with a slightly less dubious record compared to its main partners on this crusade.

Closely related to the above, is the glowing appearance of Brazil as a key player that could stand up to the United States. The full frontal reaction of Dilma's government to the revelations of espionage on the federal government, as well as on key energy companies, was by no means an accident, nor was the fiery speech of the president before a plenary session at the UN.

In many of the main countries of the south, the moves surrounding the spying revelations – which, without going any further, include Chile's and Mexico's president-elect – have been rather gimmicky with varying levels of hype and very little substance, but in the case of Brazil it seems to have become a turning point for taking the lead as a legitimate and vigorous voice for the respect of Human Rights on the Internet.

The approach taken by Brazil has been nothing short of surprising.

Only days before the IGF, and after meeting with Fadi Chehade, on behalf of the ICANN, Dilma announced a global forum using the multistakeholder model to discuss these issues in Brazil in April-May 2014. Without any clear objectives or expected results, and the surprising support of Chehade, there is some concern on the part of civil society representatives that this new forum may seek to undermine the IGF as the global stage for debating these issues.

In principle, it does not seem necessary to create a new global instance, taking into account the need for having real multisectoral participation, which is still not specifically guaranteed by Brazil, and the existing legitimacy of the IGF today, even with all its problems.

The need to create workspaces and debate around how we want the Internet to be built in the future is not only inevitable but also urgent. It seems unreasonable to think that strengthening the benevolent self-regulation and monitoring by the U.S. government into a multisectoral model full of vices, is the best way of solving the current problems. The role of governments is also important and urgent, but with the respect for Human Rights and multisectoral involvement as a starting point. Hopefully the Chilean government can also take an active role in this area in the short term.

Mexico discusses Internet governance

*Israel Rosas*⁴⁸

In mid-February, local ecosystem actors met for the second time in Mexico City to discuss Internet governance. This is a Mexican venture inspired by the Internet Governance Forum and the multistakeholder model.

Defining Internet governance

The term Internet governance refers to the mechanisms related directly or indirectly to the development and use of Internet. The degree of formality of these mechanisms varies depending on their scope, making it possible to identify issues of Internet governance in a range that goes from the development of technical standards to the design and implementation of public policies through to laws and regulations.

A working definition for this term is found in paragraph 34 of the Tunis Agenda for an Information Society, from 2005, while work was being carried out by the World Summit on this same topic. It recognizes that ecosystem stakeholders must work together for the development of the Internet:

34. A working definition of Internet governance is the development and application by governments, the private sector and civil society, in carrying out their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of Internet.

Thus, the working definition recognizes a model for Internet governance in which each stakeholder takes part in equal conditions and on the

⁴⁸ Israel Rosas is analyst of telecommunications and Internet governance related issues.

performance of their respective roles. While the definition contained in paragraph 34 recognizes governments, the private sector and civil society, the ecosystem has also recognized the academia and the technical communities in line with paragraph 36 of the same document. This model for Internet governance is known as “multistakeholder”.

Spaces for discussing Internet governance

Based on paragraph 72 of the Tunis Agenda, the ecosystem requested the UN Secretary General to create the Internet Governance Forum (IGF). This forum was established as a propitious place to discuss the issues of Internet governance under the multistakeholder model.

The original mandate of the IGF was awarded for five years, between 2006 and 2010. In 2010, the mandate was extended until 2015, which means that this year it will be necessary for the General Assembly of the UN to decide if it renews the mandate of the forum, and for how long, if the decision turns out to be positive. This is particularly relevant because Mexico will host the IGF in 2016 if the forum continues to exist.

Regionally, the actors of the ecosystem found that the global Internet governance agenda had some peculiarities with regard to Latin America and the Caribbean (LAC). For example, in relation to digital disparity, there are some regions of the planet where vast populations have access to Internet connections, therefore their discussions are more focused on issues like net neutrality or definitions of broadband. By contrast, there are countries within the region that still have alarmingly low rates.

Thus the Regional Preparatory Meeting for Latin America and the Caribbean, for the Internet Governance Forum (LACIGF) was formed. The first meeting was held in Montevideo, Uruguay, in 2008. Like the IGF, this meeting takes place annually, but around countries of the region. The agenda of each issue remains subject to public consultation among the community, a few months in advance.

Mexico: discussions on Internet governance

As global discussions found their particular agendas at regional level, some countries identified the need to create more opportunities to further discuss these issues. Thus, in Mexico, the Internet Governance Initiative Group came forth as an effort driven by various actors of the Internet ecosystem of the country.

The Group proposed the idea of holding an event inspired by the IGF and the multistakeholder model, leading to the Discussions on Internet Governance, which first took place in November 2013 in Mexico City. At that time, the effort proved to be useful for exchanging views about issues that are relevant to the development of Internet in Mexico.

The second edition was held on 17th and 18th February, 2015. As with the first edition, it took place in the capital and was appropriate for bringing the various actors of the ecosystem together in a single place to express their ideas concerning Internet development in the country.

The working groups focused on the following topics:

- Introduction to Internet Governance
- Government, Data and Open Access
- Net Neutrality
- Tensions regarding Internet rights
- Infrastructure security and resilience of the network
- Security and cooperation with authorities
- Access, competence, reducing the digital divide and multiculturalism on Internet
- Local models for Internet governance

The manifesto for Internet governance

During the second event of Discussions on Internet Governance, the ecosystem revealed the Manifesto for Internet governance. The document was presented during the opening ceremony by the National Digital Strategy Coordinator of the Office of the Presidency of the Republic, Alejandra Lagunes.

The manifesto seeks to concentrate the coinciding factors of the actors and stakeholders of the ecosystem, in order to develop them into a dynamic document that will serve as a benchmark, both at national and international level. Currently, the document is subject to public consultation via a platform for citizen participation, belonging to the Government of the Republic.

Thus, the discussions on Internet governance have established themselves as an appropriate space for any actor of the ecosystem to make their voice heard and sharing their proposals under the multistakeholder model. Sessions can be watched on the YouTube channel dedicated to the event.

The region is preparing for the Internet Governance Forum

Pilar Saenz⁴⁹

From 27th to 29th of August, the Sixth Regional Preparatory Meeting for the Internet Governance Forum (IGF) will be held in Cordoba, Argentina, a discussion space where, in addition for best practice sharing, it will serve to raise issues and challenges implicated in building this great new public space that is the Internet.

What is Internet governance?

Internet is a collaboration product. It began as a partnership between government and academia networks to which was later added the private sector and civil society. For those who are regularly online, the Internet has become a new public space that facilitates organization and participation, as well as becoming a medium for the creation, production and distribution of culture.

At present, Internet has more than two billion users around the world, a towering figure for a medium that has an expansion of less than 30 years. For some persons, the question is how to get to the other five billion users, but for others the challenge is to ensure an open, participative and free Internet for these future users. So they can use it on their own terms to fit their needs and not simply another medium managed by the commercial interests or by the control and regulation of state agencies. Therefore, the challenge is that the Internet remains the space that guarantees, allows and facilitates the exercise of rights and not just a controlled means of communication or distribution channel.

The Internet management, the way in which decisions on its infrastructure, protocols and services are taken, is what is called Internet governance. This refers specifically to “the development and application of principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet”. These topics cover the Internet entire universe and generally augment tensions between various components, for instance, security and privacy, freedom of expression and the protection of intellectual property, innovation and access, among others. Multiple sectors (not only governments and private sector but also the academia,

⁴⁹ Pilar Sáenz, activist of the collective RedPaTodos and member of Karisma Foundation.

technicians and civil society) are simultaneously interested on these topics. Without the equal participation of all stakeholders, the balance could dangerously tilt in favor of the interests of those who hold political, social or economic power, and, consequently, those who can generally be involved in discussion forums and decision making processes.

After a long and thorough analysis, an approach was reached whereby the Internet governance model should reflect the cooperation spirit among stakeholders. In addition, since the network is really an emergent process, which is constantly changing and evolving, its management should be flexible enough to allow changes in response to new technologies, applications, users and challenges. This suggests that it cannot be thought traditionally: a corporate management model cannot be used, as the Internet is not owned by anyone, nor can be operated by a governmental authority, since not all of its infrastructure is public; a mixed management model is not sufficient, since it should allow participation of civil society, academia and technicians in the discussion.

The search for an Internet governance model began in 2003 at the World Summit on the Information Society (WSIS) in Geneva. It continued with the work of the Working Group on Internet Governance, which submitted its report in 2005. Finally, during the second phase of the WSIS in Tunis, that same year, it was decided to create the Internet Governance Forum (IGF).

The IGF is a multistakeholder forum (this concept goes beyond the notion of multi-sectoral, as it implies more commitments of the parties, the absence of barriers to access to discussions and equal participation) that provides a space for dialogue between different stakeholders on the Internet's public policy issues. It is part of a cooperation agreement between stakeholders to address issues relating to public policy on the Internet, and not to its technical and operational management. Finally, it is accepted that Internet governance should be a multilateral, transparent and democratic model, with the full involvement of governments, the private sector, civil society and international organizations, whose objectives are to ensure an equitable distribution of resources, facilitate access for all and assure a stable and secure functioning of the Internet, taking into account multilingualism.

The invitation is to participate in the discussion

The Internet Governance Forum is an exploration effort. It is a free access space that is not designed to make decisions, but to confront different points of view and to stimulate dialogue and discussion in order to establish a good practice standard.

The IGF can lead to practical results if the conditions for the exchange of knowledge and experience are given, including for listening the web users and helping identify new issues to be addressed in the formal processes that are being managed by Internet specialists. Thus, the IGF and regional preparatory meeting are forums that bring together governments, companies, NGOs, groups of consumer rights and Human Rights activists, Internet specialists and media in one dialogue where all participants have to adjust their expectations. Among the topics to be discussed at the sixth regional preparatory meeting for the Internet Governance Forum, to be held this month in Argentina, are, among others, access and diversity, privacy and Internet security.

The call is to get involved in the global discussion processes, but also at regional meetings, in where policies can be consolidated, and best practices and problems can be shared. The sole aim is to invigorate the processes of civil society groups that increasingly bring together collectives, institutions and individuals that advocate for the Internet and use it to vindicate other rights.

Technology must be leveraged to follow the proceedings, even remotely, and to participate in the discussion. There is no doubt that the contributions in this matter will greatly influence the future of humanity, as there is no barrier to participate, it is just a matter of getting involved.

Netmundial and the future of Internet governance

Marília Maciel⁵⁰

The Internet governance regime is going through a moment of re-evaluation and changes. Under the United Nations, several meetings will be held in preparation to the review of the World Summit on the Information Society (WSIS+10), which will take place in 2015.

1 A geopolitical shift and the role of Brazil

In parallel, the United States government announced its willingness to transfer the stewardship of the IANA functions, particularly of its unilateral oversight over the root zone file (a server that is the base for the functioning of the domain name system) to the multistakeholder community. In the

⁵⁰ Marília Maciel is a researcher and coordinator of the Center for Technology and Society at Fundação Getúlio Vargas (FGV) Law School.

midst of these processes, the Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial), convened by the Brazilian government, was an important milestone.

The fact that a developing country took the lead on these discussions is a symptom of a shifting balance among governmental actors. The United States lost its moral high ground after Snowden's revelations, creating a relative vacuum of leadership. Therefore, there are political conditions to promote the redistribution of power in the regime in favor of developing nations and to try to move forward issues that have been stalled. Those seem to have been the goals of the Brazilian government when it decided to convene NETmundial.

The meeting was also marked by visible lack of coordination among BRICS countries on Internet issues. Russia heavily criticized NETmundial and did not accept the final document. India was more moderate and affirmed that the country could not endorse the document as a whole, although it contained many positive aspects. The meeting happened in the moment in which Brazil has established a positive dialogue with European countries, particularly with Germany, on Internet Governance issues. The problem of mass surveillance brought them together, but the collaboration is being extended to areas such as privacy and infrastructure.

In the institutional debate, Brazil argues for the need to conciliate multilateral and multistakeholder arrangements. The country defends the creation of a centralized platform to discuss public policy issues, with the full participation of all stakeholders, on the understanding that "fragmentation of policy spaces, among other factors, greatly undermines the ability of under resourced groups to engage with global Internet governance, because they are unable to be present in all places". Brazil did not detail what kind of arrangement it envisions, but it would probably need the collaboration of other developing countries, such as India, in order to give political weight to its ideas. This puts Brazil in a challenging position, as it needs to develop a broad range of diplomatic alliances.

2 NETmundial outcome document

The agenda of NETmundial covered two main points. The first was the identification of universally acceptable principles related to the Internet. The second was the identification of a roadmap for the evolution of the institutional architecture of the Internet governance ecosystem. This last topic encompasses the governance of domain names and IP numbers and the process for the development of global public policy issues related to the Internet.

In terms of substance, some important achievements were made in NETmundial. Human Rights were mainstreamed: they should be equally respected online and off-line and should underpin the development of the whole ecosystem. The right to freedom expression and association, the right to development and the role of the Internet to promote it, for instance, were included.

Surveillance was an important topic as well. The document took into account the problem of collection and processing of data, not only by governments, but also by private actors. This approach was positive, since existing documents seem to be focused on governmental activities. It was unfortunate, however, that the principle of proportionality – widely recognized in international legal doctrine – was not included as a limit to surveillance related activities.

The document recognizes the importance of the participation of all stakeholders in the discussion of cyber security issues and that international cooperation on topics such as jurisdiction, law enforcement, cybersecurity and cybercrime should be held in a multistakeholder manner. This is a remarkable process, if we consider that most of the processes in this area have been intergovernmental.

Multistakeholder participation – the involvement of governments, civil society, companies, the technical community and academics – was considered a pillar of the Internet governance regime. It was also recognized that the respective roles and responsibilities of the stakeholders should be interpreted in a flexible manner with reference to the particular issue under discussion. By doing that, the document offers a more up to date interpretation of the roles and responsibilities set forth by the Tunis Agenda, which granted limited roles to non-governmental actors, which do not correspond to the reality of Internet policy development. Coupled with that, the NETmundial document also recognizes that the roles and responsibilities of actors is one of the topics that need further discussion and understanding, together with issues of jurisdiction, a benchmark to evaluate the implementation of the aforementioned principles and the issue of network neutrality.

A distributed, decentralized and multistakeholder model of Internet governance was endorsed by the meeting. The majority of participants seem to believe that it would not be appropriate to create one centralized body to deal with Internet issues, but to take advantage of multistakeholder networks and, possibly, of mechanisms for improving coordination.

Great emphasis was put on increasing transparency, accountability, effectiveness and globalization of institutions. That also applies to Internet Corporation for Assigned Names and Numbers (ICANN), responsible for the management of the domain name system. Participants expect that “the process of globalization of ICANN speeds up leading to a truly international and global organization serving the public interest with clearly implementable and verifiable accountability and transparency mechanisms”.

3 NETmundial: the process

NETmundial Multistakeholder Statement^[8] – the outcome document of the Meeting – was elaborated in a very open and participatory manner, by means of successive consultations. The Multistakeholder Executive Committee (EMC) was the body responsible to go through more than 180 contributions presented in the online platform and to draft an initial outcome document based on these contributions. This draft was put under public consultation online. More than 300 comments were presented.

The comments received online, the points that were raised from the floor during the two days of NETmundial and the comments made by remote participants (NETmundial hubs and individuals) were analyzed by the EMC to produce the final draft. On the last stage, this draft was presented to the High Level Multistakeholder Committee (HLMC) for political validation. This particular moment was one of the shortcomings in terms of process. HLMC’s main responsibility was to ensure that the international multistakeholder community would meaningfully engage in the NETmundial process. However, the valuable political resources of this committee remained underexplored until very close to the meeting. The HLMC had little contact with the process of drafting the NETmundial text and with the consultations being held, but it was informally given the capacity to veto parts of the text right before the final plenary session. This was the moment in which some controversial changes were made, such as the weakening of the text about the separation of the policy and operational aspects when seeking for a new model to perform the IANA functions or the inclusion of an OECD text about the limitation of responsibility of intermediaries. This was considered an undue influence by some actors and this would be a procedural issue to improve for the future.

On a positive note, all the drafting sessions in NETmundial were open to observers, who could follow the changes made to the text in real time. The openness of the drafting process is an important legacy of NETmundial.

4 Conclusion

NETmundial was an unprecedented event, in which an outcome document was generated in a multistakeholder way. The meeting showed that it is possible to extract concrete outcomes from multistakeholder discussions: the methodology of NETmundial could be improved and maybe replicated in other global multistakeholder processes, such as the Internet Governance Forum (IGF). Even if the outcome document is the result of compromise (therefore the language will certainly not please all the actors), it presents positive steps forward, both on principles and on roadmap.

The document will be as relevant as actors decide it to be. If the ideas contained in the document are good and useful, they will certainly be taken forward to other fora and upcoming meetings, serving as tool to influence the WSIS review process. Politically, NETmundial represents the existence of a window of opportunity to promote a healthy redistribution of power in the Internet governance regime that could tip the balance towards the Global South.

Argentina and progress towards multistakeholder model

Ramiro Alvarez Ugarte⁵¹

Under the NETmundial meeting held last month in Brazil on the Future of Internet Governance, Argentina announced the creation of a national organization dedicated to raising strategies on Internet governance. This was an announce on which Argentine delegation not overemphasize: Communications Secretary Norberto Berner did not even mention the issue in his opening speech.

Anyway, this is a significant event. Through Resolution 13/2014, the Ministry of Communications of Argentina created the Argentine Internet Policy Committee (AIPC). And it is a space that seems to be the first step toward a multistakeholder model in governance in Argentina. But it is thought that the process will be slow.

Indeed, the first step of the AIPC will be to develop Internal Operating Rules which will aim to “coordinate the participation of the various stakeholders

⁵¹ Ramiro Alvarez Ugarte is Access to Public Information Area of ADC's director.

and to design a national strategy on the Internet and its governance”. And the first step on this path is to articulate positions inward state. It will be after this internal process that AIPC will open to other sectors, which is necessary for a true multiparty governance model.

These models are complex: the incorporation of different actors leads necessarily to question the logic behind the model of action and representation of each of them. And for the time being, from the State, there were conflicting signals. Indeed, Berner recognized the complexity of the process and the autonomy of each sector to define its way of action when he pointed out in an interview to a newspaper that “the first challenge is to define who are, in Argentina, the multiple stakeholders”. He noted that “the first step is to define the universe, define how representation theory will operate. But beware: each sector has to choose their represented ones, that then will speak at AIPC. That will not be something I decide”.

The definition is interesting because it accounts for the relative autonomy of each sector, a necessary element for multistakeholder governance model work as it is supposed to do. But other definitions of Berner generate certain precautions. For example, Berner said it will be necessary to “go find out all the associations that are related to internet, but especially those who have the representation of users”, which conflicts with the relative autonomy that was mentioned earlier. It is also problematic that certain actors – as Fibertel – have been excluded before the deliberation process has even begun.

In any case, Argentina is not innovating: multistakeholder governance model has several years of operation at international and local level. What is at stake here is to create a process of deliberation and action broad and inclusive, where all stakeholders are involved in the design of regulations of a public good as the Internet. Argentina seems to have taken the first step in that direction.

The need for a digital agenda in Bolivia

*Camilo Córdova*⁵²

In the run up to a presidential election, a civil society group is organizing itself to propose a digital agenda to the Bolivian candidates. The issue is becoming urgent as delays in creating a serious digital development plan will only increase the levels of social exclusion.

⁵² Camilo Córdova is an activist and representative of the collective “More and Better Internet for Bolivia”.

Social exclusion is a process by which individuals or groups within a population are completely or partially excluded from fully participating in the society that they live in. Analyzing the Internet connections in Bolivia under this concept allows us to identify the following problems:

Economic exclusion. Only people who have sufficient financial resources can afford access to the Internet. Currently the price of a 1Mbps ADSL connection represents 18% (average cost of an ADSL connection 1mbps = \$ 35) of the national minimum wage (\$ 205) while in the rest of South America the fees do not exceed 7%.

Exclusion due to speed. Bolivia has one of the slowest Internet access speeds in the world. According to a UNDP report (2012), 70% of Internet connections in Bolivia have speeds below 0.512 Mbps, so it is no surprise that Bolivia often gets compared to Africa when it comes to Internet speeds.

Exclusion due to coverage. In Bolivia, only 3.33% of the municipalities have access to quality Internet via a DSL connection. Access is limited even in urban areas, such as the case of El Alto - La Paz, where ADSL coverage shows us that only 10 out of 650 areas have Internet access.

Moreover, Bolivia does not have an ICT strategy or digital agenda for development. Among the government programs of the candidates for the upcoming presidential elections in October this year, there are no structured public policy proposals based on the use of ICT, yet it is clear to see the need for development plans in order for them to be implemented.

Within the framework of such poor connectivity, and while the country finds itself in a period of elections, members of a citizen group called “More and Better Internet for Bolivia” are pushing for the creation of a digital agenda. How could this be interpreted? According to Ernesto Piedras:

They are a set of private, public, academic and social policies to promote economic development based on the use of Information and Communication Technologies (ICT). However, they are NOT about solely increasing the number of Internet users, nor the government acquiring new technology or creating ICT business incentives. Neither are they about setting up websites for government agencies or teaching computing at schools... All of these would be isolated efforts that would not include everybody and not promote the growth of the whole country.

The civil society event called “Digital Agenda for Bolivia” gathers specialists, technicians, activists, academics, entrepreneurs, authorities and general users with the aim to provide a space for citizens to discuss the state of technology in our country and create a joint agenda of citizen demands related to the topic. Additionally, there is the proposal

of solutions for the problems that are identified, which would be useful for the political parties so that they can take on the agenda, analyze and implement it within their government programs.

Without a digital agenda that covers regulatory and economic challenges, including citizen use of technology, the State runs the risk of perpetuating the social exclusion of Bolivians from the democratic global platform that the Internet has become. At this point, it is the duty of the presidential candidates to consider the scope of this issue in the development plans for Bolivia and we hope that the efforts of civil society in the formation of a participatory and democratic agenda will be valued by the upcoming authorities.

Internet governance in Colombia

Gloria Meneses⁵³

At Digital Rights LAC, we wanted to ask different specialists in the region about their personal appraisals on digital rights issues. This is the case of Gloria Meneses from Colombia. We asked her what the main achievements were of 2013, regarding the work of civil society in that country in relation to Internet governance. Here is her reply.

Since 2012, the RedPaTodos collective and the Karisma Foundation have shown interest in the issue of Internet governance. For this reason, we have participated in IGF and preparatory meetings. For further discussion, we formed a multistakeholder group on this subject. During 2013, this initiative was consolidated with the participation of civil society organizations (Colnodo, FLIP, AGEIA DENSI Colombia, Karisma Foundation and RedPaTodos), the private sector (.CO and Google), government interest (both MinTic and the CRC have accepted to participate in future meetings) and some people associated to academia (University of the Andes, Javeriana University and Jorge Tadeo Lozano University).

The main objective for 2014 is to include the issue of Internet governance into the government's agenda and to further the discussion in order to ensure its presence in regional and global forums, representing the country's position. Furthermore, to elaborate on some key issues such as neutrality, regulation and Human Rights on the Internet. In that vein, we expect to hold a national forum on neutrality during the first quarter.

⁵³ Applications developer, member of the Fundación Karisma.

Moreover, together with Colnodo in Colombia, and similar organizations in Latin America, we have supported the initiative of seeking dialogue with the LACNIC civil society. Within this space, we hope to participate in discussions at regional level and even propose forms of cooperation between groups and initiatives around the region.

Last but not least, some virtual activities are also being planned, related to the use of social networks as a means of positioning the subject, together with face to face meetings in other areas, including universities, and participating in related events, even covering technical aspects, where a subject could be shown and thus expand participation to other individuals and organizations who may be interested.

Civil society's role in the Internet governance debate

*Amalia Toledo*⁵⁴

A couple of months ago, I had the opportunity to organize and moderate a panel discussion at the Online Freedom Coalition (FOC) conference, which took place in Tallinn, Estonia, from 28th to 29th April 2014. The panel “Experiences of Civil Society to nurture the international debate on Internet Governance” aimed to generate a dialogue on how to promote civil society participation in the global Internet agenda.

The panel was formed from activists from Latin America and Africa – Paz Peña from the NGO Derechos Digitales (Chile) and Lilian Nalwoga from Collaborative on International ICT Policy in East and Southern Africa (Uganda) –, and academics from North America and Europe – Robert Guerra from CitizenLab (Canada) and Kristina Reinsalu from the e-Governance Academy (Estonia). As ideas were shared and developed, the dialogue with the audience became vibrant and passionate, allowing us to share, reflect and present concerns and opinions about civil society involvement on Internet governance.

During the conversation, it was emphasized how the multistakeholder model has allowed an increasing civil society participation in international discussions on this matter. However, this has not been translated into an entirely democratic and egalitarian model for stakeholders. Many times, those who hold political and/or economic power cornered civil society

⁵⁴ Amalia Toledo is project coordinator at Karisma Foundation's Law, Internet and Society Group.

and the many interests that it brings to the table. In this sense, Paz Peña said that, at the international debate, the public interest has lost place, so it is time to put back into the agenda the recognition that the Internet is a public good. She added that the cyberspace, on the other hand, is a place that offers the opportunity for networking, bringing distant and disparate groups close together sharing many needs and interests. And this may serve, among others, to challenge the dominant patriarchal models in order to empower women and transform the established power structures in the interest of creating a more egalitarian society.

On the other hand, Kristina Reinsalu shared some Estonian efforts intended to promote citizen participation, leveraging digital technologies and, thus, fostering more transparent models. One example she offered us was the notion of crowdsourcing for the development of initiatives that arise from civil society and which are made possible thanks to the networks woven in the cyberspace. In Estonia, she told us, civil society has developed an online crowdsourcing platform in which citizenship has worked on policy proposals that have the potential to improving the country's democracy. In mid-April, the president of the Republic submitted 15 proposals that were born of this process. As of today, the proposals are under review and discussion in the legislature. Several aspects can be highlighted in this process. Undoubtedly, Estonia boasts a robust civil society, able to propose. This goes hand in hand with the recognition and promotion by government political branches of the civil society role in the construction and advancement of a participatory democracy.

Robert Guerra highlighted some of the benefits bringing by civil society, such as the ability to attract online users, contributions to global discussion agenda – i.e., narrative related to development, disability, gender, Human Rights –, activism that has managed to question governmental actions, demanding accountability, etc. However, Internet is a place of challenges and transformations. And as regards to Internet governance and the multiplicity of meetings and forums that are addressing the issue, he stressed the massive difficulty for participating in them. Therefore, he drew attention to the need to promote mechanisms to facilitate civil society participation.

East African panorama, according to Lilian Nalwoga, is far from the Estonian. There are few civil society organizations that are working on the subject, four in Uganda and a few others in East African countries. She told us that encouraging participation with other stakeholders is a real challenge, because there is no political will, lack of knowledge and understanding on the subject by both the government and social sectors, and because the issue is not yet seen as one of public interest. The trend, however, has been the adoption of laws to silence the voices of users,

to stifle the critics. In this sense, Lilian stressed the need for both civil society and the private sector to find common ground, and promote closer dialogue with governments. In this way, she said, the subject could be brought to the national and local arena in East African countries.

Other ideas were highlighted. Responding to the question how the FOC could support, in the long term, civil society, the answer can be summarized in the following sentence: “You have to practice what you preach”. That is, if this intergovernmental coalition seeks to advance Internet freedom, fostering a forum for governments to coordinate efforts and work with civil society and the private sector in a multistakeholder process in order to support the capacity of people to exercise their Human Rights and fundamental freedoms online, then, it is expected that commitments made and actions taken are based on that aim and do not remain empty words. At the end, governments represent their citizens; therefore, they shall protect interests by the group as a whole, and not a select few.

A constant concern is the funding source for civil society and its participation in international forums. Although no response to this difficult issue was offered, it was stressed that in order to promote a balanced debate on Internet governance, it is required to tackle this problem and offer greater stability and opportunities for civil society.

Finally, the panel closed with a reflection that called for activating solidarity mechanisms among civil society. And on that, the Latin American civil society has a lot to show and share with the world.

My Experience with the Internet

Karina Gálvez⁵⁵

“I know nothing about the Internet!”. This was my first reaction when I was invited to participate in the South School on Internet Governance, an event held in Washington D.C. from March 29th to April 1st. This feeling didn’t disappear throughout the whole encounter, but rather grew.

My encounters with the net of networks until then had been as a user, to search for specific information, always knowing ahead of time which steps I had to take to get to it. When I started to hear about IPv4 and IPv6 protocols, domain names, zero rating, net neutrality, and other technology concepts, my feeling of knowing nothing about ITCs became a certainty. But I had

⁵⁵ Karina Gálvez is an economist and co-founder of the Centro de Estudios Convivencia in Pinar del Río.

found a great treasure: I had the curiosity and the conviction that I needed to know, especially after having heard that the internet can facilitate the realization of one of the most basic Human Rights: freedom of expression.

A workshop with three friends experienced in the issue drew the curtains from my eyes and, boom! there I was: after just one week participating in the South School on Internet Governance, asking questions and understanding. I couldn't believe it! It almost seemed easy. It wasn't really, but an approach to the most elementary concepts, in the clearest and most didactic way, with practical examples and participatory discussions, made this workshop my first real entrance into the world of the Internet, into which I had but glimpsed, without daring to cross the threshold.

At the LACIGF, held in Costa Rica on July 27th-31st of this year, I was impressed by the movement of ideas and people around these topics. Every sector represented participated in the discussion under equal conditions: the State, the private sector, academia, the technical sector and civil society. Some of us Cubans also participated, but it was hard to feel party of the discussions.

In Cuba, the problem isn't lack of economic resources (though they exist) or lack of concern by the government; the main difficulty for Internet access is the lack of political will. This is the same reason why there aren't any independent publications or private companies: the Cuban government blocks any personal initiative from its citizens.

In Cuba, it is very difficult to access the web. The possibility to use the Internet through Wi-Fi hotspots in some parks around the country, paying the equivalent of 2 dollars per hour, with salaries that range between 25 and 30 dollars per month, cannot be considered even minimally acceptable access for any person in the 21st century.

After participating in the workshops, it was very clear to me that the Internet access problem in Cuba was an extension of the violation of the right to free expression. Just as the right to free and public expression is violated by law, the right to be connected and to access new technologies that facilitate this right isn't even part of the public debate.

Nonetheless, today there are many people in Cuba who use Wi-Fi in parks and who connect mainly to communicate with their relatives off the island through video calls or via Facebook. There has also been an increase in small businesses (called "independent workers" in Cuba) who work with technology: cell phone and computer repair shops, software updaters, etc. How do they do it and how did they learn without an Internet connection and without resources? I don't exactly know, but what is true is that in Cuba you can find cutting edge technology and people with the technical skills to use it.

My curiosity when entering the world of the Internet and its governance, especially from its social and Human Rights connotation, had to be shared with other people and communities. First, I thought that it would be enough to relate with people already within this world and, at a small scale, I did. I spoke with young telecommunications students who work in technology-oriented jobs. Their professional and technical training was clear from the way they spoke and they were as amazed as I when the conversation turned toward matters of Internet governance, net neutrality, communications surveillance, zero rating or who decides domain names.

It is rare to find a debate on technology and society in Cuba. It is nonetheless possible (although I cannot be sure that in official and academic circles these matters are discussed, the citizenry is kept out of these debates). I was even more impressed when speaking with people who never connect to Facebook, for instance, a 70 year-old lady told me: "I would love to be able to see the world through the Internet!". One person asked me: "Is it true that Cubans are less connected than Haitians?".

After using a new invention, humanity moves at a faster pace and then, in the midst of debates and discussions, it looks back on the social problems and the divisions it has created, and we realize how we distance ourselves from human dignity when we're clouded by the advantages offered by these great inventions or discoveries. This looking back isn't backtracking however, nor a rejection of the good, but rather pausing to observe what we should change and how to do it. We look back to calibrate and moderate, to synchronize progress with human development, which is, after all, the ultimate goal. This is the effort currently underway on the Internet.

Cuba begins its connection to the Internet at a time when the world is looking back on the most all-encompassing communications phenomenon in human history. Even with difficulties, we begin to connect. Joining the world of the Internet is an advantage for the Cuban people. We didn't seek this advantage, but we must nonetheless make the most of it. Cuba has no reason to suffer the same problems as in the beginning. We can be a nation that respects the right to be connected, avoiding discrimination, violations of privacy and conformism with only partial low-cost Internet options.

The Cuban citizenry has the right and the duty to participate as protagonists in this process that is just beginning on the island, but first we must train, educate and inform ourselves.

To me, this has been a first incursion into the world of interconnection and now I'm sure of two things: from now on, we cannot live without the Internet and we must know it well if it is to make us ever more human.

PART

5

COPYRIGHT

Copyright law reform in Brazil

Eduardo Magrani⁵⁶

The advocates of access to knowledge cause perceive the current moment as a turning point on the formulation of a democratic management, concerned with the interests of all those who dedicated themselves to the process of updating copyright and ensuring its social function.

The Brazilian Copyright Law reform imposes itself as an efficient and viable solution to the contemporary Brazilian crisis. However, it should not be considered separately from all the other social and legal solutions, since it is only one of many other instruments destined to ensure the balance between the copyright interests and the interests and rights of society in general.

The legislative copyright reform consists on a great necessity and is the adequate path to update the law to Brazil's contemporary needs. Also it could correct deviations related to both the process of maximizing the copyright protection and the problematic associated to the distorted law-making process.

Conscious of the current law shortcomings and of all the problems it involves, Juca Ferreira's mandate as minister of Culture (2008-2010), under the commands of president Lula and in accordance to the previous minister's management, attempted through the Copyright Law reform to develop and to strength the country's cultural economy. These measures would ensure, at the same time, the authors' constitutional rights and society's right to education, culture and information. Historically, it is the first time Brazil adopts a progressive attitude towards copyright regulation.

After a long process of hearings, seminars and meetings, initiated in 2007, that involved many different groups of Brazilian society, the Ministry of Culture elaborated a bill to Copyright Law reform, which was taken to public consultation in June, 2010.

During public consultation, the Ministry of Culture presented elucidative explanations that allowed society to understand the exact government intention towards Copyright Law reform. Among the main goals of the

⁵⁶ Professor of Law and Technology and Intellectual Property at School of Law at Fundação Getulio Vargas (FGV). Researcher at the Center for Technology and Society (CTS-FGV). Project leader on E-democracy and Internet of Things. Brazilian coordinator of Creative Commons and the Digital Rights: Latin America and the Caribbean project.

proposal, we can highlight the following: to widen and ensure effective incentives and ways of protection to authors and their creations; to promote the balance between the rights of all stakeholders; to widen and democratize the access of general population to cultural goods and services; to ally the current legislation to the new paradigms established by the digital environment; and to enable State's actions towards the creation of public policy to promote, supervise, regulate and protect both society and national interests inside and outside the country.

On December 23rd, 2010, the bill's drafting was finished and its final text was sent to the Chief of Staff with alterations inspired mainly by the almost eight thousand comments made by society through online mechanisms of public consultation.

In January, 2011, Ana Buarque de Hollanda was nominated to the head of the Ministry of Culture and, due to this management modification, the Copyright Law reform bill returned from the Chief of Staff to the Ministry of Culture. During the text analysis made by the new Minister of Culture, together with the head of the Intellectual Property section of the Secretary of Cultural Policies, it was decided that the text would be reopened to public consultation. This new process occurred between April 25th and May 30th, 2011. This time, however, it was done in a less democratic and accountable manner, since only specialists could comment about very few selected topics. After this chapter of the bill's elaboration was finished, the text was sent back to the Chief of Staff.

Since the first month of her management, Ana de Hollanda made clear she didn't share her predecessors view about the promotion of free culture, especially on online environment. Therefore, she turned backwards.

After almost two years of harsh criticism, Ana de Hollanda left the Ministry, leaving behind a legacy of political inability to deal with important civil society groups. She was also known for going against the interests related to free culture and access to knowledge.

In September, 2012, president Dilma Rousseff nominated senator Marta Suplicy - member of PT, ex-Mayor of São Paulo and ex-Minister of Turism - to replace Ana de Hollanda. As one of her first acts as Minister of Culture, Mrs. Suplicy brought back Marcos Souza to his former office. Before being dismissed by Ana de Hollanda, Mr. Souza was responsible for the head of the Intellectual Property section under Gilberto Gil's and Juca Ferreira's consecutive mandates as Ministers of Culture (2003-2010).

Marcos Souza was the main advocate inside the government of the Copyright Law reform. He was discharged from his office on March, 1st, 2011, two months after Ana de Hollanda had been appointed to be the new Ministry of Culture. Through this action, Ana de Hollanda made clear her disagreement towards one of the main pillars of Lula's cultural policy.

Due to management change, the bill returned to the Ministry of Culture. Soon it must be sent to the National Congress, reawakening the debate on the importance of Copyright Law reform.

The advocates of access to knowledge cause perceive the current moment as a turning point on the formulation of a democratic management, concerned with the interests of all those who dedicated themselves to the process of updating copyright and ensuring its social function.

Colombian constitutional court overturned copyright law

*Carlos Cortés Castillo*⁵⁷

On April 13th, 2012, the president of Colombia Juan Manuel Santos signed Law 1520 – known among the media and social networks as ‘Lleras Law 2.0’ –, which main objective was to increase the legal protection against copyright infringement. Last January, but just recently available, the Constitutional Court overturned it arguing procedural irregularities, leaving behind any analysis regarding its content.

Law 1520 implemented some of the intellectual property provisions of the Free Trade Agreement (FTA) signed between Colombia and the United States. In general terms, Law 1520 raised the protection threshold for copyright infringement, both in general terms and specifically for the Internet, on issues such as Digital Rights Management and Anti-Circumvention provisions.

Senator Jorge Enrique Robledo (prominent member of the left-wing Polo Democrático Party) challenged the law claiming two procedural issues: on one hand, as the First Commission of both the Senate and the House are in charge of intellectual property issues and related rights, they should have approved the law instead of the Second Commission of each chamber.

⁵⁷ Colombian lawyer and journalist.

On the other hand, taking into account that the law affected the right to freedom of expression, it had to be passed as a Statutory Law.

Several offices of the Government, the Ombudsman Office and several private groups defended the constitutional grounds of the law. Most of them argued that the Second Commissions in Congress are in charge of bills related to international commerce and treaties, among others. Hence, as Law 1520 was basically implementing international obligations under the FTA, the procedural requirement was properly followed.

In addition, the defenders of Law 1520 said that the constitutional precedent pointed towards a flexible interpretation of the commissions' competences, as bills usually include several topics that fall under different commissions. Although Law 1520 did address intellectual property issues – they said –, it certainly developed international commerce affairs.

By means of ruling C-011 of 2013, the Constitutional Court acknowledged the flexibility criteria, but dismissed such argument in this case. According to the Court, there is a difference between the topic of a Law, which determines the commission's competence, and the source or framework of the obligations that develops. Beyond the FTA, Law 1520 is an intellectual property regulation:

“At this point it is worth emphasizing that what has been subject to the constitutional control of this Corporation is the internal regulation regarding the economic rights of the authors, pursuant to the commitments acquired by the Colombian state under the Trade Promotion Agreement with the United States, having the law under examination no connection with trade relations between the two States, neither it relates in any way to the international scope” (informal translation).

Having determined this procedural fault, the Court declared Law 1520 unconstitutional and refrained itself from any further analysis. While it was foreseeable to avoid any content judgment once the procedural challenges succeeded, the Court could have said something regarding the nature of Law 1520. That is, if it was necessary to pass the bill under the statutory proceeding.

Last year, president Santos had summoned Congress to pass the bill under urgency conditions – triggering a shorter legislative process –, to have it ready for Barack Obama's visit to the Summit of the Americas, which took place in Cartagena, in April, 2012.

This political gesture prevented an adequate discussion in Congress and within civil society. Back then, a group of international intellectual property academics and experts sent a letter to the presidents of both the Senate and the House expressing their concern for the bill: “We find that many of the changes that upgrade protection for copyright go beyond what the FTA requires and are, in fact, more restrictive than U.S. law itself”.

In similar terms, civil groups like the Foundation For Press Freedom, Karisma Foundation and the Center for Freedom of Expression Studies of Palermo University in Argentina, addressed before the Court different issues regarding the balance between freedom of expression and copyright enforcement in Law 1520.

The Court did not solve such issues, which will be back in the public agenda in the coming weeks. Last May, the Ministry of Foreign Trade filed – as an ordinary law – Bill 306, which, in general terms, is the same Law 1520. Apparently, the government took in some of the criticisms and did not request an urgency process. However, we will have to see if they will allow the bill to be debated among civil society.

Access to culture and copyright in Uruguay: #noal218, a civil society victory

*Jorge Gemetto*⁵⁸

In the course of a few weeks, the Copyright Law was no longer an unknown subject in Uruguay and moved to shake the cultural community, occupying a place in the mainstream media.

In early July, the Uruguayan government had included an article in the Accountability Bill (one omnibus bill that mostly deals with administrative issues), which extended the term of copyright from 50 to 70 years after the author’s death. Article 218 (that was its number in the bill) was included at the request of the Uruguayan Chamber of the Record Industry (CUD, in Spanish) in coordination with Uruguay’s General Association of Authors (AGADU, in Spanish), entities that historically led the Copyright Law reform, succeeding in imposing growing restrictions. This time, for the first time, they received a political setback, due to strong opposition from many sectors.

⁵⁸ Jorge Gemetto is co-director of “Ártica”, a Cultural Center online (Uruguay).

#noal218 [‘not to 218’] was the response’s name of various civil society organizations, students, musicians, writers, illustrators, actors, editors, feminist groups, free software groups and international Human Rights organizations, which joined forces in the initiative to remove the article in question and to avoid, as pointed out on its blog, the “privatization of culture in Uruguay”.

The main virtues of the #noal218 movement were the fast reflexes in launching the campaign, the articulation of various recognized social activism sectors, the determination to seek audience with political representatives and formulate before them the claim, the ability of network organization and the proper use of digital media.

When evaluating the movement’s success, none of these factors was less important than the other. In several media, it was stressed that #noal218 was a social media phenomenon. And, indeed, in part it was. Undoubtedly, effortless use of online communication by young activists, digital media savvy, was a unique characteristic of the movement. It was impressive the communication pace of the movement, with discussions and debates that opened on social networks all the time, as opposed to the silence of the measure promoters, which only declared in front of the so-called traditional media and through a brief text published, in the form of a press release, in the AGADU website.

Similarly, the ability of network organization with a less hierarchical structure based on bonds of trust and teamwork resulted in quick decisions that were key in achieving objectives. Obviously, there is a generational factor that determines this big difference in the communication and organization forms and in this case favored the activists for the right to culture.

However, it would be a mistake to believe that the #noal218’s victory was achieved only in the social media. To begin with, there was a strategy that included the traditional media. These, which are used to always listen one voice, were surprised by the presence of a new social actor predisposed to break the hegemonic voice and patiently explain a concept like public domain, unfamiliar to the general opinion. The press coverage did not stand out for their accuracy or fairness. But at least, this made it clear that there was a conflict where the interests at stake were not only the ones of the chambers of commerce or rights management entities, but also the interests of independent artists, students, teachers and culture users in general.

Moreover, there was a determination for rapprochement with political representatives that largely explains the campaign's success. The government did not have an unequivocal position in favor of the extension of copyright terms, but it had responded to a specific demand from a sector, with no information that there were other sectors opposed to the measure. The interesting thing is that when activists requested meetings with government officials and made public their claim, those policy makers who had a position in favor of social sharing of knowledge were surprised. Several officials acknowledged feeling happy to find a new social partner, that would serve as a support to begin routes that before could not undertake due to lack of social support. Others, who did not have a definite position on the copyright issue, said they were grateful to receive a new view on the subject, other than the AGADU's and CUD's historical demands.

It should be noted that the political conditions in Uruguay for a movement like #noal218 are significantly more favorable than in other Latin American countries. Uruguay is not part of the Trans-Pacific Partnership. Therefore, the country does not currently suffer international pressures to tighten its Copyright Law. In this context, reversing the extension of the terms of protection does not imply any cost at international policy level. It is conceivable that the situation would be very different if Uruguay decides to join the Trans-Pacific Partnership or if the free trade agreement with the European Union prospers. For the free culture movement, these are potential threats to consider when thinking about the future.

As it was already mentioned, the extension of the term of copyright was defeated. However, the #noal218 movement did not take the victory as an end in itself, but as the beginning for a positive agenda on access to culture and copyright. The Uruguayan copyright law is extremely restrictive: it penalizes everyday socially accepted practices and it is in conflict with the right to education and access to culture. For that reason, from the new platform promotes a Copyright Law reform that recognizes the cultural practices associated with the use of new technologies, that do actually protect the authors, and that promotes a free culture. The Uruguayan government has committed to establish, within the next few months, the framework conducive to an institutional debate, with the largest number of voices represented. It is expected that the recommendations made in that forum pave the legislative route aimed at ensuring the right to culture.

The reform of collective management of music in Brazil

Eduardo Magrani,⁵⁹ Mariana Valente and Pedro Belchior⁶⁰

The Brazilian Senate approved a bill that seeks to reform the collective management system of copyright regarding music. After continuous protests by the civil society, the bill that establishes the need for greater transparency of the collective management national institution is now awaiting the sanction of the president.

Absolutely controversial topic in the area of copyrights, the collective management has generated discontent for decades on the behalf of authors, artists and users of musical works. In Brazil, the most pleased element is the Central Office of Collection and Distribution (ECAD, in Portuguese), the institution responsible for the collection and distribution of rights related to the public performance of music and also the holder of the legal monopoly to perform the activity.

Even though, on the last weeks, Brazil took a significant step towards the reform of collective management. Unanimously approved by the Commission of Constitution, Justice and Citizenship (CCJ) of the Senate, the report of the replacement of Senate Bill 129/2012 was followed by the approval of a request for urgency, which referred the Senate Bill (PLS) 129 directly to the plenary session of the Senate, which approved it by the end of the same day. The PLS was sent to the House of Representatives and there they took the same procedures. After being approved by the House with a single change regarding an exemption for churches, it now depends only on the sanction of the president.

But the story and the mobilization behind the PLS 129 are old. In the early 90s, when Brazil was chaired by Fernando Collor de Mello, the National Copyright Council (CNDA, in Portuguese), the agency then responsible for overseeing the ECAD, was deactivated. A few decades of legal monopoly without public oversight were sufficient to create a distorted and obscure system.

⁵⁹ Professor of Law and Technology and Intellectual Property at School of Law at Fundação Getúlio Vargas (FGV). Researcher at the Center for Technology and Society (CTS-FGV). Project leader on E-democracy and Internet of Things. Brazilian Coordinator of Creative Commons and the Digital Rights: Latin America and the Caribbean project.

⁶⁰ Mariana Valente and Pedro Belchior are researchers at the Center for Technology and Society (CTS) at Fundação Getúlio Vargas (FGV), in Rio de Janeiro.

Given the context created by the reckless management of ECAD, different Parliamentary Committees of Inquiry (CPI, in Portuguese) were introduced at national and regional scopes – one in the Senate (1995/96) and three in the Legislative Assemblies of Mato Grosso do Sul (2005), São Paulo (2009) and Rio de Janeiro (2011). On these investigations, crimes such as perjury, tax evasion, misappropriation, embezzlement, conspiracy, restraint of trade and abuse of economic power were appointed, but this did not lead to major consequences.

In 2011, a CPI was established in the Senate to reinvestigate the ECAD. Chaired by Senator Randolfe Rodrigues (PSOL/AP) and reported by Senator Lindbergh Farias (PT/RJ), the CPI rose diverse irregularities and crimes, among which the arbitrary expulsion of associations of ECAD's board, the unjustified replacement of the auditing service under contract, the payment of rewards to the employees for profit sharing, the distribution among ECAD's executives of values originally related to attorney's fees of the winning party, misappropriation of undistributed credits and cartel formation, among others.

The report, by showing irregularities and crimes, forced Brazilian artists and music users to take positions on the matter. As a result, the Senate designed the PLS 129/2012, in order to establish conditions to the exercise of powers conferred to ECAD by national legislation.

Months after its submission to the Senate, circumstantial changes brought the PLS 129 back on the agenda: the modification in the Ministry of Culture, with the new minister Marta Suplicy and the consequent return of the former director of Intellectual Property, Marcos Souza, allied with the new leadership to culture in the House of Representatives. Thus, articulated by GAP, a group formed by artists and other agents of the national music scene, the PLS 129 was referred to the Senate's Commission of Constitution, Justice and Citizenship (CCJ) and renovated by its rapporteur, Senator Humberto Costa (PT/CE), resuming the process that led to the approval of the PLS in Congress.

The final step to the project's approval was the articulation of the "Procure Saber" initiative, captained by other national artists of great renown. As a result, the PLS 129 was approved with urgency by both houses of the Congress, which ended with the approval of the bill in the plenary session of the Senate.

The renewed version of the PLS 129 kept some and altered other provisions of the previous project. The five elected fronts for the basis of the new version remained the same: Transparency, Efficiency, Modernization, Regulation, and Inspection. Changing the previous version, there is no provision of an autonomous law for the collective administration, but of modifications in the current Copyright Law, in order to prevent dispersion of legislative efforts. Another prediction of the replacement is to empower the Ministry of Culture to qualify and to supervise the associations related to ECAD. The previous version, due to political circumstances, gave the Ministry of Justice this task.

The new PLS 129 abandons the initial idea of dividing the activities of associations by categories of rights and predicts that associations thereafter have to prove their effective and regular management, foreseeing procedures that respect the right to contradiction and full defense in the case of penalties for poor management. ECAD itself becomes a target of clearer duties and obligations in order to ensure the transparency and the efficiency demanded by artists and users of musical works. For example, the new ECAD shall manage a single register of works, an old plea of members of the music segment, and it will be allowed to artists and users the constant and permanent monitoring of the data related to public execution of their works.

Other relevant issues concern: the fee related to the associations' administration, so that the rights holder receives at least 85% of the amounts collected; the limitation to the terms of the associations' main officers; and the equal right to vote, preventing power asymmetries among the associations.

Therefore, as the PLS 129 is approved in Congress, the next step is the presidential sanction. The pressure at this moment focuses on that. In parallel, it is expected that the president of the Republic considers the movement of artists and civil society and sanctions the law, but also takes the necessary measures for the (re)creation of an entity engaged in the supervision of the new ECAD's performance.

Thus, the approval of the PLS 129 in Congress represents a major step forward, but it is essential to mobilize and monitor the process and the presidential approval of the project with extreme attention to any veto and changes that may happen away from the eyes of those directly interested in reform.



Copyright in Argentina

*Beatriz Busaniche*⁶¹

At Digital Rights LAC, we wanted to ask different specialists in the region about their personal appraisals on digital rights issues. This is the case of Beatriz Busaniche from Argentina. We asked her about how the law has evolved with regard to copyright issues on the Internet in 2013.

The debate on copyright is open all over the world and Argentina is not an exception, even though the country's direction on public policy is difficult to predict.

To round up a year riddled with Human Rights related news and new technologies, it can be said that 2013 was a key moment for consolidating the discussion on copyright in the country, in circumstances where a project that would make public policy more flexible in this area is not just desirable, but possible.

The public debate on the topic is open, particularly because of a variety of judicialized cases that have sparked interest among the general public and the press. The “Taringa!” case is probably the most famous one, because of the attack of the book industry against one of the most popular Spanish-language sites, which could settle the unresolved situation on the scope of the responsibility of intermediaries in the infringement of copyright laws, committed by users.

The other key event of 2013 was the verdict in the case of Pampa Films against Youtube, which not only acquitted Google as an intermediary, but went on to establish an important principle enshrined in jurisprudential matters. It concluded that users who upload full movies onto video platforms do not commit a criminal offense because such behavior is not comparable to the crime of fraud, as stipulated by Copyright Law.

Organizations like Vía Libre Foundation have taken the initiative to open a sustained public debate on the need to design a public copyright policy that is faithful to constitutional principles, which is socially just and fulfills the aim of promoting art, science and culture, appropriately for intellectual property, also by furthering and respecting the human right of accessing and participating in cultural activities.

⁶¹ Beatriz Busaniche is a graduate of Social Communications at Universidad Nacional de Rosario (UNR). She works for the development of Free Software at Foundation Vía Libre.

Several debates and discussions with some of the key players of the country's cultural sector have led to the conclusion that the need to change the Copyright Law is undeniable. Even sectors with close ties to industry, along with representatives of collective management have recognized the need to modify and update the law in Argentina. The search for consensus among multiple stakeholders and the creation of superseding projects are still pending but could perfectly be set as goals for 2014.

Copyright in Brazil

Marcos Wachowicz⁶²

At Digital Rights LAC, we wanted to ask different specialists in the region about their personal appraisals on digital rights issues. This is the case of Marcos Wachowicz from Brazil. We asked him what the main achievements for 2013 were with regard to copyright and what could be expected for 2014.

The year 2013 marked the re-opening of the subject of reforming legislation currently in force in Brazil, with the new measures introduced by the Minister for Culture, Marta Suplicy. However, the year ended without the bill to reform Law 9.610/98 (Intellectual Property Law or LPI) being passed by Congress. This was foreseen by some parliamentarians and was expected by various sectors of Brazilian society.

The process of revising the country's LPI has been in the making for a long time, more than eight years. It all began in 2005 when, at the end of the First National Conference on Culture, it became clear that not only did the existing intellectual property laws need revising but also that the role of the State in this area needed to be redefined.

A number of governmental actions followed to stimulate debate in the country (eight seminars and more than 80 departmental meetings). On June 14th, 2010, the bill was presented to the public for a formal process of consultation through the Internet. For 79 days, any individual or institution in the country could send their contribution via an online platform which allowed immediate publicity for their suggestions. By the end, 8,431 individuals, legal entities and collective organisations had participated. During all this time,

⁶² Marcos Wachowicz has experience in Law, with emphasis on Intellectual Property Law, working mainly in the following subjects: computer law, intellectual property, copyright, Information Technology and software law.

the effort and the material collected promoted discussions that led to the maturing of ideas about the reform, increased clarity about the concepts, arguments and different points of view that surfaced during the process, and a more precise reading of how far the reform could go to get a balance between the public interest and the participation of the private sector.

So, in August 2013, with the enactment of Law 12.853, it was possible to proceed with one of the fundamental points of the reform, which refers particularly to the system of regulating the collection and distribution of copyright material by collective action organisations, through external supervision of their activities.

2014 began with a high expectation that the reform bill would soon be delivered to Congress. One of the points that had already caused controversy refers to the rules concerning the elimination of content protected by copyright which was possibly published unlawfully on the Internet, as well as questions about the limitations, uses and free access to intellectual property.

The fact is that in 2014 the timings of the legislative calendar will have to take into account two socio-political factors: FIFA's World Cup, which will take place in Brazil in the first half of the year, and the presidential elections which will take place in the second half. Both events will have an effect on the country's political agenda. Therefore, if the delivery is delayed, the outlook becomes uncertain regarding the space the government agenda will have to confront the debates in Congress.

The privatization of copyright enforcement: the Brazilian context

*Pedro Nicoletti Mizukami*⁶³

After years demanding stronger public sector response to copyright infringement, IP industries have now shifted to the strategy of forcing governments to assume the role of facilitators in agreements between private parties. In Brazil, this tendency is clearly noticeable in industry demands related to copyright enforcement in the digital environment

⁶³ Graduated in Law at Pontifícia Universidade Católica de São Paulo - PUC-SP (2002). Masters in Constitutional Law at the same institution (2007). PhD student in the Public Policies, Strategies and Development Program at Universidade Federal do Rio de Janeiro (UFRJ) Institute of Economics (PPED / IE). Member of the Technology and Society Center at Fundação Getúlio Vargas (FGV) Direito Rio.

within the National Council on Combating Piracy (CNCP – *Conselho Nacional de Combate à Pirataria*).

The CNCP: a brief history

The year of 2005 is a turning point in the history of copyright enforcement in Brazil. It was in 2005 that the Brazilian government finally gave in to the pressure exerted by the IP industries through the US government and definitively internalized the international IP enforcement agenda. That was the year when the National Council on Combating Piracy and Crimes against Intellectual Property (CNCP – *Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade Intelectual*) effectively became operational, with the mission to serve as public-private forum for the discussion of IP enforcement policy and coordination between industry and government. [1]

The events that led to the creation of the CNCP were documented in detail by the *Media Piracy in Emerging Economies* report, available in English, Spanish, Russian and Chinese. That story is reasonably long, but can be summarized as the result of years of pressure on Brazil promoted by the IP industries through the United States Trade Representative (USTR) and its Special 301 reports. The validity of the “pirate country” lists produced for Special 301 is extremely ambiguous in a post-WTO world. It is undeniable, nonetheless, that the lists had a fundamental role in the process that resulted in the creation of the CNCP in Brazil and in the drafting of a National Antipiracy Plan, currently in its fourth edition. Regardless of the fact that commercial sanctions can only be imposed after a WTO ruling and never unilaterally – strongly diluting Special 301’s power to intimidate – the lists continued to serve as fuel for effective pressure in Brazil halfway through the past decade.

While internationally Brazil defends a progressive IP agenda, and was an important actor in the debates that led to the approval of WIPO’s Development Agenda (2007) and the Marrakesh Treaty (2013), the domestic context is considerably more ambiguous. As an illustration, at the same time that Brazil was presenting a strongly argued defense of evidence-based policymaking, and demanding respect for Recommendation 45 of the Development Agenda at the 5th WIPO Advisory Committee on Enforcement, the CNCP was still widely publicizing three spurious numbers on the damages supposedly caused by piracy to the Brazilian economy. These numbers, we found in *Media Piracy in Emerging Economies*, had no clear source or methodology.

Contradictions like this are to be expected in complex political processes, such as those related to intellectual property. The existence of the CNCP, furthermore, gives Brazil the opportunity to criticize maximalist IP policies in international fora, backed by the argument that international standards on IP enforcement and industry demands are all being met domestically.

Nonetheless, the Ministry of Justice eventually demonstrated some sensibility to the academic debates on copyright and piracy and criticisms of antipiracy discourse. For the 2012-2014 mandate, the Ministry admitted as members of the Council the University of São Paulo's GPOAI and the Center for Technology and Society of FGV Law School. Both research centers maintain views on IP enforcement that clash with CNCP's traditional approach to the subject. ^[2]

As a councilor for CTS-FGV, I had the opportunity to directly confirm the analysis contained in *Media Piracy in Emerging Economies*. For example:

- The boundaries between what is public and what is private are sometimes blurry in a forum composed by both industry and government actors;
- The CNCP mainly operates towards strengthening the repressive measures of the National Antipiracy Plan, in detriment of the educational (antipiracy propaganda) and economic (business model-related) measures that are also part of its three-pronged approach to “combating piracy”. (Considering how industry awareness campaigns are, we are better off without the educational measures, but a conversation on business models would be a healthy step forward for the CNCP. Unfortunately, the industry councilors usually do not receive mandate to discuss this issue from their employers);
- The government usually shifts discussions on more important/sensitive themes to its Inter-ministerial Group on Intellectual Property (GIPI, Grupo Interministerial de Propriedade Intelectual) and other fora where the private sector has no direct participation; ^[3]
- The CNCP has been historically more concerned with counterfeiting, the informal economy and contraband, as opposed to piracy, in the definition established by note 14 to article 51 of TRIPS; ^[4]
- As a consequence, when it comes to online piracy, previous attempts to deal with the subject in the Council never really took off. This situation, however, could change.

Since the interplay of forces and interests within the Council is reasonably complex – industries as diverse as the film, beverages, pharmaceutical and tobacco industries are represented –, the priority of the CNCP has so

far been addressing concerns that are shared between as many different sectors as possible. In other words, the CNCP has prioritized repressive measures focused on the informal economy and clandestine cross-border flows of goods. For that reason, coordination between the Federal Highway Police, the Federal Police, Customs and agencies such as Brazilian Health Surveillance Agency (ANVISA, Agência Nacional de Vigilância Sanitária) has reached a considerable degree of maturity and the CNCP is working towards helping authorities at the state and local levels to achieve a similar level of organization. As concerns over physical goods piracy and counterfeiting diminish, it is inevitable that attention will finally shift to online piracy.

The CNCP and online piracy

Industry's first serious attempt to deal with the subject in the CNCP happened in 2008, when a graduated response/three strikes system was put under discussion. A working group was set up to carry forward a project called "Cooperation with ISPs". The goal was to have the CNCP act as mediator between content industries and ISPs, for the implementation of an entirely private system where ISPs would forward notices to users found sharing copyrighted material in p2p networks.

At a first moment, disconnecting users was proposed as a sanction after the third notification, but rapidly taken off the table in light of the backlash against Hadopi in France. The proposed measures included lowering bandwidth of suspected infringers or blocking p2p protocols. The idea was vetoed by the Ministry of Justice itself in September 2009, after an unfavorable opinion by its own Department of Consumer Protection and Defense (DPDC, Departamento de Proteção e Defesa do Consumidor), understandably concerned about negative impacts on users' privacy rights.

In August 2012, the working group was resurrected with another objective. Industry seemed to have given up on the idea of graduated response, and set the matter of p2p file sharing aside, to focus its demands on the creation of a notice-and-takedown system in Brazilian law. There were rumours at the time that the Marco Civil, a framework on Internet and digital rights, would be voted at the Chamber of Deputies (something that, as of this writing in February 2014, has not happened). Industry representatives claimed that in the absence of a notice-and-takedown system in Marco Civil, industry would be left "unprotected". The Copyright Reform Bill, which would include such a proposal, had not – and still has not – been introduced in Congress.

Since Marco Civil was gestated from within the Ministry of Justice and the bill had already been sent to Congress, it was evident at that point

that the discussion was closed. Nonetheless, this last minute attempt to desperately resurrect the subject, along with other recent developments, reveals a strong industry preference towards a “privatization of copyright enforcement” approach at CNCP, wrapped in a language that insists on “cooperation” instead of coercion.

“Cooperation”

The legislative process is usually slow and by its own nature more sensitive to the demands of a variety of actors, and to interests that are frequently contradictory. In issues related to online enforcement, industry representatives seem to currently favor strategies that either completely ignore the state or have the state act as a mediator of agreements between the different industry actors that will effectively enforce IP rights. Legislation, in this context, is of secondary importance and serves only to invest public authorities with the function of mediating the aforementioned agreements or to establish mechanisms of content removal that are then entirely maintained by private entities (such as, for example, notice-and-takedown systems).^[5]

It was following this reasoning that the working group that was created to import a graduated response system into Brazil had as its goal “a cooperation agreement with ISPs”, instead of legislation to the same effect. And it is following the same strategy that a recently proposed project at CNCP has the objective of having the government encourage cooperation agreements between IP rights holders and payment facilitators/systems (Visa, MasterCard, PayPal, etc.). The next targets for these agreements will be advertising networks. If this sounds a lot like SOPA, it’s because SOPA was the inspiration for the proposal, which has the strategic advantage of bypassing the legislative process.

With or without legislation – establishing general incentives for cooperation or specific mechanisms for content removal –, the future seems headed towards the complete privatization online copyright enforcement. Agreements between companies, best practices manuals, technical standards, and not legislation, will be the instruments that will determine the rules and the enforcement regimes for copyright infringement.

Much like in 2005, we are witnessing another turning point in Brazil. This time, to a scenario where the fora dedicated to IP enforcement policy are entirely private, discussions happen behind closed doors (sometimes mediated by public authorities) and the regimes produced leave users in conditions of

extreme vulnerability, and without a chance to be heard. Beyond the more substantive questions regarding the nature and legitimacy of such regimes, we face the challenge of finding means to help civil society react against unfair enforcement practices and of identifying actors within industry fora who might be able to defend public interest goals. Besides fighting for legislation to establish checks and balances in private enforcement regimes, we need to understand how to deal with the issue directly at the source.

- [1] Fora such as the CNCP are exactly what ACTA refers to in its article 28(3) and (4): “Article 28 [...] 3. Each Party shall, as appropriate, promote internal coordination among, and facilitate joint actions by, its competent authorities responsible for the enforcement of intellectual property rights. 4. Each Party shall endeavour to promote, where appropriate, the establishment and maintenance of formal or informal mechanisms, such as advisory groups, whereby its competent authorities may receive the views of right holders and other relevant stakeholders”.
- [2] Besides the two academic institutions mentioned above, the 2012-2014 composition of the CNCP is as follows: Representing the public sector: the Ministry of Justice, Ministry of Foreign Affairs, Ministry of Treasury, Federal Revenue Service, Ministry of Development, Industry and Foreign Commerce, Ministry of Culture, Ministry of Science, Technology and Innovation, Ministry of Labor and Employment, Federal Highway Police, Federal Police, Chamber of Deputies, National Senate, National Public Security Office.
Representing the IP industries: the Brazilian Association of Intellectual Property (ABPI, *Associação Brasileira da Propriedade Intelectual*), Interfarma (Association of the Pharmaceutical Industry and Research), National Forum on Combating Piracy (FNCP, *Fórum Nacional de Combate à Pirataria*), Instituto ETCO (representing the tobacco, beverages, fuel, and software sectors), and the Brazilian Video Union (UBV, *União Brasileira de Vídeo*).
Former members such as the Brazilian Association of Record Producers (ABPD, *Associação Brasileira de Produtores de Discos*), Brazilian Association of Software Companies (ABES, *Associação Brasileira das Empresas de Software*), and Motion Picture Association (MPA) are listed as collaborators and can participate in all meetings of the Council.
- [3] For more information on the GIPI: PORTO, Patrícia Carvalho da Rocha e BARBOSA, Dênis Borges. “O GIPI e a governança da propriedade intelectual no Brasil”. Radar IPEA n. 29, 2013, p. 19. Available at: http://www.ipea.gov.br/agencia/images/stories/PDFs/radar/131009_radar29.pdf
- [4] The conflation of piracy and counterfeiting in public discourse has been a hot topic in CNCP, which improperly uses the word “piracy” to describe a variety of offenses, including counterfeiting and circumstantially related but very different crimes such as contraband. Hiding behind what some in the Council classify as an “excessive concern for technical terms”, there are battles between the different industry members for attention and priority in the CNCP’s activities, as well as the strategic use of numbers and research results across completely unrelated industry sectors in the quest for stronger enforcement.
- [5] IIPA’s 2014 Special 301 submission provides many examples of this type of demand. The Mexican chapter suggests that the country should “enact legislation to create incentives for ISPs to cooperate with right holders to combat infringement taking place over their networks or platforms [...]” The Argentina chapter mentions the need to “develop processes that enhance cooperation between rights holders and online intermediaries in ways that are likely to contribute to a decline in online piracy”. The Brazil chapter argues that “active government involvement could help to bring ISPs and rights holders together to find effective means to deal with the most serious forms of online piracy, and to prevent its further growth”.
WIPO’s December 2013 Building Respect for IP newsletter included two examples of recent cooperation agreements between private entities: a Memorandum of Understanding, signed between the International AntiCounterfeiting Coalition (IACC) and Taobao Marketplace, and an agreement signed by Google, Yahoo!, Microsoft and other companies, supported by the Interactive Advertising Bureau, to establish “a set of best practices to address online infringement by reducing the flow of ad revenue to operators of sites engaged in significant piracy and counterfeiting”.



A discussion that could finally change copyright in Peru

*Miguel Morachimo*⁶⁴

In the last chapter of a long debate, the National Institute for the Defense of Competition and Protection of Intellectual Property suspended the board of the Peruvian Association of Authors and Composers for one year. But what hides within this long discussion in a country like Peru, which is advancing firmly in its economic and cultural development? A radical change, perhaps.

During October 2013, an investigative report managed to inform the public on how copyright is designed and enforced in Peru. Its revelations have prompted congressional hearings, a state decision to suspend the directors of a collecting society, the first designation, after ten years, of a new director for the Office of Copyright and up to thirteen bills that aim to modify the most controversial parts of the law. Does this represent a real change for copyright in Peru or is it just a temporary phenomenon?

Although the report by Marco Sifuentes and Jonathan Castro on the questionable operations of the Peruvian Association of Authors and Composers (APDAYC) was not the first to talk about the issue, it has been the main one that has attracted the most attention in recent years.

The facts that were questioned covered at one end, the various conflicts of interest that linked APDAYC managers with radios, record companies, producers and a small group of artists. This also exposed a level of deep social discontent regarding certain rules inscribed in our legislation which allow collecting societies to charge for the use of music in marriages, nonprofit activities and small businesses, such as hair salons or warehouses. Additionally, they would also include artists and works that are not even directly or indirectly part of their catalog.

Throughout several weeks, the number of reports that covered the bewilderment and reaction of artists, entrepreneurs, authorities and users towards the APDAYC, multiplied. In short time, and despite the attempts of its directors to justify their actions, the whole episode left an imprint among the Peruvian people, leaving them with the impression that something was certainly wrong with the APDAYC and that something needed to be done about it.

64 Miguel Morachimo is Hiperderecho's director.

The national authority in charge of supervising the collecting societies is the National Institute for the Defense of Competition and Intellectual Property (Indecopi). This administrative body was created during the nineties in order to specialize and decongest law enforcement on key trade issues such as intellectual property, competition and consumer protection, among other issues. Although Indecopi has the power to initiate cases on its own initiative and issue sanctions, their decisions can finally be checked in a court, which is quite common.

In recent years, the Copyright Office had accumulated several investigations and even sanctions against the APDAYC, but little has this done to make matters change. In early March, there was confirmation that the APDAYC was applying questionable rules for measuring popularity and distribution of royalties among its associates, which persuaded the Indecopi Copyright Commission to order the temporary suspension of the current directors of the company. In response, the APDAYC called the decision “unfair and illegal” and announced that they were willing to exhaust all possible means of defense and had already filed an appeal which has put the decision on hold.

In parallel, special hearings were held in Congress within the commissions of Culture, Supervision and Consumer Protection. As a result, there are currently thirteen bills pending that seek to change different parts of Legislative Decree 822, Copyright Law of Peru. Some of these bills propose changing specific rules on how collecting societies operate, stemming from the allegations in recent months against the APDAYC. Therefore, there is an intent to change the method of electing its governing board, banning re-elections, avoiding direct and indirect conflicts of interest and the obligation of having to convincingly demonstrate their legitimate representation of works that they charge for.

However, there are also proposals for even deeper reforms. Some proposals include new exceptions and limitations for domestic purposes, non-profit activities, libraries, small businesses and religious activities. Our Copyright Law, published in 1996, has been changed very few times and has almost always worked in favor of a more rigid and maximalist system. For the first time in eighteen years, there are many bills that seek to put the rights of users at the same level as those of the authors. Regardless of the outcome, the mere discussion of these issues is very necessary and welcome in a country that is moving forward in many cultural aspects and is eager to have better access to culture and knowledge.

The best thing that can happen after the APDAYC scandal is not the resignation of its officers or the dismantling of the collecting society.

Without overlooking the existing individual responsibilities, perhaps the best thing that could happen is that the APDAYC will serve us as an excuse for us, as a country, to confront and discuss a long pending issue. A state that seeks to build its cultural policy and to promote respect for intellectual property cannot afford to close its eyes to its own reality, which is summarized in little things like the fact that the largest center for retail sales of illegal copies in the whole country (Polvos Azules) is located just a few blocks away from the Supreme Court.

Peru needs to identify the current problems of the copyright system and discuss possible solutions. It is a debate that is rarely spoken in public about yet we often act as if we have a very clear understanding of it, in areas such as the secret negotiations of the Trans Pacific agreement (TPP) where Peru is merely sitting and waiting to assume obligations that weigh much more than any given law passed in Congress.

Intervening the APDAYC is necessary, just as it is for the authorities to be made responsible for ensuring that the laws are enforced. However, intervening the copyright system in Peru is urgent to put a stop to cases like that which involved the APDAYC, also for building a culture of compliance supported by clear and consistent rules and maintaining the balance between fair compensation for creators and defending the human right of access to culture and knowledge.

Copyright and access to culture in the digital environment

*Allan Rocha de Souza*⁶⁵

The fifteenth century houses important both social and technological transformations, which mark the emergence of a new modern era, with remarkable ruptures with the previous period. The creation of Universities and their independence towards Church, in the late Middle Ages, had already resulted on literacy increase and, as a result, also on a book demand, which led to the expansion of scribes' work field. The later invention of the printing, by Gutenberg, in 1436, and the paper, in 1440, allowed the reproduction of books in a scale infinitely superior in comparison with the known scale then.

⁶⁵ Professor and researcher in civil law, copyrights and intellectual property at the Law Undergraduate course, UFRRJ. Professor and researcher in copyright and cultural policies at the Postgraduate Program (stricto sensu) in Public Policies, Strategies and Development (PPED) at Institute of Economics, UFRJ.

The ease of reproduction, the literacy of a larger number of people and a more intense and diverse literary production lead to a period of cultural hatching – the Renaissance – and, concomitantly, to a cultural industry, in which stood out printers and sellers books.

This new economic opportunity, which enabled a commercial-scale reproduction and distribution of books, led to the emergence of the first invention privileges, granted, exclusively, to the Venetian Republic editors. The privileges granted by the Crown to the booksellers are the first specific legal setting for the protection of the rights of creation, thus protecting them from the competition of others, guaranteeing them a monopoly and ensuring the development and sustenance of local editors, with positive consequences for the Kingdom, grantor of the privilege. Another very relevant factor that drove the granting of privileges is its political function, which main objective was to control what was published and read, setting a limitation – a censorship – to the content that was produced and put into circulation.

The changes brought by the printing press and movable types, paper, literacy and the possibilities that were created can be compared to the changes that occurred due to the replacement of analogue by digital technology, from the 1980s. But there are some differences that help to contextualize the challenges posed to the regulation of copyright in our time.

The main thing is that, then, the emergence of support for the creations whose reproduction and distribution were economically viable enabled the organization of a cultural industry that was sustained by the control of the production and circulation of the media, where literary creations were inserted. On the other hand, the revolution of digital technologies of communication and information leads to the dematerialization of the support, dissipating, as a result, the control in which the cultural industry has sustained for five centuries.

As in other times, the new context created an industry's demand for an upgrade on the legislation that regulates the cultural market, in order to ensure the continuity of the legal control on the sector's economic flows, in an environment in which the physical support is no longer necessary. This regulatory review, as at other times in the history of technological diffusion, aimed to expand the scope of protection with the expansion of its object, gradual extension of deadlines, reduction of limitations.

In the international scenery, these changes are symbolized by the TRIPS Agreement, OMC, and the "Copyright Treaty" and the "Performances and Phonogram Treaty", OMPI. Nationally, this attempt to ensure the continuity

of the control of production, reproduction, circulation and use of creations conformed the Law number 9.610 from 1998.

The elaboration of the legal text, normative, is only a first step in the process of consolidating the social norm, which is still undergoing though a dispute about their meaning, scope, effectiveness and, mainly, efficiency in the social shaping of desired behaviors. But, this time, the established cultural industry had not counted on the complacency of society that, in many ways, remains resisting the implementation of legislative commands.

The acceptance of these exclusive rights and their scope had never been peaceful, but the social opposition had never reached the current level. What has changed in our time that allowed a massive and widespread resistance to the normative political structure negotiated by industry? To answer this question is the challenge that is put to all researchers, professionals and activists. But, because of its complexity and implications, the question can only be faced satisfactorily in a collective way, so what follows is a brief illustration of a hypothesis, an explanation of the possible reasons and justification of social resistance to digital control.

The penetrability of technology, the network communication – by all and for all –, the ease and cheapness of reproduction and dissemination of works object of protection, together with the new possibilities of creation and use allowed the social and cultural ownership of these assets, regardless of the desire of industry and beyond their ability to control.

The dematerialization of support and digitization of works resulted in a wide availability and access to previously unthought cultural content, in direct conflict with the normative text built by and for the consolidated industry. Attempts to perpetuate control are unsatisfactory and, little by little, fail.

At the same time, we witnessed, from the last years of the last century, the revival of a range of sleeping rights, the cultural rights, in particular the right of access to culture. Predicted in the Human Rights Declaration of 1948 and the Covenants on Civil and Political Rights and on Economic, Social and Cultural Rights of 1966, besides the Inter-American Human Rights Convention, remained inert for decades, without radiate its effects on goods of cultural nature protected by copyright. The perception and social resistance to entrapment of these goods arise from materialization of access, made possible by mass digitization and availability of works, shaping and consolidating the demand for the realization of a right previously not widely envisioned.

Rights do not grow on trees, they are constructions derived from social demands that find their political paths in the legislative process or in judicial recognition, but whose delivery always depends on the substantial voluntary acceptance of its command by groups and individuals to whom they are intended.

The political and economic power was enough to build a new international legal framework and also develop national standards intended to perpetuate the control achieved over the physical media in a new technological context.

However, the new forms of production, reproduction, dissemination and use of creations, that were made possible in this new context, enabled the empowering of citizens, seen, then, only as recipients of cultural goods, which started to demand the realization of the right of access to culture, opposing the wishes of industry.

We are, today, witnessing a situation where, contradictorily, formal prohibition coexists with large material access, in a clear scenario of social delegitimation of the legal text. The composition of these divergent demands with a large emerging picture of emerging rights is the challenge that arises for two decades.

Open educational resources

Eduardo Magrani⁶⁶ and Pedro Belchior⁶⁷

Besides the practicality it could bring to the authors, free licensing can also contribute to promote the most important constitutional rights in the scope of cultural production: the access to culture and the access to knowledge.

Open Educational Resources (OER) were mentioned for the first time in 2002, in a UNESCO conference. Participants at that forum defined the OER as a vast provision of educational resources, enabled by information and communication technologies, for consultation, use and adaptation, facilitated by free licensing.

⁶⁶ Professor of Law and Technology and Intellectual Property at School of Law at Fundação Getúlio Vargas (FGV). Researcher at the Center for Technology and Society (CTS-FGV). Project leader on E-democracy and Internet of Things. Brazilian Coordinator of Creative Commons and the Digital Rights: Latin America and the Caribbean project.

⁶⁷ Researcher at the Center for Technology and Society (CTS) at Fundação Getúlio Vargas (FGV), in Rio de Janeiro.

Given the limitation of copyright protection, the transaction costs needed for the legal distribution of works are normally too high, creating obstacles to the practice and leaving both the author and the user in a situation of juridical instability, since it isn't clear how the available works could be legally used. Regarded as a possible way to solve this problem, free licenses, that are nothing more than standard use licenses, could specify which forms of utilization are allowed.

Open Educational Resources are theoretically digitalized materials offered freely and openly to educators, students and self-learners, so that they can be used and reused in learning, teaching and research activities. OER are easily found on the Internet and can be accessed by teachers, educational institutions and students. Their main function is to contribute to the renovation and amplification of the educational systems worldwide. Under this perspective, Creative Commons performs a key role in the consolidation of OER as CC licenses are one of the most efficient and useful means to assure a wider availability of courseware related to the Open Educational Resources.

Currently, there are several initiatives focused on the promotion of OER. In the United States, a program launched by the North American Ministries, dedicated to higher education, offers a fund of 2 billion dollars to teaching institutions in order to develop technical courses. The material produced by this program in its four years length is entirely licensed in CC-BY. Another important initiative to OER's trajectory is the one made by the Massachusetts Institute of Technology (MIT), which has allowed the virtual divulgation of all MIT's digital contents known as MIT OpenCourseWare (MIT-OPW); its goal was to make all the material used in most graduation and post-graduation courses available to online consultation. MIT's served as an example to the Universities of Princeton, Stanford and Harvard, which have posteriorly followed the Institute's pioneer achievement.

In Brazil, a growing community takes interest for OER. Since 2008, the OER-Brazil project facilitates discussion, provides training, work on community building and awareness and work with policy makers to addresses and develop policy and legal instruments to foster OER in Brazil. One of the victories was the inclusion of OER within the goals of the National Plan of Education, among others. But a bigger victory we see in the country is the social engagement in the debate through social media and more. This community is internationally recognized and receives support from UNESCO, Creative Commons, among other organizations. To support the

community and knowledge in the area, the OER-Brazil project publishes a series of resources, including a very comprehensive FAQ, currently under translation for English and Spanish by OAS.

Still concerning Brazilian panorama, the Secretary of Education of the City of São Paulo announced in 2011 that all the material produced to the municipal schools would be available to download, meeting demands which are both internal and related to other municipalities. The initiative has been guaranteeing the free use of São Paulo's educational programs by schools all over Brazil, adapting them to the local realities without any eventual cost generated by licensing.

Moreover, as essential developments of the global awareness concerning the major importance of OER in the governmental scope driven by UNESCO's 2012 Paris OER Declaration, a couple of Brazilian legislative proposals should be mentioned. Bill n. 1513/2011, authored by congressman Paulo Teixeira (PT), has the aim of freely licensing all works subsidized by public entities and private entities under the control of public shareholders. More recently, the House of Representatives of the State of São Paulo approved the entire Bill 989/2011, which consolidated the policy of availability of Educational Resources bought or developed by direct or indirect public subvention. Nevertheless, the governor of the State of São Paulo, Geraldo Alckmin, interposed the Bill. According to him, the project suffered from "a birth vice" since only the executive could regulate the use of computers and Internet in its own activities. This statement is controversial and highly doubtful, besides representing a real setback in the promotion of OER.

It is certain that a higher degree of promotion of OER shall be sought. The need of massive dissemination of knowledge and culture cannot be only one topic in an agenda whose projects seem to be far from concretion. Besides the practicality it could bring to the authors, free licensing can contribute greatly to promote the most important constitutional rights in the scope of cultural production: the access to culture and the access to knowledge. Thus, free licensing allows society to have more access to information and knowledge, generating a significant growth in the production of these goods. In this context, the creation of an infrastructure which could support such responsibility makes itself necessary and the OER represent a huge step in that direction.

Exceptions and limitations to copyright for libraries and archives in Colombia: update & upgrade more than necessary

Luisa Fernanda Guzmán Mejía⁶⁸

As part of the sagas of laws that seek to modify the copyright system in Colombia, ignoring the need to fully review and update the exceptions and limitations, it is premiering in Congress the Law Proposal 306 of 2013 (Ley Lleras 4). Libraries, archives and civil society will present their concrete proposals on round tables. What will happen?

On May 15th, the Minister of Commerce, Industry and Tourism and the Minister of the Interior of Colombia filed in the House of Representatives the law Proposal 306 of 2013 – known by netizens as Lleras Law 4 –, in a new attempt to implement some of Colombia commitments on intellectual property under the Free Trade Agreement with the United States after the Constitutional Court declared unconstitutional the law proposal 1520 of 2012 (Lleras Law 2) due to procedural defects in January.

Despite the comments made at the time by civil society, the new project is virtually identical to the Lleras Law 2. Additionally, it suffers from the same faults: rises the protection of copyrights without introducing appropriate mechanisms to balance the system, which could be achieved by revising and updating existing exceptions and limitations that are already outdated in the face of new realities 2.0.

Unlike previous episodes in the saga of laws and in response to a request by the collective RedPaTodos, this time the Colombian government has committed itself to discuss the Law Proposal 306 with civil society. As a result, round tables will be organized shortly. Libraries and archives, committed to their important role of providing access to culture, education and information, will submit a proposal on exceptions and limitations to copyright, enabling them to fulfill their aims with full legal certainty in these new technological contexts.

Panorama of copyright, libraries and archives in Colombia...

The only exception and limitation available to libraries and archives in the Colombian legal framework on copyright is the reproduction of a work for preservation intentions. Article 38 of Law 23 of 1982 provides

⁶⁸ Luisa Fernanda Guzmán Mejía is a member of the Karisma Foundation.

this possibility only to public libraries and when required for conservation purposes; on the other hand, the Andean Decision 351 of the Andean Community of Nations, in its Article 22, enables libraries and archives to reproduce original works in the event of loss, destruction or irreparable damage without profit-making purposes. This decision, whose character is preeminent or of preferential application over domestic law, establishes an exception and limitation much broader than Law 23, since it is not restricted only to public libraries and it includes also archives.

In this regards, the National Copyright Office (hereinafter DNDA, in Spanish) has ratified that under the Decision 351 the protection for libraries and archives is not possible for different use than reproduction, as for example the distribution of copies (Concept 2-2006-9790 of September 29, 2006). This is a legal obstacle for lending of copies by libraries and archives. In turn, it prevents the acquisition of works in other countries as both the lending and the import are forms of exclusive distribution right, according to Article 3 of Decision 351, and, therefore, require the express prior authorization of right-holders.

This authorization is necessary because Colombia has not exercised the power established on 1996 WIPO Copyright Treaty to determine the conditions under which the distribution right is exhausted. That is, even though the first sale of a work's copy has been made in the country, the authors or right-holder retain the prerogative to control how the work is still being distributed. In Colombia, the distribution right is not exhausted (DNDA Concept 2-2005-6647 of July 14th, 2005).

The Law 1379 of 2010 established that, due to its educational nature, libraries are not required to seek right-holder authorization when lending books and materials, and making them available to their users, "in cases expressly falling by the rules governing the limitations and exceptions to copyright and related rights". Paradoxically, this provision does not allow public lending without the required authorization, because as it was evidenced before, there is no express limitation and exception on distribution right. In turn, the law only applies to the National Network of Public Libraries, which articulates and integrates state public libraries and their services in the various territorial units.

If in the world of atoms rains, it pours in the digital...

The above scenario shows how the copyright rules restrict library and archive activities in Colombia. However, the situation could be more daunting. The new Law Proposal 306 provides that, regardless of a subsequent infringement of copyright or related rights, whoever circumvents without authorization

effective technological protection measure (TPM), laid down to control access to or unauthorized use of work, shall incur civil liability and shall indemnify damages. While this proposal provides an exception on access to a work by non-profit libraries, archives or educational institutions, which would not have access otherwise, for the sole purpose of making acquisition decisions, this is clearly insufficient. The protection to these measures prevents circumvention for lawful acts under the existing limitations and exceptions as reproduction for preservation, and it could also affect the access to and use of works that are in public domain and that incorporated these measures at some time. Additionally, it would not be allowed to disable such measures to facilitate access to works by persons with disabilities, necessary for the functioning of e-Braille and text-to-speech devices.

Meanwhile at WIPO...

Since 2010, treaty proposals on limitations and exceptions for libraries and archives are been prepared at WIPO, which include the possibility of parallel imports, lending services to users and others libraries, making copies in accessible formats for use by disabled persons, the use of orphan works, obligations concerning TPM, among others. The WIPO Standing Committee on Copyright and Related Rights, in its meeting to be held from July 29th to August 2nd, will resume the dialogue on this important subject, suspended while the newly approved “Marrakesh Treaty to Facilitate Access to Published Works for Persons who are Blind, Visually Impaired, or otherwise Print Disabled” was adopted.

Colombia signed the treaty on June 20th, pending the ratification process before Congress and subsequent internal implementation. Of this will depend that libraries and archives can convert works into accessible formats and, ultimately, facilitate access to education, culture and information to people with disabilities.

Copyright in Chile

*Francisco Vera*⁶⁹

At Digital Rights LAC, we wanted to ask different specialists in the region about their personal appraisals on digital rights issues. This is the case of Francisco Vera from Chile. We asked him: what is the most critical aspect of the TPP concerning intellectual property for countries in our region?

⁶⁹ Francisco Vera is Derechos Digitales' public policy director.

The greatest threat to Human Rights in Chile's digital environment is not posed by a lawsuit or bill but by a free trade agreement known as the TPP (Trans-Pacific Partnership). Negotiations for this agreement are being secretly conducted among 12 countries from the Asian Pacific and most of the information available about these negotiations was leaked by some of its chapters.

This agreement poses a threat against both Chile as well as Latin America because it exceeds the scope of what is traditionally viewed as free trade, comprising sensitive regulations concerning intellectual property and continuing down the path of failed bills such as SOPA and PIPA, which posed serious violations of the human right to expression and information, privacy, access to information and due process under the pretext of regulating certain aspects of the Internet and protecting copyright.

What is currently being negotiated in the TPP is the surrender of several tools for controlling the Internet to rights holders, in detriment of the general public, opening the door to mechanisms for removing content without a judicial order and implementing systems for disconnecting infringing users, thus forcing Internet service providers to control and monitor our online activity.

Countries that are under immediate threat are Chile, Peru and Mexico; however, the risk extends to the rest of the region as well since shady and untransparent de facto norms are being imposed on an international level. It is believed the TPP will be signed by mid 2014, which is why today, more than ever, we must demand an open and transparent TPP. For more information visit tpabierto.net.

Copyright in Colombia

*Carolina Botero*⁷⁰

At Digital Rights LAC, we wanted to ask different specialists in the region about their personal appraisals on digital rights issues. This is the case of Carolina Botero from Colombia. We asked her what the main achievements were regarding the "exceptions and limitations to copyright" and what direction these discussions took in 2013.

⁷⁰ Lawyer, blogger, lecturer and researcher. Creative Commons colider in Colombia and a member of Fundación Karisma.

Bearing in mind that Colombia is anticipating a copyright reform, essentially to fulfill the commitments of the FTA with the USA (i.e., commercial interests of the holders), 2013 was, however, an interesting year for the “positive agenda” that the country’s Karisma Foundation is pushing, which has exceptions at its central axis, which are understood as guarantees of fundamental rights and not as favors for the holders.

Last year began with a bill of five new exceptions to the Colombian legal system. The project had good intentions but did not meet the needs of the beneficiary communities and ended up being removed.

Half way through the year, during a series of workshops organized by the Ministry of Commerce to advance the FTA, the government received several civil society proposals to strengthen the exceptions. The proposals are currently still being studied.

During 2013, Law 1680, an initiative by Senator Juan Manuel Galán, was also approved, which seeks to provide access to knowledge for the blind and visually challenged, through the use of Information Technology and Communications (ICT). This law includes an exception to enforce this fundamental right and, although it does not have the scope of the Treaty of Marrakesh, it is seen as a step towards in the right direction.

The Treaty of Marrakesh is a historical document that, for the first time, recognizes minimum standards for the exercise of fundamental rights in the copyright system. As one of the first countries to subscribe to the treaty, Colombia now has the important task of implementing it.

These discussions, which have provided visibility to the exceptions and their legal functions, are central to pushing the aforementioned positive agenda.

PART
6

ACTIVISM



Activism and the Internet

*Miguel Lago*⁷¹

“What you promote is couch-activism”. This is a phrase that everyone who has used the Internet as a platform for civic mobilization has heard. The logic of it is interesting and, at first glance, it seems to make sense. A click on its own does not reflect or suggest a great deal of engagement in a cause. After all, if a cause matters, we will do much more for it than a click right? Yes, if the material conditions the world provided for each citizen were perfect. Yes, if the citizen didn’t need to work or pay bills. The degree of direct participation that went into democratic decisions in Athens was only possible because of slavery and the fact that Athenian citizens did not need to work. There was no scarcity of time. So, how to open more fronts for participation in and democratize modern societies, or go beyond voting, in the current job market which makes “free time” a scarcity? The Internet may be the solution for this problem.

The existing criticism towards couch-activism, which undervalues the “online” mobilizations, tends to come from a few intellectuals and activists, who can make the time to engage themselves, because of the reality of their work schedule, where it be professionally (working in NGOs, in academia) or in correlation with their profession. Thus it is possible to participate in assemblies, meetings, engage in more long-term, continuous ways, in issues that really take more time to be addressed. Unfortunately, this is not the reality of most workers, who, in Brazil, must comply with their mandatory 44-hour weeks, as well as the average displacement time from home to work in metropolitan areas, of on average 1 hour. This represents at least 50 hours dedicated solely to your work. As such, discussing full involvement is all well and good, but not everyone can go out to the streets in the afternoon, or fit in an amphitheater where a forum is being held, because unfortunately people have to work. And while people are working there will always be a group of select few who participate in political life.

In this context, the great advantage of digital activism is that it breaks such space and time barriers. You can participate at any given time, at

71 NGO Meu Rio’s coordinator.

the level of engagement that your time and workload allow for. You can participate from home, from work, from the bus. And if you only have 5 minutes a day to participate, the Internet allows you to do so. Online activism is the only way to assure the democratic inclusion of the majority of the working population in political participation. It is the only means, in the current social arrangement, to assure that the maximum amount of people participate.

In Brazil's case, it is clear that online activism, even though it can be inclusive, is also exclusive, as a great deal of the population does not yet have access to the Internet. But this is an increasingly declining trend. And it's better to have a declining trend than the permanent exclusion that time and space generate.

But access to the Internet is not enough to include people. It is essential to make good use of the Internet. In fact, complaints which don't channel demands, or voice causes, do not generate change. Networks for mobilization such as Avaaz, Change, All Out and Meu Rio are able to help people articulate their demands, connect them to decision makers to whom these must be voiced, and create a solidary community to deal with several causes. It is up to these networks to try different experiments and interfaces of calibrated participation in order to configure the right level of engagement that each worker can handle.

And it works. In just 2 years, Meu Rio Network allowed locals to alter the State's constitution, prevent the appointment of candidates with civil or criminal condemnations for direct or indirect Public Administration positions, prevent a flexibilization of environmental legislation, enable the creation of a police precinct specialized in disappearances and avoid the demolition of the 10th largest school in the country. In 2 years, more than 30 public policy changes were made in the city.

Online activism is what gives Brazil a chance to continually and consistently democratize political disputes, which, for a long time, remained in the hands of forerunners and elites. The "we are few, but we are strong" must and shall be replaced by "we are many, and we are transformers".

Right to protest and policing in social networks

Francisco Vera⁷² and Paz Peña⁷³

Today, activists and police from around the region are faced with a new battleground: the social networks. While for some it is the most effective way of being organized, for others it is fertile ground for surveillance.

At the time of writing, somewhere in a city of Brazil, one of the most highly anticipated matches of the FIFA World Cup 2014 is being played. While fans indulge in frenzied celebrations, it is almost certain that the Brazilian police are watching over certain social network users from that country. Why? To “prevent” any likely disturbances throughout the event that could possibly arise from any of the protests that have been announced.

Why did the police decide to monitor social networks? Mainly because, whether we like it or not, they are not only the most popular platforms on the Internet, but they are often the only means that the public have for communicating with one another. Thus, over time, they have become platforms for promoting various forms of Human Rights, such as petitions, gatherings, associations and freedom of expression.

With the student protests of 2011 (which are still occurring today), the use of social networks in the organizing of the students in Chile was paradigmatic for the exercise of Human Rights on the net. So much so, that you cannot analyze these mobilizations without taking into account these platforms, along with the positive and negative consequences for the student movement.

It was only a matter of time before the police surveillance mechanisms would reach the use of social networks, especially in countries like our own, where “democracies” that suffer the many ills of post authoritarianism are still abound. Surveillance practices that do not conform to law, should not be permitted, for being arbitrary actions that seek to punish the exercise of fundamental rights and intimidate different activists.

The monitoring social media has several modalities. The first and simplest is to identify the event, organizers or Facebook groups, which given the social nature of this social network and its policies that aim towards the use of real names, make matters easy for the work of the police and intelligence, without requiring any special skills.

⁷² Francisco Vera is Derechos Digitales’ public policy director.

⁷³ Paz Peña is Derechos Digitales’ advocacy director.

Another method is to demand companies like Facebook or Twitter, through court or government orders (the latter is considered dubiously legal), to hand over the private information of its users, allowing police and intelligence services to identify people who exercise their right to anonymity through pseudonyms or false names.

But there is also a third, and more worrying, category which involves the use of specific technologies that can be offered by the social networks themselves, to facilitate the identification of suspects. This is the case, for example, with the use of facial recognition systems, although today it is not possible to extend their use within law enforcement and security agencies. A case in Chile, however, has caught our attention as it raises the alarm on their potential uses.

During one particular protest, which occurred only a few weeks ago, a Chilean policeman was brutally beaten and attacked by a group of hooded rioters, an incident which was unanimously condemned by all sectors. A witness managed to record some footage of the incident and, based on those images, the Chilean prosecution claims to have carried out “facial recognition which has led to pictures of someone that it resembles”, resulting in the arrest of a student who was allegedly involved in the events.

The above phrase evokes the use of social networks and technologies. Fortunately, for now, Facebook does not allow random face searches for any given photograph, unless it is on your list of friends or friends of your friends, and is far from being an accurate process, which means that the procedure itself had very little technology behind it.

What probably happened in the case described was that the so called “facial recognition” only consisted of comparing video images with Facebook pictures by eye. But, if in Chile alone there are millions of users of this social network, where did the police start their search? Other background information, additionally suggests that the suspect had had not even attended the march, so now all the research procedure is being questioned.

In this new stage of social media monitoring and prosecution of social protests, there are different ways to address the problem. It's easy to take a technologically determinist approach and trust that the only solution is to convince and train the participants to use safe tools for communication (TOR, encrypted emails, etc.). However, adopting these tools, which can actually help a lot of activists, does not necessarily solve the underlying problem.

The problem with this approach is that it ignores that both security and privacy are not defined by the use of a tool, but by cultural patterns.

Saying that “Facebook is evil” to other members of social movements, who through this platform have succeeded in exercising many of their rights, is not the best way of trying to understand the complexities behind the use of technology and ignores the networking potential of a platform that consists of so many users. The ways of approaching the privacy and security of our data depends on variables such as age, gender, social class and so on. One way of working with activists at risk, due to the monitoring of social networks, could start with understanding and assuming these conditions.

Bearing all of this in mind, we must not forget the main perspective: the political dimension. Prosecution agencies in countries like Chile and others in the region, do not adequately respect our fundamental rights. They often operate in a sloppy or abusive manner, without a warrant authorizing them to do what they do. Such abuses, within the digital environment, pose a threat to millions of people who can be prosecuted for numerous reasons that have little to do with the prosecution of a crime, but more so to undermine, prevent or restrict the exercise of several fundamental rights.

In this scenario, it is essential to have policies that limit the excessive and disproportionate collection of data by social networks and, at the same time, prevent the police and security forces from having free and indiscriminate access to this information. This is the only way that we can effectively protect the fundamental rights of users from these services, allowing them to exercise their rights through the platforms which they consider most effective to achieve the social changes that many people crave.

Internet and democracy: the protests of June in Brazil

Eduardo Magrani⁷⁴ and Mariana Valente⁷⁵

In the protests of June, online information was a key factor to the change of position of the traditional media, the great public and the political system. As already indicated, the tipping point that made the masses take the streets was the complaints, through social networks, regarding gratuitous police violence against protesters.

⁷⁴ Professor of Law and Technology and Intellectual Property at School of Law at Fundação Getúlio Vargas (FGV). Researcher at the Center for Technology and Society (CTS-FGV). Project leader on E-democracy and Internet of Things. Brazilian Coordinator of Creative Commons and the Digital Rights: Latin America and the Caribbean project.

⁷⁵ Marina Valente is a professor and researcher at the Center for Technology and Society (CTS) at Fundação Getúlio Vargas (FGV), in Rio de Janeiro.

The so called *protests of June* in Brazil had an incubation phase that dates back to August 2012. That was when the mayor of Natal city, in the northeast of Brazil, announced a raise of R\$ 0,20 for the bus fare and, against such raise, approximately 2 thousand people went to the streets, resulting in its revocation. This episode was marked by media attention and police repression, launching the basis of the protests to happen in the first semester of 2013, which became very intense in June, headed then by the Free Fare Movement (“Movimento Passe Livre” or MPL, in Portuguese).^[1]

The MPL organized a series of marches in different Brazilian regions, starting in the city of São Paulo, motivated by an increase, made on June 2nd, in the urban transport fare (subway, bus and urban trains), from R\$ 3,00 to R\$ 3,20. The three first protests happened on June 6th, 7th and 11th, and were repressed with police violence, resulting in wounded people at both sides – protesters and policemen. The traditional media did not hesitate to adopt a clear anti-protests view: the words “vandals”, “rioters” and “vandalism” were constantly repeated. A big newspaper from São Paulo published, at this moment, an editorial calling for more police repression.

The great shift in the public opinion began on June 13th, when the riot police of the Military Police of São Paulo violently repressed part of the already thousands of protesters and journalists, at times in answer to acts of aggression, at other times without previous aggression. It was on the Internet that information started to pop up: it was enough to be online to become aware of police brutality, therefore bringing to light the distance between the traditional media version of the facts and that of the protesters, who were then organizing themselves around independent media groups on the Internet.^[2]

It was on the following days that the protests gained massive adhesion all over the country^[3] and the demands were widely diversified. From this moment on, the traditional media would report the protests with an enthusiastic encouraging speech, repeating emphatically the word “peaceful”.

The newspapers and opinion makers would try to explain what the protesters wanted. One thing was sure: the protests were not anymore limited to the raise of transport fares. Various monitors of online activity emerged, each of them offering their graphical analysis. The CausaBrasil platform monitored the activity on social networks in that period (from June 16th on),^[4] indicating the prominence, in the month of June, of the following demands: (i) fare price, with declining importance through the month, (ii) Dilma Rousseff’s government, a growing agenda through the month, (iii) political reform, (iv) PEC 37,^[5] highlighted on June 26th, (v) democracy, a demand that remained stable through the monitored period.^[6] On top of those demands, it can be

pointed as structural factors of the period, a feeling of distrust in the traditional representative system and on political parties organizations, as well as a desire for new ways of political participation and the broadening of the democratic sphere, combined with a dissatisfaction with the insufficiency and partiality of traditional media coverage.

By the end of June, the pace of the protests decreased. President Dilma Rousseff made a statement on national television on June 21st, trying to make a stand against the demands that still appeared to be incomprehensible. The messages were: to press the Congress to approve a proposal from the Executive, which had already been rejected, aiming to direct resources from Pre-Salt Layer oilprospection for education, and the establishment of an exclusive constituent power for political reform. The following days were taken by the discussion by constitutional experts about the adequacy of such a reform, which ended up not taking place.^[7] On the other hand, the appeal for the destination of the oil royalties was partially agreed upon by the Brazilian Congress.^[8] But the main achievements brought by the protests concerned the initial demands, present in the social agenda since the movement was still headed by the MPL: urban mobility and transport. In more than 100 cities throughout the country, bus fares were reduced.^[9]

Brazil then entered the list of countries that, since 2011, have been the stage of broad protests, organized through the Internet, as well as discussed and publicized on online platforms. However, seeking similarities between the Brazilian protests and those around the world is fruitless: Brazil is going through a very unique moment, from economic, social, institutional and political standpoints. But something that definitively connects all these protests is the role of new technologies in the articulation of social movements, protests and manifestations, and especially the effective potential of those technologies in regards to the ends of social transformation and political impact.

Internet and information: social networks and alternative media

No one would question that the Internet was the main tool for spreading information about the protests. A research made on June 20th in Rio de Janeiro revealed that 91% of the respondents got information about the street marches through social networks.^[10] Facebook, particularly, served both to organize and publicize the protests. It was common that a single event page for each city would be created, a page that would be updated for every new protest. Alternative pages regarding the same protest would also appear, each with its own internal discussion. As such, more than a platform for mobilization, Facebook was, during that period, a space for broad debate, with potential for confrontation and development of discourses.

In the protests of June, online information was a key factor to the shift of position of the traditional media, the mass public and the political system. As already indicated, the tipping point that made the masses take the streets was the denouncing, in the social networks, of police brutality against protesters.

To organize the flux of photos and videos uploaded on the networks, some personal profiles and mainly alternative media groups stood out. The most prominent of those groups was *Mídia NINJA*. A free acronym to *Narrativas Independentes, Jornalismo e Ação* (Free Narratives, Journalism and Action, in Portuguese), the group was created in 2011 by people already involved with networked initiatives (from a collective called *Fora do Eixo*). Gathering together texts, photos and videos of collaborators that participated in the protests, connecting with each other mainly through their cell phones and diffusing the material via Twitter and Facebook, *Mídia NINJA* drew attention of Internet users and had their contents reproduced by traditional media. During the protests, *NINJA*'s live streaming was watched as if it were a TV show, and showed people's perspectives in real time, crudely and without any edition, as an alternative to those of journalists that recorded the events from helicopters, far from the heat of the moment.^{[11] [12]}

Mídia NINJA adopted an activist profile, connected to social demands, focusing on police brutality, and such was the reception and adhesion to the model (today there are more than 200 thousand followers on its Facebook page) and even its critics (the group's leaders were hardly questioned in an important national political television show, *Roda Viva*) that one can only agree with the existence of a latent demand for alternative information in Brazil, in a less hierarchical and more decentralized format. The two-way street between informant and informer was also seen in the relations between traditional and alternative media, since the messages of the former were decoded, mainly in a critical manner, by the alternative media, which also gave subsidies to traditional media information.^[13]

Potential and blockades

The Internet capacity to serve as a box of resonance of citizens' demands and opinions could be seen on all its potential during the social manifestations of June. Maybe like never before, the protests imposed themselves as an almost unique subject, what is impressive for a decentralized space, and the political specters of the discussion varied between extremes. However, it was also clear that, as debates previous to those events pointed out, this space's potential as a way to amplify the public sphere bumps into clear limits in the architecture of private spaces of network interaction and the almost endless possibility of monitoring that the Internet presents.

In the first case, we are referring to the so called filter bubble,^[14] a state of ideological and cultural isolation generated by algorithms that select the information to which the Internet user has access. As private spaces of interaction – such as Facebook – offer a personalized experience to the user, showing him information arising from users that were recently added to his network or from users with whom he maintains a closer relationship, bubbles of insufficient porosity to diversity of opinions would be formed, compromising a potential improvement of our democracy. It is also necessary to pay close attention to the control of contents and users on these websites, which is undertaken via terms of use applied unilaterally and without the possibility of recourses.^[15] Users' complaints on the disappearance of posts and on the blocking of pages and users because of allegedly abnormal utilization or term violation had been numerous.^[16]

On the other hand, the protests of June happened almost simultaneously to the Edward Snowden's scandal, which brought to the public sphere something that was being discussed in specialized circles: the huge amount of personal data that we produce and make available on the Internet and how this data has been treated as public. The state control of contents and online organization can obviously intimidate and restrict the flourish of movements from civil society. During the protests, the Brazilian Intelligence Agency – ABIN, in Portuguese – had supposedly admitted monitoring social networks in search of public information, including WhatsApp (communication app whose information cannot be considered public).^[17] Moreover, the recent arrest of three managers of the Black Blocs' Facebook page – an anarchist group that acted on the frontline of the protests, frequently by means of violence – on February 4th, under the accusations of conspiracy and incitement to crime, apparently based only on the fact that they manage the Facebook page, was the clearest evidence that monitoring practices are a reality in Brazil.

Taking the debate about the blockades into account is essential to social movements and theorists interested in the widening of the Internet's emancipatory potentials and the development of demands that reach the political system. Only to begin with, we claim for the immediate approval of the Marco Civil and the Data Protection Law!

[1] Founded in 2005 at the Fórum Social Mundial de Porto Alegre, the MPL was structured to claim zero taxes on transportation for students. Organizing marches against increases in the values of transport taxes in cities from different regions in Brazil and growing throughout the country, in a structured way, but independent of parties or other entities, the movement's claims were increasingly focusing on the "zero taxes" cause by appropriating the theme of mobility as a social right and primary need of life in large cities. "The MPL has no finality in itself, it should be a way to build another society. On the same hand, a struggle for students' free pass has no end in itself. It is an initial tool for the debate on the transformation of the recent understanding of

- public urban transportation, rejecting the market's understanding and engaging in a fight for a public, unpaid and fine transport system, as a right of society; for a public transportation out of the private initiative, under public control (workers and users)". (Letter of the MPL's Principles).
- [2] The "Revolt of Vinegar" spread on the Internet - becoming martyrs of June's protests, protesters were being arrested for possessing vinegar, which works to minimize the effects of tear gases. Memes were created, defense and "how to behave in the marches" manuals spread across the network. Facebook was the primary tool for reporting, discussing and organizing the marches.
 - [3] Conservative estimates determined that, only on June 17th, 300,000 people across the country were participating. The numbers have been contested by many people on social networks. On June 20th, even after several achievements in the transportation sector, the media said 1.4 million people were on the streets.
 - [4] CausaBrasil's methodology consists in monitoring Seekr, Facebook, Twitter, Instagram, YouTube and Google+ through pre-registered hashtags, related to the protests, and listed on public file which is open to public suggestions.
 - [5] The proposed Amendment to the Brazilian Constitutional n. 37 (PEC 37, in Portuguese) planned to limit the power of criminal investigation to civil and federal police, with the main effect of removing such prosecutorial power from the Public Ministry (Ministério Público, in Portuguese). In an informative way or not, PEC 37 was used as a flag to anticorruption demands from the idea that the Ministério Público has a key role in investigations against public officials.
 - [6] Other relevant guidelines were the actions of the police in the early days of the marches of June and the World Cup in the final days.
 - [7] The exclusive constituent power was replaced by the idea of a plebiscite, which was eventually replaced by the creation of a working group, in the House of Representatives, which will submit a proposal until October for possible vote concomitant with the 2014 elections (The marches of June resurrected the theme of political reform).
 - [8] Congress approved a bill (subsequently published on September 9th) which states that 75% of the royalties owed to government arising from the oil exploration of the Pre-Salt Layer, 25% to health, and, in the same proportion, the equivalent to 50% of the Social Fund created by previous law.
 - [9] See Erminia Maricato's article in the September 4th, 2013 edition of Carta Maior magazine, evaluating the various victories of protesters, mainly from the urban mobility's point of view.
 - [10] Research conducted by Clave de Fá Pesquisas e Projetos, Aham! Interativa e Plus Marketing, in June 20th, 2013.
 - [11] Clearly there were also journalists from major communication vehicles in the crowd, and there were several incidents involving assaults and arrests against these journalists, especially on June 13th.
 - [12] The tool: the "mobile units", consisting of a laptop in a backpack (and possibly others to serve as a battery), connected to 3G or Wi-Fi from someone in the neighborhood, which binds to the cell phone. To charge the equipment, the team often counts on the goodwill of merchants and neighbors. (In the middle of the turbulence, from Estadão.com.br on July 6th, and the War Memes, from Piauí Magazine, July 2013).
 - [13] A small controversy was established as one of the leading newspapers of Brazil stated that a survey indicated that 80% of shared links with reference to the protests originated from traditional vehicles. The statement, unvarnished, ignored that the reference to the news was often made in the form of criticism, as the type of material provided by the alternative press was not always in the form of sharable links.
 - [14] The basic reference for this subject is the Eli Pariser's book "The Filter Bubble", published by Penguin in 2011. See article here and a critique of it here.
 - [15] When Lawrence Lessig, in 2005, in his book "Code", paid attention to the risks to democracy of a world in which the code would be a regulatory instrument, he was not yet able to predict that tools which allow intensive interaction, such as social networks, could be extremely antisocial accordingly.
 - [16] One of the most common complaints of social movements comes from feminist movements, which often have materials and pages blocked because they use images of the female body. As one of the protests' agendas were the LGBTT's and reproductive rights, the phenomenon occurred frequently during the June journeys.
 - [17] See ABIN assemblies network to monitor the Internet, published on Estadão.com.br on June 19th, 2013.

Hacking team in Chile: does the software comply with the minimum quality standards established by the Chilean legal system?

*Valentina Hernández*⁷⁶

Chile's Investigative Police Force (PDI) confirmed the purchase of a modern spy software by the Italian company, explaining that it is a tool to face highly organized criminal activity. Is it proportional to the use of a computer program of this nature?

Towards the end of 2011, all the inhabitants of the city of Buenos Aires and its suburbs wanted their SUBE, as the public transport card for our city is known. The new technology promised to solve a problem and avoid one in the future. On one hand, we would. On July 6th, Chile's Investigative Police Force (PDI) confirmed the purchase of a Hacking Team's software called "Phantom". The clarification of this matter happened after a group of hackers broke into the system of the Italian company and leaked 400 GB of information, among those several emails talking about the purchase were found. The PDI justified the purchase as a part of a plan to increase their operational abilities in the investigation of organized crime, international terrorism and large-scale drug trafficking.

Phantom is a variation of the Remote Control System, the Hacking team's key product, and it is what is known as a trojan: a malicious software presented to the user as a genuine and harmless software but when executed gives the attacker remote access to the infected device for both computers or smartphones.

This software is capable of collecting emails, turn on the camera or the microphone of these devices, and access files, even those that have been already deleted, among many others functions. The big intrusive ability of this software immediately raises one question: does it fulfill the minimum legal standards established by the Chilean legal system?

The Criminal Procedure Code, just like certain special laws (the Antiterrorism Law, the Drug Law or the National Intelligence Agency Law) contemplates and allows, in the investigation of certain crimes, the exercise of investigative management that infringes the fundamental rights and

⁷⁶ Valentina Hernández holds a law degree from the Faculty of Law at University of Chile. She is a NGO Derechos Digitales' researcher.

freedoms from subjects under investigation, as long as they fulfill a series of prerequisites. Among those, a prior judicial authorization allowing the execution of this action is needed.

Is Phantom legal?

The ninth article from the Criminal Procedure Code, titled “Prior judicial authorization” requires the Public Prosecutor’s Office to ask authorization to the Magistrate Judge to execute an investigation management that takes away, disrupts or restricts fundamental rights. Given the extremely intrusive nature of this tool, this management is unavoidable.

But among the leaked emails (indexed by WikiLeaks), there is one that attracts attention. It is a conversation between the Hacking Team and Jorge Lorca, salesman of Mipoltec, company working as intermediary between the Italians and the police. In these emails, Lorca explains that this tool will be used as a “support to get the client’s IP data and to access to information that they could not obtain with a court order”.

This information contradicts specifically what the PDI has said in a public statement and, if it’s true, it is a capital offense to the Chileans’ constitutional rights and an utter contempt to due process.

Unfortunately, this would not be the first time the PDI acts outside the law to get information in the exercise of its functions, violating the right of privacy.

Is Phantom proportional?

It is difficult to give a legal answer without knowing any details of the reasons why this tool has been used. In a preliminary way – and only from the huge wide range of possibilities of surveillance, tracking and information record that “Phantom” gives – we think that the number of cases where the use of a technology of this kind would be proportional is extremely unusual and limited, exceeding the constitutional limits in most cases.

Now, if used, it should be only in crimes of highest social dangerousness and with a previous legal warrant that delimits the range of this intrusive activity to get the essential data for the criminal investigation.

The problem is that the high capacity of this tool encourages the opposite; this is why control and transparency mechanisms are essential to avoid massive surveillance and political or ideological persecution, charges already existing against Hacking Team. Thus, it is time for the Police Investigative Force to give a more complete explanation about this software and its use in Chile.

Internet rights in Ecuador: the possible triumph of activists?

Analia Lavin⁷⁷ and Valeria Betancourt⁷⁸

The appearance of the “Free Internet” coalition was crucial in raising the alarm on one of the most controversial articles of the new criminal code that would allow the monitoring of Internet. But is the possible end of Article 474 sufficient enough for the government to respect fundamental rights in communications?

After the revelations of Edward Snowden in June this year, the Assembly of Ecuador passed a resolution rejecting the “illegal and indiscriminate use of espionage” carried out by the United States and considered it an attack against the “right to privacy and the privacy of all the inhabitants of the planet”. A few months later, the Ecuadorian representative in his speech at the UN General Assembly criticized how these practices ignore “the right to privacy and freedom of expression of all citizens”.

During the same period, however, the Assembly of Ecuador discussed and approved a new penal code that legalized the systematic surveillance of communications, jeopardizing the exercise of these rights which were zealously defended in the case of U.S. practices.

Civil society organizations, user groups and Internet users closely followed the discussions on the law and got access to drafts which put them on alert. Together, they formed the “Free Internet” coalition and launched a campaign that included digital activism, along with meetings with Assembly members from all the political parties and reports sent to the president. Although at the time of writing this note there is still no official confirmation, it appears that the most problematic aspects will be eliminated from the final text.

Article 474, the most controversial aspect of the new penal code, requires Internet service providers to store user data “in order to carry out the corresponding investigations”. This article, however, goes far beyond mass state surveillance, extending the same storage requirements to “subscribers of telecommunications services that share or distribute their voice or data interconnection to third parties” and seeks to bring these policing functions to the citizens themselves, promoting a culture of permanent distrust where everyone could potentially end up spying on each other.

⁷⁷ Analia Lavin is part of the communications team of APC.

⁷⁸ Valeria Betancourt is director of the Policy Program of Information and Communication at APC.

Besides contradicting rights enshrined in the Universal Declaration of Human Rights, this item violates the Constitution of Ecuador, which recognizes the right to personal and family privacy. It also establishes that both privacy and interference of virtual correspondence require minimum guarantees as authorized by the owner or judicial intervention. The alertness raised by Article 474 would be generalizing the limitations of a law which, on the contrary, should be the exception. As stressed by Ecuador's representative to the UN General Assembly, and mentioned above, privacy is closely related to freedom of expression and practices, such as censorship, affect the quality of democracy in the nation.

But Article 474 not only legitimizes the systematic violation of fundamental rights of citizens, it also presents serious problems in its implementation. Storage of "data integrity" of people's communications for at least six months that are required by law, would force service providers to exponentially multiply their storage capacity, to update their physical and virtual infrastructure and strengthen their security protocols.

The very high costs of these measures, which will probably end up being transferred to the end user, will also have an impact on the investment priorities of companies, who would have fewer resources to extend their services to less profitable areas.

Finally, the volume of information and data which the law requires to be preserved (basically all Internet traffic and telecommunications in a country of fifteen million people) multiplies the risks of interception, analysis and non-consented use for commercial or political purposes as well as compromising the security of electronic economic transactions of the government, among other things. If this article is approved, the criminal code, instead of protecting internet users would actually expose them to conditions of extreme vulnerability. Such legal content, ultimately limits the deployment of network usage for social, economic, political and cultural development.

These were some of the arguments used by the "Free Internet" coalition. Activists involved in the campaign, however, think that the decisive factor was the decision on privacy in the digital era, recently approved by a committee of the UN General Assembly. The resolution, pushed forth by Germany and Brazil, states that the "monitoring and/or interference of illegal or arbitrary telecommunications, as well as the illegal or arbitrary collection of personal data, are highly invasive acts that violate the rights to privacy and freedom of expression and may contradict the principles of a democratic society". Ecuador is among the 23 countries that signed the resolution.

The assemblywoman who announced the annulment of Article 474 on Twitter (an announcement that, again, has not yet been made official), referred to “political and ideological coherence” as the reason behind this decision. While Ecuador supports such resolutions at the UN and offers political asylum to Julian Assange, to position itself as a world leader in Human Rights, the situation within the country is worrying. This year, for example, an organic law of communications was approved which, among other problematic aspects, demands electronic media to register the identity of those who publish comments. If it seeks political coherence, Ecuador must renew its commitment to the fundamental rights of its own citizens.

The online mobilization against Jair Bolsonaro, Julien Blanc and the rape culture

Michael Freitas Mohallem⁷⁹

In March 2014, the world was surprised by the results of the research “Social tolerance to violence against women” by the Institute of Applied Economic Research (IPEA), which indicated that Brazil is a country that tolerates violence against women. More than 65% of men had agreed that “women who wear clothes that show the body deserve to be attacked”. The results provoked strong reaction in social networks and thousands of women left the image of their nakedness convey the message that “they do not deserve to be raped”.

The online campaign, started by journalist Nana Queiroz on her Facebook profile, had 40,000 likes and was followed by a review of the research conducted by IPEA. Although errors were found in the tabulation of the results and a less shocking conclusion was published, the new data that one in every four Brazilians is tolerant to abuse against women has not diminished the feeling that this is still an obscure feature of most men in the country.

What could have been an isolated moment of feminism in the spotlight has remained a living and active feeling in social networks. One of the signatures of the demonstrations is its objectivity: the end of rape culture may depend on cultural change at a deeper level and, therefore, time

⁷⁹ Michael Freitas Mohallem is a professor at Rio de Janeiro Law School and Avaaz’ campaign director in Brazil.

consuming, but what people are looking for through the recent online actions are immediate results, able to signal the change in the tolerance degree with misogynistic, and sometimes criminal, statements.

That's what it was possible to detect last November when a group launched an online petition asking the Brazilian government to deny Julien Blanc his visa request to enter the country. The "Hitch artist" sold lectures on how to become a womanizer, but his videos available on the Internet made people sick to their stomach by the humiliating way the girls were treated. Blanc speaks to the camera, laughs, uses physical force to abuse women, as if they were also spectators of his actions. What they thought about it did not matter much to the guy. They are objects of his "business".

The campaign touched thousands of people, caught the attention of the press and caused the Secretariat of Women Policies (SPM) to position itself publicly on the matter. Rather than simply condemning Blanc's action, the SPM ratified the claim and began to pressure the Ministry of Foreign Affairs (MFA) to prevent Blanc from entering Brazil. In only four days, the petition reached 350,000 subscribers who celebrated the confirmation by the MRE (Ministry of Foreign Affairs) that, in Brazil, Blanc would not have a chance to propagate violence against women. As a result of intense online reaction, his visa will be denied.

In the third and most recent episode, Congress member Jair Bolsonaro offended female congress member, Maria do Rosário, again on the House floor. He said: "The only reason why I don't rape you is because you don't deserve it". The words of Bolsonaro, although not new, this time provoked the reactions of women and men who do not tolerate the rape culture. The repulse at the idea that rape is a possibility that depends only on the offender's will motivated thousands of people to start discussions about the act.

Cristian, a member of the Avaaz community, started an online petition asking the impeachment of Bolsonaro's mandate for breach of parliamentary decorum. In a few days, the campaign won the support of 250,000 people and motivated protests in front of the National Congress. The deputy Federal Attorney General, Ela Wiecko asked the Supreme Court to judge Bolsonaro for inciting rape. Members of various parties have also agreed on Bolsonaro's impeachment and the Ethics Committee of the House may be challenged again in the next legislature. Once again, the strength and intensity of what happens on social networks seems to provide assurance and support for institutions to continue fast in the direction of what before could not be realized.

The various demonstrations against the known hatred and prejudice in the performance of Jair Bolsonaro opened healthy space for reflection on the limits of freedom of expression. And once again we are faced with a known limitation of this right that becomes mixed up with the principles of democracy: hate speech does not receive the full protection that we should provide to all other forms of expression of ideas. This congress member summarizes a paradox of the proportional representative system. While he is the most voted congress member of the State of Rio de Janeiro, he represents an ideology of a minority group in the state and in Brazil.

In Bolsonaro's case, it is important to observe that it has to do with a political strategy of conservative speech radicalization in order to compose the bizarre character he wishes to personify. Public figures who become famous for extravagances or, worse, with attacks to other groups in society, should suffer careful public scrutiny so that people know who is the man or woman behind the character.

The pressure against Bolsonaro has been working. From network to courts, people seem determined to change the way we look at crimes against women once and for all. Avaaz promises to organize a great act of delivery of signatures in Brasília when it reaches 500,000 supporters. It could be a great time to fight the culture of abuse and silent violence against women.

Jair Bolsonaro and Julien Blanc do not represent new ideas. They are personalities that grow and feed on the still wide conception that women should be overpowered. The novelty is in the form of current campaigns. In each of these collective manifestations, what we see is the feeling that tolerance to violence against women denigrates much more than the few who defend it. Perhaps the end of their public careers does not mean the end of the culture of women oppression, but they will be promising victories of the power of online actions and the invitation to multiply them.

Technology and political participation

Eduardo Magrani⁸⁰

There is a scenario still quite unfavorable in Brazil for greater effectiveness of direct democratic participation in the legislative framework in relation to the commencement of popular initiative bill.

⁸⁰ Professor of Law and Technology and Intellectual Property at School of Law at Fundação Getúlio Vargas (FGV). Researcher at the Center for Technology and Society (CTS-FGV). Project leader on E-democracy and Internet of Things. Brazilian Coordinator of Creative Commons and the Digital Rights: Latin America and the Caribbean project.

The first obstacle is due to the fact that, according to the Federal Constitution of 1988, a popular initiative bill, to be presented properly, must contain signatures of at least 1% of the Brazilian electorate (about 1.4 million people). In addition to this requirement, which is itself a major impediment, there are two more obstacles: the fact that only accept physical signatures in practice, despite the Constitution and Law No. 9,709/98 speak only need to “subscribe” not expressly mention the physical medium and; the problem of not having a clear and efficient system for the validation of signatures. As a result of these obstacles, the Brazilian Constitution of 1988 celebrates 26 years of age and over that period only four projects of the genre were approved in Congress.

Over the 26 years of “citizen Constitution” other forms of direct participation provided for in FC/88 as the plebiscite and the referendum were used only twice. The first time, in 1993, the population – through referendum – kept presidentialism and the republic as form and system of government. In the second, in 2005, the population, through a referendum, rejected the prohibitions of firearms, provided in disarmament statute. Otherwise, local plebiscites were conducted only on the creation of new states and municipalities.

It is evident, therefore, the under-utilization of the mechanisms of direct participation in the legislative sphere, despite the recognition of its validity in democratic terms is quite evident even in a mostly representative system like ours. In this scenario, seeking primarily to overcome the obstacle related to the high number of physical signatures required, several bills currently being processed have the proposal to encourage and enable more clearly that the popular initiative bills can be signed electronically.

However, it is still clear a lot of uncertainty with regard to participation by virtual means. There are already, however, technological mechanisms to reduce the risks. New technological paths have allowed significantly minimize the risk of violations of platforms and forgery of signatures through a more reliable system of authentication of signatures. The digital certification, for example, is considered an extremely effective tool allowing minimize security risks and achieve functional equivalence with handwritten signature.

A more sophisticated validation system should always be pursued as effectively to prevent fraud and crucial in order to give more credibility to online political participation.

The collection of electronic signatures for popular initiative bill proposition reduces to a great extent the logistical problems associated with the collection of signatures on paper. The online signature collection procedure

acts as a catalyst in the democratic process enabling much more breadth and efficiency collection of thousands or even millions of signatures in a smaller range of time and cost.

One of today's major challenges of Brazilian democracy is rightly think best ways to combine initiatives and mechanisms for the types of direct democracy, participatory and representative, aimed at achieving greater legitimacy of our political system. To this end, it is essential not to neglect the ways enabled by the Internet to the improvement of democratic society.

Collaborative development in Labhacker: including the “external element”

Cristiano Ferri⁸¹

With about a year and a half of existence, we now have a clear vision of the direction of an innovation lab focused on legislative citizenship. We're talking about Hacker Laboratory of the Brazilian Chamber of Deputies, which was created from the conducting of a hackathon aimed at developing projects of transparency and participation in the federal legislative process, which took place in October 2013. The goal was to establish a permanent hackerspace in the House, so that these projects could be continued, as well as encourage the creation of new similar ideas.

Innovation labs in governments

The Labhacker came in the wake of innovation laboratories for citizenship that are emerging in various parts of the world. The MediaLab Prado in Madrid, the GovLab in Chile, the Policy Lab in the UK and the MindLab in Denmark are some good examples, though more based on the work of the Executive. The Labhacker was conceived as a space for interaction that could house any citizen interested in legislative transparency or issues that facilitate interaction with Parliament. Currently, with free Internet and space for free use, hackers, politicians, researchers and others interested in the subject frequent Labhacker.

We know, however, that many of the applications developed on hackers marathons are prototypes, many of them still in a rudimentary stage or non-functional. In general, they are not being continued by their authors.

⁸¹ Cristiano Ferri is the coordinator of Hacker Laboratory of the Chamber of Deputies.

And the reason comes from the lack of resources for its realization and implementation difficulties of the initial idea. We think here in Labhacker that we could help in the process of further development of this idea. With small multidisciplinary team, not more than ten people, made up of experts in information technology, project management, administration, law and other areas, we do some work to continue these projects and generate new ones.

For example, in the Hackathon 2013, one group of participants developed an application called Parliamentary Rhetoric, with innovative proposal of preview of the most trending topics in parliamentary speeches in the form of soap bubbles. As the project's code is open, the staff here in the Labhacker made some improvements in it, changed the layout, included more databases and released a new version more functional.

And the social, where does it enter?

Now, our main difficulty is to include the “external element” in Labhacker work processes. We believe, of course, that one of the most important values of a hacker space in the public service is the opening to anyone to develop ideas, projects and debates on citizenship – preferably that has to do with the Legislature, but not necessarily – being physically here or remotely.

Therefore, that collaborative action networked, horizontal, transparent and interactive needs to be part of our DNA in Labhacker. However, I will confess that, on a daily basis, it is not that easy and I explain better exploring here the three dimensions that are part of our métier: the social universe, the bureaucracy and politics.

The restless politics

Let's start backwards, talking about politics initially. The main difficulty in engaging parliamentarians in the Labhacker collaborative activities is the complicated and dynamic parliamentary agenda. Regardless of the profile of the deputy, if more intense, or more relaxed, if right wing or left wing, all without exception, have an agenda of unceasing professional activities, ranging from meetings in the many permanent and temporary committees, party meetings, parliamentary fronts meetings, to the attendance of countless people, social representatives, business people, councilors, mayors, in his office. Oh, one should also not forget the huge routine plenary, which runs from mid-afternoon until late evening. In addition, there are other activities such as appointments with ministers and other political authorities to solve problems in their area.

Therefore, involve parliamentarians in hacking is not easy, because we have to compete for their time, attention and energy to this myriad of activities. We see that increasingly they are open to this type of action, some more, of course; others less, because many still do not understand fully what is to be hacker, which has been a controversial term. But when we can attract parliamentarians for the activities of Labhacker, they, in general, like, add a lot in the activities and some even start to incorporate/intensify certain interactive practices into their daily activities.

The sturdy bureaucracy

Let's talk now of the bureaucratic part. This is one of the most problematic. I, as a public servant for 22 years already experienced (and still going through) discouraging experiences, will not deny to implement innovations. Speaking the obvious: there is a lot of demotivation, lack of commitment, limited vision, individualistic action, corporatist sentiment, among other negative aspects of some public servants. Of course, there are many other professionals open to improvements, struggling to innovate in their work and help a lot to bring new values for public administration.

Now, with the "Access to Information Law", transparency became a rule. Not make public actions, information and data has become the exception. Moreover, that must be justified to occur. In addition, the State, according to this law, must be open to citizen participation in their activities. Well, that should mean total change of attitude in the conduct of the bureaucrat. However, in practice it has not been so well, because there is still some blind obedience to secular proceedings and a generally conservative legal interpretation of the laws. Moreover, all to reiterate averse culture to the incorporation of citizens in the work processes of public administration and difficulty in seeing things from the side of society.

We will not invade your beach

To end this story, let's now turn to the social side. There are growing proportion of interested transiting through Labhacker, participating in the hacking and developing projects on legislative transparency, political education and so on. In general, this participation has been sporadic, however. Some develop interesting projects but, for various reasons, cannot keep them or evolve them. As I said earlier, from what I gather, the main problem is the lack of resources to work on projects systematically.

In fact, contrary to what occurs in other countries, where foundations and NGOs can fund to develop and maintain projects on legislative transparency, in Brazil it has been much more complicated. The guys managed to make creative data visualization and intelligent applications at certain times of galvanizing efforts with collective action fronts, as hackers marathons and hackdays, and then need to return to their own work (which usually does not have much to do with that), and the projects are becoming aside.

Well, discussing solutions to these problems is a subject for another article because the matter is complex. Meanwhile, let's bring together politicians, public servants and hackers who are in order to develop interesting projects in this area and cool things are coming out. What for example?

The Indignados movement in Central America reconfigures the traditional class struggle

Bernardo Gutiérrez⁸²

Not too many people suspected that April 16th, 2015, would mark a before and after in the politics and society of Guatemala and Central America. When the special prosecutor office against impunity (FECI) from the Public Ministry (MP) unveiled a network devoted to custom frauds (linked to members of the government), a Facebook event summoned people to attend a “pacific rally to ask for the resignation of Otto Pérez Molina (president) and Roxana Baldetti (vicepresident)” on the 25th.

The Facebook event (no longer operational, although the wall is recovered and it is available on Dropbox) was created around a narrative that has no precedent in the region: “No political or ideological affiliations, no discourses or shows, this is just the Guatemalan people, tired of the unscrupulous politicians governing us. Let's get to the Central Park, show our inconformity and let everyone know that we are not asleep”. #RenunciaYa has not only established as a shout-out slogan but rather as a movement with nodes distributed all over Guatemala and the world. From the web to the street, this movement began to leave its mark in the political agenda and to reconnect unequal historical struggles to a new imaginary.

82 Post journalist, writer, convinced transnacionalist.

In June, #RenunciaYa became #JusticiaYa (its main Twitter account is @justiciayagt). The new Indignados, as they started to be called, had a key role in the reconnection and reconfiguration of the classical Guatemalan struggles. The mini documentary *The encounter: three months of citizen protests* shows the evolution of a movement that shouted “yes, it was possible” after the resignation of the vice-president Roxana Baldetti and that was the key to inspiring the riots that started taking place in June, in demand of the resignation of the president of Honduras, Juan Orlando Hernández.

These two countries organized an unprecedented bi-national rally for the 4th of July and are taking over the anti-corruption discourse in Latin America, a discourse that used to be linked to the right wing. In the hands of popular movements, the anti-corruption cause becomes a strong, symbolic blow for the government and it is already generating uneasiness.

Both in Guatemala and in Honduras, technopolitics is barely just a layer that coexists with other paradigms and that reconfigures the already existing struggles, making it possible for there to be a metanarrative that includes said struggles and technosocial processes that respond to a global pattern.

Part of the Honduras case study from the #technopoliticLATAM investigation I made for OXFAM is presented below. By the end of September, the complete study will be published.

From #JusticeNow to #ResignNow

On June 28th, 2009, the people of Honduras were called to vote on a referendum to decide on a change in the Constitution that would allow presidential reelection. The Supreme Court of Justice, against the referendum, commanded the armed forces to arrest president José Manuel Zelaya. The designation of Roberto Micheletti as president was the final confirmation of a coup d'état and opened the door to a new type of violence and political repression.

Since 2009, Honduras' social statistics have only gotten worse. What stands out are the high levels of poverty, corruption, militarization and violence (for example in 2013 one person was killed every 78 minutes, according to the Observatory of Violence from the Autonomous National University of Honduras). The existence of The Tigers (special operation forces trained in the USA) and the Homeland Guardians (group that encourages children to use weapons) round off one of the worst scenarios of militarization and repression in Latin America.

Furthermore, “the leaders of the coup faction had religious domination interests”, which translated into the prohibition of the morning-after pill and an intense persecution of the feminist interests. Femicidio – word used in Honduras instead of femicide – has had an increase of a 263.4% between 2005 and 2013.

In this scenario, denouncing Human Rights violations became the epicenter of the Honduran struggles. There are hardly any emerging citizen processes or any digital activism and “the isolation of the struggles prevails”. The National Front of Popular Resistance, that tried to encourage a pacific form of struggle after the coup d’état, consolidated as a new forum for establishing a dialogue between “feminist movements, unions, teacher leaders, students, farmers, LGTB, socialists, liberals, independents and artists”. Other important social causes are being addressed by the communities that oppose the looting of their common goods by mining companies or the concessions being granted in their territories (water, resources).

The introduction and use of the Internet in Honduras has many peculiarities. Despite of the low percentage of users (18,6%), 60% of Hondurans connect to the Internet to access digital social networks, what makes it the most active country of Central America. Even though Twitter has boomed, since 2009 Facebook is the most used social network.

Social movements do not interact much with the digital environment. There are some remarkable exceptions such as the video blogger La Chiki or campaigns against femicide on Twitter (with the hashtag #ObservaMujeres standing out), but other than that, social struggles use more traditional formats. Among other peculiarities about Honduras, there is the fact that the amount of mobile phones is larger than the amount of people, a lot of Internet connections are made from those devices and the use of mobile networks (WhatsApp) is high.

The wave of protests that broke out at the beginnings of June, 2015, in demand of the resignation of president Juan Orlando Hernández has given new meaning to the social struggles in Honduras. Its narrative disruption incorporated actors that were ideologically different and contributed to the rise of a new political actor: Honduras’ Indignados. Additionally, this process has technopolitical characteristics, such as the self-convocations that use social networks as a platform, the citizens’ ability to self-organize, the breaking up of the frontier between the Internet and the territory, and the empowerment of the people on an emotional level.

When the president publicly recognized that the National Party had accepted illicit money from the Honduran Social Security Institute (IHSS), people showed their indignation through the use of hashtags such as #renunciaJOH or #fueraJOH. One day after (July 5th), over twenty thousand people participated in a rally in Tegucigalpa organized using the social networks: The Rally of the Torchs. The demonstrations expanded throughout the country and the media started talking about the new Indignados movement, which was partly inspired by the protests against corruption in Guatemala that have been demanding for the resignation of the president Otto Pérez Molina since April.

The #renunciaJOH protests started taking place every Friday, thus creating a new space of action and collective dialogue. In addition, an international connection with the movements in Guatemala was established. In this country, where #RenunciaYA evolved to #JusticiaYA, changes in the electoral law are already being demanded and the transnational Guatemalan citizens are setting the political agenda.

On July 4th, both countries organized an unprecedented binational rally that renewed the Latin American anti-corruption discourse and included popular movements in the process. This was rather confusing to the American lobbyists that generally try to apply the neoliberal shock doctrine using corruption as an excuse. In the case of the Honduran Indignados, there have also been mass actions that evidence a sense of collective identity, such as the defense of the journalist David Romero (who brought the corruption scandal to light) through the use of the hashtag #WeAllAreDavidRomero

The study conducted together with Alejandro González (Outliers Collective) exclusively for this report analyzed the tweets that use the hashtag #ResignJOH between the days 05/06/2015 (Day of the Rally of the Torches) and 06/07/2015. The results show quite a decentralized topology and a big density (many nodes having conversations in multiple directions).

A distinctive feature of the graph is the importance of the collective identities (like the humorous profile @notibomba) and, in particular, the importance of the ecosystem of Anonymous. Nodes such as @legionhonduras, @anonshonduras, @anon_honduras or @ibero_anon have been fundamental to the configuration of the public imaginary of the new Indignados.

At the same time, the accounts of some journalists, alternative media or writers (@Chaveztoon, @julissa_iras, @soyfdelrincon) stand out, as well as the account of politicians from the Freedom and Refoundation Party

(LIBRE), which emerged as an evolution of the National Front of Popular Resistance (such as @beavalleM or the former president José Manuel Zelaya, @manuelzr). In the graph, it is even possible to see international accounts like @personalescrito (Brasil) or @takethesquare (15M España).

The traditional social movements present on the streets are not specifically outlined in the study about digital networks of #resignJOH. The official account of the National Front of Popular Resistance (@fnrphn) has little relevance and the political actors that started the #ObservaMujeres campaign in 2014 are not considered either. The lack of the traditional social actors in the study is due to the fact that Twitter is not their most widely used digital network and also because these actors do not attribute much importance to the Internet.

Hacking patriarchy: the first #femhack experience

Gema Manzanares⁸³

Some weeks ago, we started to plan the Nicaragua femhack: we made a public announcement inviting women with diverse backgrounds to propose seminars and workshops. The announcement spread across social media and reached a group on programming in which most participants were men. “Are there women programmers?”, “It sounds weird to me, I’ve never seen women doing this”, “It’s something I’ve never seen; I haven’t even met many docile women in the computing field” were some of the comments. Is anyone surprised?

“Science and technology provide fresh sources of power,
that we need fresh sources of analysis and political action”

— Donna Haraway (1991)

What is the source of this inability to see and acknowledge women involved in technology, science and engineering? I think of many reasons: educational programs where girls socialize to achieve order and where they rarely have the opportunity to disassemble and reassemble things; indifference towards women’s contributions to technology and science throughout history; contempt for women’s abilities; among other.

⁸³ Gema Manzanares is a communicator, (cyber)feminist, activist, founder of @EnRedadasNi and Nicaraguan designer.

But it's the idea of the female technophobia what troubles me the most. When they say that women are simply "afraid" of using/creating technology, they are blaming us and justifying a social system of disadvantages. They are conveniently overlooking that there are huge access gaps, between men and women, to basic rights such as education; and that the system delegates to women household responsibilities, so they have less time and income to dedicate themselves to their own interests. Just to illustrate my point: according to ECLAC, in 2013, two out of three people without Internet access worldwide were women.

But there are women who can indeed be found in these places: women who live on the Internet, women programmers, developers, women studying engineering, women who learn to repair computers and cell phones; and we see that the path is not an easy one. In a context where practically all our interactions take place through the screen, women have to deal with trolls and bullies, who target them for their attacks just because they are women.

A cyberfeminist proposal

A lot has been written about cyberfeminism and yet not enough. Cyberfeminism acknowledges technology as a key element for the social changes of the last decades and it proposes to build fairer and more equitable societies through the Internet. As cyberfeminists, we believe that technology is not neutral: because it is always used based on subjectivities and human prejudice.

We saw the need to promote the involvement of more women in courses and jobs relating to engineering, mathematics, computing and science in general; the need to review the course of history to rescue the life of women who have made contributions to these fields; the need to reflect on our own practices, on the content we are creating and sharing online; and the need to re-signify spaces and create new ways of interacting, new languages, new ways of creating knowledge. But we also identified systems of daily oppression empowered by a sexist way of thinking that we must be aware of so that measures can be taken to mitigate its impact on our lives.

Many feminists are using the new technologies to promote and defend women's rights, many women are becoming involved in technology projects: developing companies, writing codes, running online businesses, maintaining blogs on diverse subjects, keeping diary videos; the question remains: what can we do to bring them together?

#femhack

By the end of last year, we, a group of women interested in promoting a feminist interpretation of technology use, agreed to work collectively on a global event to make visible the need of a space of mutual recognition and collective creation for women and queers. That is how the idea of #femhack was born.

The first thing we made clear was the diverse and adaptable nature of #femhack. We weren't talking about a single event that would follow the same methodology in all countries: we wanted an event as diverse as the women who were planning it, with its own agenda, its own content work and its own identity in each place. We all agreed about the need of femhack being a safe space: free of sexist remarks, racism, homo/lesbian/transphobia and any other kind of violence and hatred towards participants in addition to the promotion and use of digital security practices as part of the event.

During the planning stage, we received the news about the assassination of Sabeen Munhad, who, despite not being part of the group promoting femhack, worked very hard for digital rights; she was the mind behind the first hackathon in Pakistan and a pillar of activism in the region. We thought it was fair to honor her memory around the world by dedicating femhack to her name and by taking the time in each country to share information about her life and achievements with those participating in the event.

After many discussions and postponed dates, it was decided that May 23rd would be the date for holding the event simultaneously. We started to organize activities in each of our own countries and some comrades created a website to make a public announcement and invite more women/women groups to participate around the world.

Little by little, pink spots started to appear, marking the venues of the activities on the map of the website: Mexico, Nicaragua, Colombia, Argentina, Brazil, United States, Canada, Spain, Basque Country, France, Scotland, Germany, Serbia, Austria, India, Pakistan, Indonesia, Kenya and Australia. The femhack agenda included workshops, round tables, hacker groups, forums, festivals, performances and other diverse methodologies.

We were on social media and communicated using the hashtag #femhack: recording experiences, sharing thoughts and resources, passing the torch from country to country. After May 23rd, activities continued taking place: the following Saturday, May 30th, Mexico and Colombia resumed their events and on June 6th it was our turn in Nicaragua.

Feminist Hackathon in Nicaragua

I wish I could show you national statistics and data on the binary women-technology in Nicaragua, but there are no official nor unofficial public records on the subject: because those who have the capacity and means to conduct this type of investigation are not interested and we, who are interested, do not have the capacity and resources.

As I mentioned at the beginning, we made an announcement for lecturers and facilitators. We wanted to know, hear it from women's voices, how they are interacting with technologies: we wanted to create a space to learn collectively. We received 11 proposals, new seminars and two workshops on digital security, activism, virtual identities, being a blogger, resources to learn programming online and the presentation of individual and collective projects arising from the Internet.

The event of June 6th meant a lot of learning and thinking.

We concluded that, on the Internet, personal means political: in a context where spaces are being closed day to day and women's contributions undervalued, expressing and sharing our personal experiences and opinions are revolutionary acts. We notice that there isn't a single way of coexisting with technology: that some of them are creators, some of us are prosumers, we have blogs, they create applications, some of them do programming, others write, some of them design, others take pictures, some administer forums, others edit wikis; there are so many possibilities.

We notice an adverse situation towards women who are on the Internet, manifesting through virtual violence and surveillance of our communications, which obliges us to promote and include digital security practices in all our actions. We need to develop more effective strategies for creating alliances with key people and groups to achieve a greater impact on a local level. We gained strength and support from the global network of #femhack, as well as support and advice from our Latin American comrades who live in similar contexts.

What is next for us? Internationally: more femhacks. Nationally: more femhacks. We are committed to facilitating spaces for reflection and creativity where feminism goes hand in hand with technology. We want to continue growing, see a map full of pink spots. I hope I'll be in front of this computer within a couple of months, working on a new announcement, this time for the second #femhack.

PART

7

SURVEILLANCE AND CYBERCRIME

Limits to domestic espionage: what comes from within can also strike us

Francisco Brito Cruz and Dennys Antonialli⁸⁴

Brazil must pay attention to the consequences of relying on the discourse of national sovereignty in order to react to USA's digital espionage.

The Brazilian reaction to the American digital espionage scandal set off by Edward Snowden's revelations presented various layers. On the diplomatic side, Rousseff's government articulated a negative public response through the president's speech in the UN opening ceremony. In terms of strategic planning, Brazilian State noticed the necessity of investments in infrastructure with the aim to decentralize the web (as well as the bet on cabling and on other equipment which can make data traffic cheaper inside national territory or the adoption of auditable software in the equipment^[1]). From the legislative point of view, the federal government is currently pressing the House of Representatives to vote the bill known as "Marco Civil da Internet", which now has an even more protective text concerning privacy.

In short, we can say that during the debate that followed the Snowden scandal, Brazilian government has been defending its sovereignty, as well as assuming the role of privacy guardian to its citizens in order to justify its new political agenda. One must remember, however, that the same speech used to protect the sovereignty and the security of national interests legitimized the creation of loopholes in the U.S. legal system in order to relativize the right to privacy. The Foreign Intelligence Surveillance Act Courts (FISA Courts), created in 1978, were rediscovered and strengthened after the 9/11 terrorist attacks, with subsequent amendments. This institutional arrangement removes the common judicial control on possible monitoring mechanisms that violate the privacy of citizens and is a key system for the NSA spying activities inside and outside the USA.

This does not happen by chance. Sovereignty and security concepts are broad and versatile. It is the institutional practice that has succeeded in giving muscles and shape to the discourse that uses them both. At this point, it is crucial that the Brazilian government intends not only to think of ways to subvert USA's power of surveillance, but also in establishing limits for the eventual assembly of this type of arrangement in the domestic sphere.

⁸⁴ Francisco Brito Cruz and Dennys Antonialli are coordinators of the Center of Law, Society and Internet at Universidade de São Paulo (NDIS, in Portuguese).

Recently, episodes that demonstrate the intrusive performance of the Brazilian government's intelligence agencies have multiplied.^[2] The protests that rocked the country in June this year were monitored by ABIN and various types of authorities on social networks – including personal communications via the WhatsApp application – which led to the capture of webpages' administrators and a huge sum of situations that can possibly damage the right to freedom of expression.^[3] In order to execute digital surveillance, general José Elito, from the Institutional Security Cabinet of the Presidency (GSI, in Portuguese), now has at his disposal the Mosaic program.

Amid the anticipation for the vote on the Marco Civil, the newspaper *Folha de São Paulo* reported that the Brazilian Intelligence Agency (ABIN, in Portuguese) diplomats spied at least three countries between 2003 and 2004 – Russia, Iran and Iraq. The information was included in one of the agency's reports accessed by the journalists. In quick response, the GSI stated that the documents made reference to counterintelligence activities and the operations “obeyed the Brazilian legislation for the protection of national interests”. It also promised that those responsible for the leak of secret reports will be sued. The fact reverberated internationally.

The proposal to hold data in Brazilian territory offers a new field for “domestic espionage”. Much has been – mistakenly – advocated on how the measure itself would make Brazilians less exposed to the scrutiny of other governments. Meanwhile, little has been said about the (even) greater vulnerability that the situation can represent to Brazilians. As it was already indicated by research conducted by the Center of Law, Society and Internet of the Universidade de São Paulo^[4] (NDIS, in Portuguese), rarely does the Judiciary see anonymity as a tool worthy of protection. Often, there is an exaggerated leniency with requests that present questionable identification, determining the supply of early data connection and access. Vulnerability becomes clear as we face the high numbers of Brazilian requests on data identification released by the Google Transparency Report. With data based on national territory, this resistance to privacy protection and anonymous surfing by the Brazilian authorities may have undesirable effects on democratic life.

Despite the fact that intelligence activities may have plausible justifications, this does not relieve us of the need to promote a thorough discussion on how to protect Brazilian citizens (and foreigners) against the spying activities made by their own government. It is not enough to protect yourself from outside menaces; it is necessary to establish limits to what comes from within.

It represents the opening of a broader public debate concerning the limits of state surveillance activities. The juridical doctrine which prioritizes individual guarantees related to the criminal procedural law can be a starting point, but its dogmatic will only be able to discuss the new terms of the game if it embodies fresher ideas, allying itself with other concerns, such as those involving the right to privacy, freedom of expression and particularities related to the Internet's architecture.

These issues are still very incipient in both the public debate and in academic production in Brazil. An example of this situation is the curriculum of law schools. Very few are the disciplines, the research or the entities specialized in the study of these rights. Here, the debate is just beginning. The approval of the Marco Civil and the discussion on personal data protection can serve as a boost, but universities need to reinvent their courses in order to cover the phenomenon in an interdisciplinary manner, and provide more qualified diagnoses to the civil society, promoting more elaborated interventions on the public policy scope.

Intelligence or counterintelligence activities may be necessary to maintain the democratic rule of law, but they cannot be free from public scrutiny. The purpose of the activities should be clear and well-marked, and the legal limits must be respected. Hypertrophy of the sector in the U.S. should serve as a warning: the intelligence community should be at the service of democracy, and not "taking care" of it. The Internet does not need babysitters.

[1] The act n. 8135/13 determines that "the communication of federal public administration's data must be made by telecommunication networks and IT services provided by federal public entities". This is a demand that benefits the Federal Service of Data Processing (SERPRO, in Portuguese), the largest public IT enterprise in Latin America, which "invests in the development of technological solutions in the Free Software area, as a strategic policy". Source: <https://www.serpro.gov.br/conteudo-oserpro/a-empresa-1>.

[2] In the field of electronic communications. The extensive number of scandals concerning mainly the Brazilian intelligence sector, direct descendant of the National Intelligence Service, created during the military dictatorship, is significantly clear. With no clear purpose, the analogic wiretapping can migrate to new technologies. For more on the subject, it is worth reading SNI & ABIN: a reading of the role of the secret services (Rio de Janeiro: Ed. FGV, 2002), by Priscila Brandão and Carlos Antunes, among other works on the Brazilian intelligence community.

[3] Such situations have already been summarized in a text by Eduardo Magrani and Mariana Valente, titled Internet and Democracy: June demonstrations in Brazil, Digital Rights No. 03/2013.

[4] ANTONIALLI, Dennys and BRITO CRUZ, Francisco. The right to know who it is: an empirical analysis of the actions of providing identification data of Internet users in Brazil. Mimeo, 2012. Monograph awarded with the Marco Civil Law and Development of Internet GV Prize.

Surveillance, Human Rights and the role of States: Rousseff's speech and Peña Nieto silence

Renata Avila⁸⁵

Brazil will propose an initiative before the UN for an International “Marco Civil” for the Internet. Other Latin American leaders have joined diplomatic efforts to ensure respect for Human Rights and international law, a rare occasion in which political, diplomatic, and Human Rights agendas in many countries are converging at the same time. Can the region lead the change necessary to prevent the advance of mass surveillance?

The defenselessness of information on foreign citizens and diplomacy as the only answer (so far)

Since April 2013, a series of revelations on the massive and covert surveillance of the National Security Agency of the United States of America have shaken political and diplomatic agendas in Latin America. In September 2013, the conflict escalated to the highest level.

Evidence of spying, not only on the masses, but rather on heads of government of Mexico and Brazil and strategic sectors such as energy-oil (including the Ministry of Energy and Mines of Brazil, even with the complicity of its equivalent in Canada), has forced the mandatory response of these countries to rise to a higher diplomatic and political level, using both regional and international mechanisms.

Resolutions of Mercosul, UNASUR, ALBA, and others presented before the Security Council of the United Nations and the Secretary General of the United Nations in recent months, called for the defense of privacy and sovereignty as well as respect for the rules of public international law which explicitly prohibit behaviors that threaten the enjoyment and exercise of Human Rights. However, the events of September open the door to concrete actions that could result in prosecution and penalties for the governments concerned, once confirmed that the acts of espionage were indeed executed by the National Security Agency of the United States, targeting strategic sectors of Brazil and their highest authorities,

⁸⁵ Renata is the global campaigns manager for the Web We Want initiative of the World Wide Web Foundation.

monitoring every electronic communication of the president-elect of Brazil, Dilma Rousseff, and then the candidate for president of Mexico, Enrique Peña Nieto.

The Charter of the Organization of American States, of which the United States and Canada are members, establishes that international law should be the standard of conduct of the United States in their reciprocal relations and that good faith shall govern relations between the states. The Charter has yet to address these countries' aforementioned violations of the organization's principles, which could lead to their suspension from the Charter.

Rousseff reacted strongly in her speech before the General Assembly of the United Nations, in which she qualified acts of surveillance and espionage as massive affronts to international law, the principles that should govern relations between States, civil rights, and national sovereignty. She described the activities routinely carried out by the NSA as attacks on freedom of expression, democracy and relations between nations.

Opportunity for dialogue and joint action

On the other side are Latin American citizens who, although they have received with sympathy and solidarity the force with which some governments have defended their right to not be monitored by foreign intelligence agencies, know those same governments reserve the prerogative to execute mass domestic surveillance. Low standards of privacy protection in each country and weak or nonexistent data protection authorities are outstanding problems in national agendas. While authorities are objecting mass surveillance by a third State, their citizens are asking that the same restrictions to indiscriminate mass surveillance be applied at home.

The unprecedented understanding of the threat which vigilance poses to everyone has generated a positive effect: proposals for the protection of privacy and petitions for a better accountability of intelligence agencies are being heard by executive and regional parliaments. The "International Principles on the Application of Human Rights to Communications Surveillance", recently presented before the UN Human Rights Council and open to member countries, is an example of the opportunity to promote the highest standards in the region. The establishment of working groups

to study the impact of and possible solutions to mass surveillance, newly installed at ALBA, Mercosul and the UNASUR Security Council, offer another advocacy and outreach opportunity among international experts, promoters of Human Rights, the technical community and civil society to develop the best possible framework, as long political will currently exists, a will that can fade as soon as the news fades from the headlines. The president of Brazil, Dilma Rousseff, has announced through her Twitter account the proposal of the International “Marco Civil” for the Internet, which seeks to protect the rights of all citizens around the world. This proposal would be sent to the UN and would also await the approval of a new version of the “Marco Civil”, which would expand the guarantees of privacy for citizens. Brazil appears to be establishing itself as the country that leads the global response to the war on citizens’ privacy.

The main obstacle to these regional initiatives could be the blockage by a group of countries aligned with this model of surveillance, which may have similar agreements with the NSA and DEA. This is reflected in the silence of Peña Nieto and the lack of a tough response to the revelations of direct espionage in countries dependent on military and police aid to fight the “war on drugs”. It is precisely the citizens of these countries more than anyone else who would benefit from the adoption of a regional and even global mass surveillance protection framework against arbitrary, mass surveillance, which, thus far, violates international and local regulations with impunity. For vulnerable groups, such as journalists and activists in Mexico, Honduras and Colombia, surveillance and protection against it is a matter of life or death.

Most part of the region shows the most favorable legal frameworks for cryptography worldwide. It is a peaceful and young region that confronts the possibility of offering its leaders the chance to stand up for a robust Internet that ensures maximum enjoyment of all rights as well as economic and technological potential, which will lead to greater and better human development even for marginal sectors. It is time to move from protest to proposal and from proposal to action.

[This work was carried out as part of the Cyber Stewards Network with the aid of a grant from the International Development Research Centre, Ottawa, Canada.]

The Snowden case and the Brazilian reaction

Marília Maciel and Luiz Fernando Moncau⁸⁶

The present moment asks for urgent decisions that still have to be well planned otherwise being innocuous or, even worse, delaying national development. To take good decisions, perspectives of different sectors – technical, academic, business and civil society – should be taken into account.

Introduction

All over the world, the revelations made by Edward Snowden about the communication surveillance carried out by the NSA – National Security Agency – not only caused intense discussions but also influenced the governmental agenda.

In Brazil, Snowden’s complaints altered not only the legislative agenda, but also triggered government initiatives whose objective would be to promote more safety to Brazilian communications. In the South American scope, conjunct answers were quickly articulated at the Union of South American Nations (UNASUR) and Southern Common Market (Mercosul) forums. The subject was also taken to the United Nations Security Council by the countries of the region, and there is a desire to expand the discussion to other UN forums, such as the Human Rights Council.

1 Legislative Agenda

As seen in an article published on the last edition of the Digital Rights LAC, one of the more evident impacts of Snowden’s revelations was related to the legislative process of the “Marco Civil da Internet” Bill. The U.S. espionage program brought the media’s and the Congress’ attention to matters such as privacy and communications security. The government’s wish to be portrayed as active and diligent has made him propose modifications to the Bill aiming to reinforce citizens’ privacy and to mitigate the possibility of espionage. However, the proposed modifications do not create significant impact.

One of such modifications, advocated by the Minister of Communications, Paulo Bernardo, was to include in the Marco Civil Bill a provision

⁸⁶ Marília Maciel and Luiz Fernando Moncau are researchers and managers at the Center for Technology and Society (CTS) at FGV Direito Rio.

determining that Internet companies that provide services in Brazil should store Brazilian citizen's data at Brazilian territory. However, it has to be considered that hosting data in Brazil could be far more expensive than hosting it in American servers, for example. The high cost of hardware and backbone access and the smaller broadband coverage in Brazilian territory are some factors that impact the costs. Even Brazilian companies frequently host data abroad.

If the government wishes to retain data in Brazilian territory, the best approach would be to create market incentives through cost reduction. Nevertheless, holding data in Brazil is not a guarantee of safety for at least three reasons. Firstly, hardware of foreign origin might contain backdoors that allow espionage by those who know these weak spots. Secondly, the communications content that navigates thought international infrastructure would remain vulnerable, since there are ways to capture data directly from submarine cable or satellites. And lastly, it is worth considering that data nationally hosted could be subjected to surveillance by actors inside the Brazilian State. It is important to remember that Brazil doesn't have, to present date, a legal instrument that protects privacy and personal data of its citizens.

Despite being problematic and ineffective, everything indicates that the proposal of holding data at the Brazilian territory will be defended by the Federal Government at the Marco Civil voting. President Dilma Rousseff requested, on September 11th, constitutional urgency for the Bill's legislative procedure. As a result, the project should be voted in 45 days at the House of Representatives. Afterwards, the Senate will have 45 days to discuss and vote the approved text. Depending on Dilma's government official position, the Bill that was built collaboratively with society might be transformed.

2 Investments and government programs

Besides the impact on the legislative procedure of the Marco Civil, the Snowden case may affect directly some Brazilian policies related to innovation and to public investment in technology. The developing of national technology has been a major concern of the Brazilian government, which launched medium to long terms incentive programs, such as the "Start-up Brazil". Besides, there are investments in communication infrastructure such as the satellite area and Internet exchange points (IXPs) in South America.

The negative impact of president Dilma Rousseff's communication surveillance, however, made Brazil take urgent, hasty measures, which might have little practical impact. These include the development of a national email service under the responsibility of the Brazilian Company of Mail and Telegraph, one of the biggest state-owned firms in Latin America, which is responsible for the postal services in Brazil. The development of national technology is welcome, but this won't protect Brazilian's privacy while social networks continue to cooperate with the NSA, besides hardware and international infrastructure that allow espionage.

Although there are no solutions of short or medium terms to the spying problem, the development of national platforms could contribute not only to the technological development, but also to encourage the usage of open technologies, that are more transparent and verifiable. This is the case of free software, which allows the analysis of the code and the identification of eventual failures and backdoors. The growing dependence that societies maintain of technology does not consist in the usage of opaque technologies. No one signs an important document without reading it; similarly, we should not base the performance of vital activities in the functioning of software we can neither "read" nor scan.

3 Actions on the international Scope

The actions coordinated on the UNASUR and Mercosul scope, although embryonic, are encouraging. The member states instructed two of UNASUR's councils - the South-American Council of Defense (CDS) and the South-American Council of Defense and Planning (COSIPLAN) - to advance on their respective projects on cybernetic defense and interconnection between optic fiber networks with the objective of making telecommunications safer and promoting the development of regional technology.

At the Mercosul scope, countries approved the "Decision of repulse of espionage by the United States on the region countries", on which they affirm that surveillance consists in a violation of the human right to privacy and to information. This demonstrates that there is political space and will to articulate measures, which is fundamental. The espionage problem cannot be resolved by unilateral decisions, only by conjunct actions that hold greater political weight and can be more fruitful in the point of view of interoperability.

It is still early to know if some of these initiatives of the Brazilian government will take off. The present moment asks for urgent decisions that still have to be well planned otherwise being innocuous or, even worse, delaying national development. To take good decisions, perspectives of different sectors – technical, academic, business and civil society – should be taken into account. This key-moment should favor the fortification of Brazilian multisectoral discussion of subjects related to the Internet, materialized at the Brazilian Internet Steering Committee (CGI.br).

Chilean government to subject Chileans to American surveillance apparatus

Gus Hosein⁸⁷

The economic benefits of being included in the Visa Waiver Program (VWP) with the US are remarkable. The ease of travel allows for the exchange of tourism between the countries and other new economic opportunities through reduced friction caused by visa approval processes. Nonetheless, this program is often used as a mechanism to seek more data on the citizenry of participating countries and Chile's involvement in the VWP places the privacy rights of citizens at risk.

In the past decade, the US Government has used the Visa Waiver Program to place pressure on other governments to hand over data on their citizens to the US Government. A country must meet certain requirements in order to be eligible to participate in the VWP, much of it centering around how data is shared between the two countries. This is problematic given the notoriously low legal protections the US Government provides for this data. US privacy law is amongst the weakest in the world, particularly as immigration and national security are used as exceptions to even basic safeguards. What is most problematic is that US law only protects US persons. Any data sent by the Chilean government would be exempted from the US's weak legal regime. When the US receives data on foreigners it customarily retains this information in its vast databases for 100 years.

Joining the VWP will mean that the United States now has access to significant amount of personal information of Chileans. This raises concerns

⁸⁷ Gus Hosein is executive director at Privacy International.

regarding which Chilean authority would be responsible for deciding and managing information shared with the US, the possibility of the US sharing this data with third parties, as well as arbitrary refusal of access to the US because of potentially erroneous data in Chilean databases. A Chilean citizen who is mistreated on the basis of this data will have no right to redress under US law and his or her data will continue to reside in the US without any real ability to appeal.

The VWP also requires member countries to adopt an 'e-passport'. The establishment of a Chilean 'e-passport' will likely result in the Chilean government establishing a database of biometrics. This includes an individual's fingerprints, names, sex, date and place of birth, nationality and passport number. Potentially, more sensitive data could be included. The lack of a privacy law in Chile means that Chileans have no legal protections to ensure that the data is accurate, that it is not used for other purposes and that is not shared with other departments or governments.

But there are concrete steps that the Chilean government can take to protect the privacy rights of their citizens. First, the Chilean government must limit information sharing with the US authorities. Second, creating a national privacy law would require that any data shared with the US is accurate and would place obligations upon Chilean authorities to provide Chileans with the necessary rights to ensure that their privacy is protected. Third, creating a national privacy commissioner will allow Chileans to appeal for assistance when problems arise, e.g. erroneous data results in Chileans' being repeatedly detained at the US border. Fourth, the Chilean government must seek strong assurances from the US about how their citizens' data will be treated and protected. Finally, Chile needs to review all the personal data held by the government to ensure that its information practices meet international standards to protect against abuses, errors and other related risks to privacy.

While Chile is being offered the opportunity to join an elite club of countries whose citizens may travel to the US without a visa, the Chilean government has failed to seek adequate protections for its citizens. These issues further justify and support the need for the implementation of strong data protection standards to ensure that the Chilean government meets its international legal obligations to protect the privacy of its citizens. By adopting international best practices on the protection of personal information, Chileans could be better protected.

* Privacy International was founded in 1990, is based in England and was the first organization to campaign internationally on privacy issues.

Information collection, location tracking & user awareness

Ellen Marie Nadeau⁸⁸

As companies around the globe are tracking data online, it's important for Latin American users to understand the steps they can take to protect their own privacy.

The past few weeks, articles regarding mobile tracking have been circulating the Internet. New technology connects the tracking of users' mobile app behavior with their web behavior, which impacts user privacy as this wealth of collected personal information is aggregated to produce one all-too-comprehensive view of phone and Internet use.

While this particular technology has received a great deal of attention, it is all-too-common for our mobile phones to collect mass amounts of our data. Other apps don't receive as much publicity as Google, so users generally aren't as familiar with what information is being collected and by whom. This was illustrated in a 2013 study by Carnegie Mellon, which mapped user expectations with privacy and security risks of mobile applications. Out of the most popular 100 Android apps, 56 collect device ID, contact lists and/or location. One of the most shocking was Brightest Flashlight - 95% of study participants were surprised that this app collected such significant amounts of data. The lack of awareness by users shows that there needs to be a significant shift in understanding - especially since the ability to monitor and turn off the tracking settings lies completely in users' hands.

iPhone makes it relatively simple to adjust setting. To learn which apps on an iPhone are tracking location, there's a simple process:

- 1** Open phone's "Settings"
- 2** Go to "General"
- 3** Choose "Background App Refresh"

On this page, one can monitor which apps are tracking user location by looking for a blue arrow next to the application name. Turning off an iPhone's location services will block active tracking. In addition to this,

⁸⁸ Ellen was Google policy fellow at Derechos Digitales.

it's important to disable passive tracking in order to prohibit apps from determining location through connections with Wi-Fi networks.

On any type of phone, privacy policies also appear when one chooses to download a new mobile app. In order to fully understand what information one is sharing, it's imperative to pay close attention to these settings. The US Federal Trade Commission is cracking down on these privacy policies to ensure that they are extremely transparent for users to make well-informed decisions. This is exemplified by the charges FTC brought against "Brightest Flashlight Free" for failing to disclose the extent of tracking and information sharing to consumers; the app developer eventually settled the charges in December 2013. As the FTC takes measures to make certain that privacy policies tell the whole truth, it is up to users to utilize this information.

With this new responsibility comes a great need for awareness and training for users around the globe with respect to their privacy. Users must know what rights they are afforded and how to determine the extent to which certain apps and websites are collecting their information. While there are a plethora of awareness campaigns, most don't focus on these issues. Latin American and Caribbean national awareness campaigns are a prime example of this. In a June 2014 report, the Organization of American States and Symantec explain current awareness campaigns throughout the region. While Belize hosts an annual ICT Road Show to discuss cybersecurity and e-government, among other topics, user privacy is not included. The Dominican Republic's Health Internet campaign aims to keep kids safe and decrease online sexual exploitation, but similarly lacks general user privacy rights education. A greater focus on these issues would help users to utilize the resources available to them, such as privacy policies and location disabling settings, to take greater control of their privacy.

There are users who revel in apps that alert them to nearby sales, offer clothing suggestions made just for them and provide other personalized marketing. If these users choose to allow apps to track their location and activities, that is their prerogative. However, this should most certainly be an active choice. By better educating the general public with regards to privacy rights, they will have the knowledge and interest to utilize existing tools and take greater control of their privacy.

What transparency standards should we demand from States using surveillance technologies?

*Francisco Vera*⁸⁹

The news that Germany sells surveillance technologies without proper licensing to Argentina, Chile and Mexico, reveals the urgent need for putting pressure on the State to balance the comprehensible need for public safety with respect to the Human Rights of its citizens.

Undoubtedly, the biggest news of 2013 was Edward Snowden's revelations about the NSA surveillance of our digital communications. This allowed the public to understand more about the scope and extent of these activities on a global scale, and of the low level protection of our online communications. But these dubious activities of intelligence agencies are not limited to the United States, the case of Latin America also deserves special attention.

A new clue was revealed by a pair of prestigious researchers who analyzed the export regime of surveillance technologies taking place in Germany. Among the most interesting aspects of the article is the fact that the global surveillance technology industry creates between three and five billion dollars a year, that Germany is also increasing its efforts to regulate the export of these technologies and that among the countries that have acquired them, three of them are in Latin America: Argentina, Chile and Mexico.

In figures reported by Der Spiegel, Germany registered exports of 1,2 million euros in surveillance technology to Argentina, 174,000 euros to Chile, and 1,2 million euros to Mexico. However, as stated in the article, the share of these technologies for monitoring use makes up around 20% of the total.

Nevertheless, Germany is not the sole supplier of these surveillance technologies and the sale of these products is not backed with the appropriate licenses from its government. Hence the fact that, for example, FinFisher, one of the technologies that should be subject to export controls in Germany and England, has been found in countries like Mexico and Panama, as shown in a Citizen Lab investigation.

Unfortunately, although most Latin American countries have democratic governments, they have states with streaks of authoritarianism and weak

⁸⁹ Francisco Vera is Derechos Digitales' public policy director.

legal and institutional frameworks regarding Human Rights. This forces defenders and activists who support the right of privacy to place all their attention on these reports about the acquisition of surveillance technology. Why were they purchased? How are these types of purchases regulated? How do they affect the rights of citizens? Many more similar questions could be asked.

Additionally, it is important to consider that discourses on public safety have taken up the agenda in several countries due to drug-related violence in Mexico, guerrillas and paramilitary groups in Colombia or smaller scale domestic terrorism in Chile. This has promoted a series of public policy responses aimed at giving greater powers to the police and intelligence agencies. The new Mexican Telecommunications Act, the PUMA espionage system of Colombia or discussions in Chile about changing its intelligence agency are an example of the new direction of public policies: providing police and intelligence agencies with new powers.

These discussions, however, leave out the pressing need (in addition to the full observance of Human Rights) to improve the current low levels of transparency and accountability, especially in the case of several agencies that are blemished with an authoritarian and undemocratic past. Greater transparency and accountability can determine whether these greater powers will have a positive impact on public safety and whether those powers are being used efficiently.

Thus, it becomes imperative to design systems which oblige agencies that import and use these mechanisms to be made accountable for their use, by taking the following steps:

- **Being transparent about the investments**, the names of the suppliers of the surveillance technologies and their country of origin, in order to have audits to see if the supplier has the necessary export licenses in its country of origin.
- **Implementing import licenses for private companies that wish to use these technologies**, limiting any possible uses which may affect the exercise of Human Rights.
- **Forcing the police and intelligence services to only allow the use of these tools by obtaining the respective court orders**, which in turn must meet the strict standards of Human Rights agencies.
- **Having mechanisms for the accountability of the police and intelligence agencies** which ensure the participation of the government, congress and judiciary in each country, through effective and informed procedures.

- **Posting transparency reports that indicate**, without having to individualize each case, how many surveillance activities were undertaken within a specific period.

The adoption of these measures is the only way to maintain a system that can reasonably balance the demand for public safety with respect to Human Rights. In times like this, where digital surveillance has become a priority for governments and activists, it is essential to adopt public policies that respect Human Rights, ensuring transparency and accountability for these activities in the region.

FinFisher in Mexico: smile, you are still being spied

Pepe Flores⁹⁰

In March 2013, the Citizen Lab of the University of Toronto published the report *For Their Eyes Only: The Commercialization of Digital Spying*. For Mexico, this report marked a turning point: the researchers found the surveillance software FinFisher operating in two telecommunication networks: Iusacell and Uninet (a subsidiary of Telmex).

FinFisher is a surveillance software made by Gamma International, supposedly sold to national security officers. The software is installed in the devices of the supervised person (mobile phone, computer), supplanting a legitimate program. For example, in May 2013, the Mozilla Foundation denounced that FinFisher supplanted the Firefox brand to go unnoticed. Once that FinFisher is installed, it gives the attacker remote control of the device, allowing him to record conversations, access saved files, download contact lists, e-mails, SMS, amongst others. FinFisher can also intervene the camera and microphone of the infected gadget.

These findings mobilized the Mexican activists in 2013 to demand to the Federal Institute of Information Access (INAI, formerly IFAI) to open an investigation, specially because of the suspicion that activists, journalists, and Human Rights defenders were target of this software. Jesús Robles Maloof, lawyer, published the column “Smile, you’re being spied”, on which

⁹⁰ Pepe Flores is the editor of Digital Rights Latin America and The Caribbean bulletin since March 2015. He is the editorial director of FayerWayer and has reported on the FinFisher case in Mexico, since 2013, in different online media.

he points out that FinFisher may have been purchased by the Federal government or a local one – or even by a body of the organized crime.

The revelations incited the deputy Juan Pablo Adame to issue a call to the Federal administration to submit a report about the use of FinFisher in the intelligence collection activities, exhorting both the INAI and the Secretary of the Interior to inquire into the matter. In the same month, members of the *Desobediencia Civil* (Civil Disobedience) group accused to have found traces of the spyware in their cellphones and computers.

However, two years have passed and the uncertainty remains about the government’s accountability regarding the acquisition and use of FinFisher. Recently in April 2015, the Special Commission of Digital Agenda and Information Technologies of the Mexican Congress – presided by Adame himself – hosted a hearing with diverse specialists in the FinFisher issue. In front of the representatives, the organization *SonTusDatos* presented the report “Global Information Society Watch 2014. Communications Surveillance in the Digital Age (GISWatch 2014)”.

During her intervention in the hearing with the Special Commission, Korina Velázquez, member of *SonTusDatos*, emphasized that “Mexico holds the presidency of the Open Government Partnership. In that sense, it would be totally congruent to try to solve some issues like its little transparency and accountability for purchasing and using spyware. It is unknown how much money is spent on what, who is being spied and why”. Nevertheless, the investigation about FinFisher (actually ongoing) has not shown any intentionality from the government in order to clarify the discussed points.

The chapter about Mexico in GISWatch 2014, written by Korina Velázquez, Cédric Laurant and Monserrat Laguna Osorio, shows that a journalistic investigation from the newspaper *Reforma*, published in July 2013, found that *Obses de México* sold FinFisher to the Office of the General Prosecutor (*Procuraduría General de Justicia*) and to other government agencies in the country. IFAI investigated the *Obses* company, which failed to contribute with enough information regarding its transactions, gaining a fine of approximately USD 100.000 for obstruction of the investigation.

The commercialization made by *Obses* contradicts the Gamma International’s supposed politics of no resale. Questioned by Privacy International in the Organization for Economic Cooperation and Development (OCDE) for the purchasing of FinFisher by countries like Bahrain, Gamma International affirmed that they only provide their

services to security forces in sovereign States, arguing that there are nations that use illegitimate copies of the software. However, a posterior leak from WikiLeaks in September 2014 showed that Gamma International is aware of who are distributing their software and their purposes. The leak also notified about a visit from the owners of the company to Mexican government facilities in 2013.

An independent research made by ContingenteMX and Propuesta Cívica found that FinFisher was used in at least four security agencies in Mexico: the Public Security Secretary, the Office of the General Prosecutor, the National Center of Investigation and Security, and the Presidential Guard. Meanwhile, the two companies involved in the Mexican case (Uninet and Iusacell) answered in 2013 that they didn't have servers with FinFisher installed in their datacenter but, as the activist Jacobo Nájera pointed out, the companies did not dismiss the possibility of any of their users doing it. Likewise, the Citizen Lab reported that, at least by September 2013, they had information about FinFisher still running in the monitored networks.

In 2014, between January and June, the lawyers Luis Fernando García and Jesús Robles Maloof made a report about surveillance technologies in Mexico, citing the case of FinFisher, amongst others. "The information obtained through the research has made possible to document a high presumption that the surveillance measures are being used with political purposes against determined groups", they claim in the conclusions of the study. "There are enough hints that surveillance measures are used against Human Rights defenders, activists, and journalists".

Also a piece published in August 2014 in *Reforma*, written by the journalist Martha Martínez (paywalled original and free access) shows that "the illegal intervention of private communications is not a theme present in neither the Federal government nor the Congress agenda" and probably "this is because the espionage is a weapon also used by those who are responsible to sanction this felony".

García and Robles' report also places Mexico amongst the top five buyers of surveillance technologies, showing an increase in the acquisition from Federal and local governments. The document suggests that these methods are being used in at least the states of Chiapas, Coahuila, Quintana Roo, Puebla, Tamaulipas and Veracruz, while the audit of the appropriate use of this software is in question because of the lack of a legal system which allows transparency and accountability. About this, it was also mentioned

in the Congress that “the travels documented in the WikiLeaks filtrations [in 2014] make seem Mexico at the level of Siria, Russia, and China” in comparison with the countries that buy surveillance technologies.

Unfortunately, as exposed in these lines, the FinFisher case makes evident the lack of commitment of the Mexican authorities with the transparency and accountability in the purchase and use of surveillance technologies; specially in the actual Federal administration, whose espionage and privacy violation records promote a reasonable doubt about the illegal use of those tools. Meanwhile, these programs and devices are still in the hands of the governments without any warrant of audit nor any possibility of documenting their abuses. So, two years later since the original denunciation, I close this text with a sad continuation of the Robles’ famous column: Smile, you are still being spied.

Surveillance balloons: how much are we willing to give up in order to feel safer?

Paula Jaramillo⁹¹

That’s the big question behind new surveillance technology implemented by two Santiago City municipalities who are now being questioned for threatening, among other rights, against the neighbors privacy.

“I can imagine, with a chill going down my spine, how clear my room can be seen. Not only during the day, because the camera has night vision too”. Stephanie Söffge is able to perfectly see the aerostatic balloon located mere 90 meters from her home’s window. Since the balloon was installed, she had to change her everyday life: “It has forced me to constantly close my windows and I’m not able to live my everyday tranquil life like I used to, I feel watched 24 hours a day, 7 days a week”.

Söffge suffers the consequences of surveillance aerostatic balloons located in Las Condesas and Lo Barnechea, military technology created in Israel and used on the Gaza strip and in the Mexico-US border. As one can conclude, it is a highly intrusive measure: it posses a 360 degrees camera with night vision and laser pointer, capable of recognize a moving person in a distance of more than 1,5 kilometers, 24 hours a day.

91 NGO Derechos Digitales’ researcher.

By the way, in Chile, the majors of both municipalities had justified their usage to fight delinquency and reinforce vehicular transit surveillance.

This event makes us think that a discussion regarding privacy and safety must be made seriously and not fall under unsubstantiated arguments. Everyone has the right to a safe life. Should be the trespass of our privacy the price we must pay for it?

This serious discussion is essential in our countries, since most of the citizens are not fully aware of the vital importance of the right to privacy, even to the point to exchange it to the bright promise of better security, without noticing, that along with it we are making that our homes and streets transform into a big open ceiling prison, being watch panoptically by strangers whose interests are unknown to us.

In this context, massive and indiscriminate surveillance measures should not be tolerated in a democratic State of law, under the risk of uncontrolled expansion without taking under account fundamental rights that are being hurt. That's the reason why Derechos Digitales, along with two others pro Human Rights organizations in Chile, resorted to a writ of protection from Santiago City's Appeals Court so it can be the legal system can determine, justify and reinforce the fundamental laws implemented.

The surveillance balloons will affect at least three constitutional rights: protection to private life, home inviolability and the right to property. Besides, on the appeal was stated how vulnerable the laws were in regards to personal data handling in Chile and its municipalities, as well as how arbitrary and controversial those measures are.

In this last point, there are concentrated aspects that goes from lack of proportion between the final goal – people's safety and traffic surveillance via cameras that allow recording even inside homes –, to the implicit discrimination that it brings, considering factors such as the ones that make the project pass and even the decision for the location of the devices (according socioeconomic indexes).

This is made worse by the fact that people in charge of the recording are not government officials and are not subject to specific obligations related to their jobs, especially worrying is the fact the absence of a confidentiality clause. It appears that the worst punishment in case of act against fundamental rights of a person is the loss of their jobs, which is clearly not reasonable in comparison.

Public policies to fight against delinquency are an obligation to our authorities, but those policies must also adjust to the legal ruling without attacking our fundamental rights, allowing them to be seriously injured and without punishment. It's time to demand for a serious debate when we talk about security, a debate that allows us to see privacy not as a nuisance but as a space that allow us to freely develop our personality and individuality.

The guardian who watches over the citizens

Fabrizio Scrollini⁹²

In Uruguay, to the surprise of many of its citizens, the purchase of surveillance technologies has also been reported. Once analyzing the scope of these digital tools and seeing the risk of them being used for anti-democratic practices, the authorities' promises of "respecting the usual guarantees" become no longer sufficient.

The news that the Uruguayan government had secretly purchased software for electronic surveillance operations was surprising, but not inexplicable. Public safety has been one of the hottest topics among public debate and the government has made progress in different types of solutions involving technology, which includes video surveillance, software and the use of drones.

"The Guardian" (name of the recently purchased software) allows authorities to analyze real-time telephone calls and emails. It is a powerful technology that, according to the authorities, will be used "with the usual guarantees", i.e. through a warrant. The technology provided by the Brazilian company Digitro had previously been used in Brazil during the World Cup. Uruguayan phone companies have already begun to acquire the equipment for its full implementation. The framework of secrecy that has surrounded this case has prevented the answering of some key questions, such as what kind of protocols will the Uruguayan security agencies follow to implement these policies? What are the institutional arrangements in terms of accountability for those who operate this technology? How will Uruguayan security agencies cooperate with other agencies at international level?

Two factors complicate the answering of these questions: the cloak of secrecy surrounding the operation and the lack of clear regulations. On

⁹² Lead researcher for Iniciativa Latinoamericana para los Datos Abiertos (ILDA).

one hand, the purchase of this tool without any parliamentary control and carried out in secret, at the very least, points towards an improper procedure in a democracy. On the other hand, we find here different types of regulations: data protection, the regulation of intelligence systems and access to public information. There has been no analysis in Uruguay of how this game of regulations establishes clear rules for operating this technology while respecting fundamental Human Rights.

This scenario should in turn be contextualized within the reality of Uruguay: a country generally respectful of the law and Human Rights. Unfortunately, Human Rights in the digital era are little understood by decision makers. An example of this was the recent declaration of the member organizations of the Network of Open Government in Uruguay, opposing a Computer Crimes Act. While the regulation has some aspects that are worthy of consideration, many of the definitions are not clear and in some aspects completely prohibits legal conducts. To date, several civil society organizations that include the DATA, CAINFO and Amnesty International have expressed their concern about the treatment of this topic.

The purchase of The Guardian and the little debate that has followed, demonstrates the need to rethink several public policies on security within the country. Uruguay is now a consolidated democracy but, in the past, authoritarian governments established surveillance systems on civilians without any control. Although that is now part of a distant past, the future that is being built should be geared towards preventing any further abuse. The technology of today allows for the monitoring of the population at a previously inconceivable scale and much more efficient than ever before. The security needs and requirements of a state, in an increasingly complex world where powerful criminal organizations also have access to this technology, are obviously very real. However, the response from the state should be guided by the principles of necessity and proportionality, with respect for Human Rights. For this matter, it is not good enough to mention “the usual guarantees”, but rather to establish adequate regulations and train all the stakeholders (government, civil society, parliamentarians and judges) for the new types of challenges being faced in the digital era.

The arrival of The Guardian and the bill of cybercrime, among other measures, predict a bleak future for digital rights in Uruguay which is part of a trend that seems to be consolidating itself around the continent. Only determined and intelligent actions, which aim towards standards and policies that provide guarantees, together with a civil society with sufficient capacity of control can help to prevent this.

Computer crime: the necessary Human Rights perspective

*Paz Pena Ochoa*⁹³

In a context of increased criminalization of cybercrime, it is time to reflect on how our laws respond harmoniously with respect to the Human Rights of citizens. The conclusions drawn may prove to be more than worrying.

Spam, fraud, child pornography and virtual terrorism, among so many other things. With the development of Internet, computer crimes have become more frequent, sophisticated and, therefore, more important in the public opinion. This has led to several laws around the region being concerned with persecution, even though in many cases they end up damaging other fundamental rights of the rest of the citizens.

The seminar “Computer Crime: New Critical Perspectives”, a joint initiative of the Center for Studies in Information Law (CEDI) of the University of Chile and Derechos Digitales NGO, sought precisely to take a look from this perspective. At the various panel discussions, the conclusions were more than disturbing.

This is, for example, the case of Law 19.223 for Chilean cybercrime, which has been in force since 1993, and that several panelists criticized for its lack of clarity regarding penal types, its vagueness in defining computer rights and ambiguity when distinguishing protected rights, even claiming that the law should be repealed like in the case of Renato Jijena, of the Catholic University of Valparaiso.

For Juan Carlos Lara, director of contents at Derechos Digitales NGO, all these weaknesses of the law are troubling when the persecution of cybercrime is necessary, proportionate and appropriate. As he emphatically pointed out, harmonic and sensible standards are required in regards to the Human Rights and avoid falling into obvious civil rights abuses such as today’s Peruvian cybercrime law.

However, the discussion went further and also touched upon the controversial topic of intellectual property crimes. In this case, the figures are revealing. In Chile, on average there have been two thousand people convicted of piracy in recent years, whereas in the United States, home of the Hollywood film industry which exports high standards of intellectual property protection to the whole world, there have been 20 times fewer, somewhere around fifty convictions a year.

⁹³ Paz Peña is NGO Derechos Digitales’ director of communications.

This apparent imbalance and huge criminalization that continues throughout most Latin American countries, masks an even more disturbing reality for Alberto Cerda, the international affairs director of Derechos Digitales, who believes that the criminal law in the region is used disproportionately under the guise of protecting intellectual property.

According to Cerda, and consistent with other authors such as Joe Karaganis, the underlying problem of piracy is not a criminal matter, but rather a clear market failure. In other words, in Latin America piracy exists because of a lack of service provision, and if there is any at all, it is deficient. Cerda states that “Up until a year and a half ago, an owner of an iPhone or an iPod had no way of legally accessing music. Now, only iTunes has begun providing services around the region, the same can be extrapolated to the case of movies, where Netflix has only recently arrived to this part of the world”.

A similar case occurs with the book industry, because while there may be an availability in the region, they are, however, very expensive and do not consider the disparity of income or levels of development between the countries. Cerda gave the attendees of the seminar an explicit example by pointing out that for an American citizen it costs an hour of work to buy a book, for a Chilean it would cost eight hours and for a Brazilian two days.

But even though there are several evidences pointing towards a market failure as a cause of piracy, the laws and international treaties (including the Trans-Pacific Partnership, TPP) attempt to find a “solution” through the criminalization of the conduct of citizens, using the criminal code in ways that often threaten Human Rights.

In this sense, for Cerda the problems in Latin America are shared by most countries: from behaviors that are too broad to be defined yet considered possible offenses against intellectual property; high criminalization (for laws, for example, the urge to make profit is not relevant for the sentence); those accused of such violations having to prove they are not guilty, rather than the police and judges working on the principle of presumption of innocence; and last but not least, the disproportionality of the penalties for these types of crimes (in countries such as Peru and Colombia, punishments are higher for stealing than for copying).

Despite the many criticisms and new perspectives that were discussed at the seminar, a certain level of uncertainty remained among the audience and panelists when recognizing how certain international treaties could continue forcing non-harmonic laws upon Human Rights.

Without going any further, the imminent entry into force of the TPP in countries like Mexico, Peru and Chile was discussed, which would accentuate all the features of criminalization of intellectual property crimes that were criticized at this meeting, but with an added negative twist: that national Congresses will have limited means of intervention and will have to apply the agreements, through legislation, that will end up being harmful to Human Rights in this regard.

Cybercrime in Brazil

*Omar Kaminski*⁹⁴

In Digital Rights LAC, we asked to different specialists in the region about their personal appraisal in digital rights issues. This is the case of Omar Kaminski from Brazil, to whom we asked which were the main highlights of 2013 with respect to Cybercrimes and what are the biggest concerns for 2014.

Two of the first specific laws about computer criminal offenses came into force in 2013 in Brazil – Law 12.735 and Law 12.737 –, though it should be noted that there were already other sparse provisions applicable to this new reality, including a 1996 law that deals with telematics interception and another law from the year 2000 aimed at cases concerning the Public Administration.

The first law, called as Azeredo Bill, had been discussed for over 10 years and eventually passed with only 2 items of lesser importance, having been challenged as harmful to privacy. And the other one was labeled with the name of a soap opera actress who has had intimate pictures supposedly “leaked” from her mobile. The advance is still small, since the penalties for the crimes are less than the desirable to discourage practices such as hacking systems and disseminating malicious code (viruses), for example.

Just as happened with the actress, the year of 2013 saw several episodes of “sexting” and “revenge porn”, even involving minors, and at least two of these cases have resulted in suicides. Crimes against honor and “phishing scams” still widely performed. Child pornography, another pest, is migrating to the so-called “deep web”.

⁹⁴ Lawyer and consultant on the relationship between law and new technologies, with emphasis on copyright, privacy, information security, freedom of expression and cybercrime.

We live in an era of the evasion of privacy, a dystopia that intensifies progressively along with the fact that our governors also practice crimes against each other, veiled or blatantly. Nations are increasingly concerned about cyber spying, security and the possibility of cyber warfare. And the problem arises when they use the pretext of fighting terrorism to violate individual and collective freedoms.

The challenges of criminal investigations in the age of Internet

*J. Carlos Lara*⁹⁵

Prosecuting crimes often involves the practice of intrusive measures in the sphere of intimacy and privacy of individuals. This fact becomes even more complex when it touches our own personal communications on the Internet. Are Latin America's procedural systems ready to face these challenges?

It is normal for states to chase and prosecute crimes that affect our society or its functioning. This naturally requires obtaining information in order to know what is happening and taking the appropriate measures. However, this search for information may often require measures that affect the interests of people or the gathering of data beyond authorized cases. These interests may be particularly affected in relation to spaces of intimacy or privacy, i.e., criminal investigation may require the execution of intrusive measures.

Intrusive measures can be identified as those permitted in the context of a criminal investigation, which aim to delve into aspects and circumstances within the margins of the private sphere of the accused and of any relevant relationships, to help solve the cases. Thus, it is possible to break the protection of privacy, under certain rules or formalities which are established at a legal level. As an exception, there are also certain scenarios that warrant the implementation of intrusive measures without prior authorization, as in cases of *in fraganti*, under set legal requirements.

⁹⁵ Lawyer, specialist in law of new technologies, focusing on the link between the public interest and the regulation of digital forms of communication.

However, it is not very clear whether our national procedural systems are capable of providing any solutions for such variables which could potentially affect fundamental rights or any other variants. Moreover, if there are such rules, their mere existence does not guarantee that the conditions for gathering information are in any way optimal for safeguarding fundamental rights.

In other words, a likely first question would base itself on the existence of some rules. If these do exist, then a second question would ask whether the rules provide a balanced framework for the infringement of rights, with the intention of finding the truth.

In this effort, it would be worthy to focus the attention on measures relating specifically to the Internet. The reasons are more or less obvious: the more details of our lives that we share on the Internet, the more evidence we leave of the things that we do and are involved in.

This may mean, for example, that plans are being made or information is being sent through email. But from such casual communication, the identity of people or their involvement in criminal acts may be deduced. The content of communications, as well as data regarding time, date, participants and location seem particularly useful for clarifying criminal acts or circumstances. Since it involves personal information, which may include personal data, as well as private or intimate details, access to this would require some special attention. Are our justice systems ready to face these sort of challenges?

In principle, the answer is negative. While Latin American criminal procedure systems tend to establish mechanisms to ensure fundamental rights, such as privacy, the complexities associated with information technology makes it difficult to offer any guarantees.

For example, emails actually fulfill the same function as postal mail, but the procedural mechanisms for seizure may not operate in the same way. In several cases, such as in Argentina or Chile, either by express means or abiding to general rules, the gathering of emails is governed by the same norms as the seizure of postal mail, which means the confiscation of servers or entire units, with very few procedural safeguards for the rest of the information within the equipment.

In other cases, emails are considered a form of private communication, comparable to telephone conversations, thus allowing a similar targeted surveillance intervention. However, it has a broader scope than in the case of telephony, including control mechanisms that are difficult to access.

In other aspects, the information concerning communications between individuals or their visits to websites (i.e., metadata) could also be under observation in a prosecution case and may not only affect personal information but the privacy of the holders of such data.

This is evident in the case of data retention laws of telephone or electronic communications. Thanks to these legal mechanisms, information related to data traffic between individuals or individuals and businesses is stored. Although it could be argued that this collection of information is necessary or at least useful for criminal investigation, collecting all of that metadata necessarily involves tracking the actions of individuals. This not only affects your privacy, but also your freedoms and even the guarantee of due process: monitoring the actions and movements of people, when there is no investigation under way is a violation of the presumption of innocence. In relation to this, the European Court of Justice declared that the EU Directive on data retention compromises Human Rights.

The future outlook in Latin America does not seem encouraging if we review the ongoing efforts. Data retention laws exist in countries like Chile and Colombia (and in Argentina, but by a decree of dubious validity) while in Paraguay there are talks about establishing a system of this nature. The resistance on behalf of civil society has been clear, however the states of the region seem to persist in seeking their means of increasing their capacity for monitoring and control.

For all these reasons, it is necessary not only to put forward evidence on the state of the region, but also to raise awareness across the board regarding the risks of establishing rules for criminal prosecution without a framework for monitoring Human Rights. In the Internet age, this implies an even greater effort to prevent the invasion of privacy. Criminal investigations should not be carried out at the expense of Human Rights.

Cybercrime in Peru

Miguel Morachimo⁹⁶

In Digital Rights LAC, we asked to different specialists in the region about their personal appraisal in digital rights issues. This is the case of Miguel Morachimo of Peru, to whom we asked in what sense the case of cancellation of the Peruvian domain thepiratebay.pe is proof of bad legislations that show lack of understanding of how the Internet works and what rights are at stake?

2013 was a year full of discussions on Internet freedoms in Peru, from the TPP negotiations to cybercrime law, through the pending proposals to filter pornographic content and new exceptions and limitations to copyright. However, perhaps the case that has shown us the fragility of our system is the cancellation of the Peruvian domain name of [The Pirate Bay](http://ThePirateBay.com).

In early December, The Pirate Bay started using a Peruvian domain name (thepiratebay.pe) as the primary address for its site. Only six days later, the Copyright Commission of the National Institute for the Defense of Competition and Intellectual Property (INDECOPI in Spanish) issued *ex officio* a precautionary measure, without any legal proceeding, ordering the Peruvian registrar the cancellation of the domain name. For the Commission was sufficient the fact that in others countries the website administrators have been prosecuted for contributing to infringement of copyright. At no time it was given the opportunity to the affected-service holders to present their case and the precautionary measure was not even notified. There is no news that a procedure for copyright infringement was initiated.

The worst is that all this was done within the Copyright Act. In Peru, an administrative agency can grant precautionary measures ordering the suspension or termination of any means by which it believes that a copyright is being infringing. That means that any website or means of expression online can be suspended without the need for ongoing proceedings or without respecting the rights of defense of the affected. It is not even necessary that someone request it because it can be done *ex parte*. Definitely, a dangerous rule when applied to the Internet and that shows how terribly fragile is our freedom of expression online.

⁹⁶ Miguel Morachimo is director of Hiperderecho NGO.

POSTFACE**CRISTIANO FERRI**

Enjoying the ideas and inquiries of these great minds from the Latin American and Caribbean region was like walking down the pathway that we take to the near future. The texts - which are generally short, objective and direct - deal with real issues in our present day, which roar in our ears every day, provoke reflections to help us consolidate the path towards a new era of reassertion and expansion of Freedom of Expression in the world, empowered by this wonderful innovation known as the Internet.

This work helps us a great deal to dispel the haze of confusion that seems innate to the citizen of the beginning of the 21st Century. We cannot deny the obvious: we are all confused. Moreover, for those who do not feel that way, I invite them to reflect on the quote (thought to be) from Edmund Murphy: "If you're not confused, then you're not paying attention". These texts call attention to several crucial points that govern and will govern our lives from now on.

That is why the chosen macro themes bring very deep and intriguing questions, starting with the protection of privacy, an increasingly expensive right to the new paradigm we live in of overexposure and monitoring from all sides, by corporations, governments or even by our friends, neighbors and acquaintances.

We live constant dilemmas. As we expose ourselves on social networks, exercising our Freedom of Expression in its digital form, we give away information about our personality and behavior. We show tastes, desires and fears. By doing so, we can receive, as a result of our interactions, many positive returns that will improve our lives, our relationships and our careers, which will bring efficiency in some way, including for entertainment and pleasure.

At the same time, we deliver a substantial part of our privacy to companies and governments, which have used such information for a variety of purposes, not yet well known, undeclared, and in many cases violating our privacy. We now begin to see the emergence of new types of villains, or the modernization of old ones: the semi-authoritarian, allegedly democratic state, under the pretext of fighting barbaric crimes, such as terrorism and pedophilia, invades the privacy of the good citizen; Or digital multinational

corporations that sell, for any who want to buy, large sets of data and processed information that detail the segmented behavior of society.

The world of today is a universe of very obvious paradoxes. At first glance, we have more access to information, power of expression and interactivity. As public and private institutions are increasingly exposed, we have the impression of living in a more transparent world, closer to the “truth”. However, everything is intense: a lot of information, interaction and transparency leave us stunned, confused by the relativization of everything, including this “truth”.

One of the paradoxes explored in this book concerns the potentialities and challenges of new forms of free speech on the Internet in the face of the need to preserve people’s privacy. As Carolina Rossini points out, privacy must be one of the pillars of Freedom of Expression and both are fundamental aspects of democracy. Therefore, we can see several examples of concrete cases in progress in Latin America and the Caribbean, with the rich diversity of the social, economic, cultural and political contexts of the region.

Juan Carlos points out, for example, how Chile still lacks regulation to protect personal data. Claudio Ruiz warns about the actions of Latin American governments in this regard. In the absence of privacy protection mechanisms, such governments have promoted dangerous measures for individual freedom, as in the case of Mexico, which included, in the last reform of the telecommunications law, explicit policies for the geolocation of mobile phones without the need for a judicial order.

Miguel Morachimo analyzes episodes in Peru, where state agencies considered illegal the use of public data by third-party websites in order to expose the personal data published in state portals. Morachimo informs us that Peru’s data protection law requires prior consent for the publication of personal data, even when published in public databases. He criticizes how such cases reveal the current distance between the value to be protected by law (privacy) and the reality of its application, since the Peruvian system, in other words, practically prevents the re-use of public information by third parties when it involves personal data.

Here seems to be another clear example where a right, revisited by the 21st Century’s own problematic (the right to privacy in times of the Internet) is “protected” in an old fashioned way, following 20th Century

or centenarian patterns: only the State can guarantee the transparency of public interest data (including public data of the people), and in its own way, which, in the Peruvian case, is based on publication in official journals and filed in public libraries.

One of the most important and effervescent discussions in this work, on the challenges to guarantee Freedom of Expression on the Internet, could be held in accordance with the diversity of the region, starting with the difficulty in “defining” Freedom of Expression, its limits and its violations on the web. Heloisa Padija, Julia Lima and Laura Tresca assist in the mission of characterizing the various types of attacks on this freedom, such as the violation of net neutrality, vigilantism practices and restrictions on the sharing of files and information. Based on research carried out in Brazil, they warn about how death threats and physical attacks on bloggers and journalists have been frequent, as well as possible killings “on account of the network”.

As reported by Eleonora Rabinovich and Atilio Grimani, countless lawsuits have invaded judicial courts in Argentina based on events that expose the tension between Freedom of Expression and protection of privacy. Many of them come from the questioning of celebrities and ordinary people who claim to have their images denigrated by websites, which are mostly just freely aggregated content on the Internet. The challenge of the courts has been to decide between possible limits to Freedom of Expression when faced with other equally essential rights such as respect for privacy and image.

The difficulty is evident in thinking the classical principles of Freedom of Expression in new perspectives, which could expand the possibilities of expression made possible by the internet. In this sense, Eduardo Magrani addresses the issue of the application of basic rules of protection to the person as the right to reply to an offensive quote published on the Internet. The right to a response on TV and radio, media with low interactivity, is generally limited to meeting criteria for responding to offensive comments in the same proportion and time, which is not in line with Internet social networking platforms, where many other variables influence the “Audience”, or rather, the participants involved in that interaction.

Once again, one can notice the attempt of restricted application of old rules to new contexts, affected and complexed by the Internet. This problem

is very critical, therefore legislators, judges and legal practitioners have difficulty understanding and monitoring the complexity of new times and, therefore, adapting their work considering the emergence of new variables.

In addition, the discussion on Internet governance could not be left out of this forum. Although it does not seem obvious to the average user, the rules and principles guaranteeing the functioning of the Internet have a direct impact on how they will be able to exercise their power of expression on the network. Carolina Rossini explores the Brazilian case of the manifest displeasure of the then President of the Republic, Dilma Rousseff, regarding the sophisticated espionage methodology revealed by Snowden through the action of the American agency NSA.

From this example, Rossini reflects on the possibility of countries with substantial resources - such as Brazil - to invest in their own Internet infrastructure, thus reducing dependence on US infrastructure. In addition, it emphasizes how new internal regulations can make a positive contribution to the protection of users, such as the famous example of the Civil Internet Framework in Brazil, which embodies substantial principles for free Internet, such as net neutrality.

In this work, therefore, there is room for in-depth reflection on the essential elements that affect the Latin American and Caribbean citizens not only in the way they access the Internet, but also in the minimally necessary requirements to access it. Camilo Córdova uses the example of Bolivia to show the impact of economic and social factors on the right of access to the Internet in poorer countries. The lack of minimal Internet regulation, according to Cordoba, significantly undermines the dream of universal access of the Bolivian people to the Internet. In addition to the difficulties of access for economic reasons, Cláudio draws attention to exclusions by speed and coverage, common practice in Bolivia.

Allan Rocha de Souza explores another relevant macro-issue in this book, which also demands new regulation: copyright. Allan shows us, in a very enlightening and synthetic way, how the regulation of authorship rights has been dealt with since the Renaissance until the present day, with a special focus on contemporary dilemmas.

He describes how the cultural industry has achieved partial success by passing prohibitive laws and sparse judicial decisions. However, he points out that this antagonizes the reality of today's world where citizens feel

empowered to produce, mix, remix, diffuse and use creations. To this end, they often choose not to comply with formal laws, which, according to him, would be socially illegitimate because they do not express important aspects of significant portions of society, such as their relentless craving for new content.

It is intriguing to note how this debate has been carried out quite heatedly in the region, with similar challenges between countries, although each country has very particular contingencies. A symbolic example of this process is the one given by Jorge Gemetto when reporting movement #noal218 in Uruguay. Activists pro-flexibilization of copyright organized a strong movement in digital social networks in the country, managing to prevent a legislative amendment that extended the term of validity of copyrights in the region. The challenge of our time is therefore to find a new balance between copyright, Freedom of Expression and access to information.

Speaking of digital activism, we could observe how some authors referred to new forms of social mobilization in Internet networks. If in the copyright debate the ways in which contemporary society develops more open rules that stimulate the production and reuse of objects of human creation, in order to reduce the cost of production, mixing and distribution of content, we also perceive the effects of the drastic reduction of social mobilization costs on the Internet.

Organizing a network for a specific political or social purpose has been shown to be fully viable today with the instruments available on the Internet, especially on social networking platforms. Such movements begin to have an effect on political decision-making. Miguel Lago emphasizes the growing impact of so-called “couch activism”. He cites the example of Meu Rio as a project that proved effective in forming and agitating networks for purposes of social influence in the decisions of the state bodies of the city of Rio de Janeiro, in Brazil.

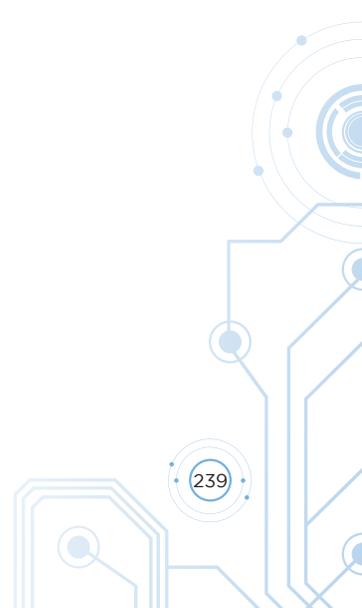
On the other hand and concomitantly, this phenomenon has brought new surveillance practices by the public security system. One of the current concerns of the police, in the words of Francisco Vera and Paz Peña, is to monitor how online mobilizations reverberate in protests of great proportions in the streets, which, for this reason, can generate social disorder.

Valentina Hernández cites the case of the Chilean police who confirmed that they had purchased the Phantom software for monitoring and surveillance of Internet users. Through this technology, the Chilean police would be able to collect emails, access files and connect the camera and microphone of users' computers. The Mexican government has also been accused of doing something similar, through FinFisher software, as described by Pepe Flores.

And that's where we get into other sensitive issues. What are the limits of security forces to investigate possible cybercrimes? What are cybercrimes? How do investigative methods of the security forces violate fundamental rights, such as Freedom of Expression and privacy?

In summary, the selected articles contained in the book "Digital Rights: Latin America and the Caribbean", edited and organized by Eduardo Magrani, present us with the current picture of difficult and intense times with controversial, polemic and complex dilemmas. The writings are glimpses that bring light to what is happening around us. They allow us to better understand how the various issues and problems being discussed in the region take place in the richness of the variety of their contexts. Yes, we live in confusing times. But as A. Einstein would say, confusion can be a state of preparation for change, a change that is necessary for our era: "In the midst of confusion, find simplicity. From the discord, find harmony. In the middle of the difficulty lies opportunity".

Cristiano Ferri Soares de Faria holds a PhD in political science and sociology from the Rio de Janeiro State University, a Master's in Public Policy from Queen Mary College and is an associate researcher at the Ash Center for Democratic Governance and Innovation at Harvard University. He is currently the Coordinator and founder of the Hacker Laboratory of the House of Representatives in Brazil, working with projects of open innovation, transparency and digital democracy.



ABOUT THE EDITOR



Eduardo Magrani has been working with public policy, Internet regulation and Intellectual Property since 2008. He is Professor of “Law and Technology” and “Intellectual Property” at FGV Law School. Researcher and Project Leader at FGV in the Center for Technology & Society since 2010. Author of the book “Connected Democracy” (2014) in which he discusses the ways and challenges to improve the democratic system through technology. He is Senior Fellow at the Alexander von Humboldt Institute for Internet and Society in Berlin. Associated Researcher at the Law Schools Global League and Member of the Global Network of Internet & Society Research Centers. Master of Philosophy (M.Phil.) in Law and Ph.D. Candidate in Constitutional Law at Pontifical Catholic University of Rio de Janeiro with a thesis on Internet of Things’ Regulation through the lenses of Privacy Protection and Ethics. Bachelor of Laws at the Pontifical Catholic University of Rio de Janeiro, with academic exchange at the University of Coimbra (Portugal) and Université Stendhal-Grenoble 3 (France). Lawyer since 2010, acting actively on Digital Rights, Corporate Law and Intellectual Property fields. Magrani has been strongly engaged in the discussions about Internet regulation that led to the enactment of Brazil’s first comprehensive Internet legislation: the Brazilian Civil Rights Framework for the Internet (“Marco Civil da Internet”). Eduardo has coordinated at FGV the Access to Knowledge Brazil Project, as project Manager, participating and interested in the copyright reform and Internet regulation policies in Brazil. He is coordinator of Creative Commons Brazil and the Digital Rights: Latin America and the Caribbean Project, alongside with prestigious Latin American organizations.

This book was produced by FGV Direito Rio, composed with the font family Gotham, in 2017.

DIGITAL RIGHTS: LATIN AMERICA AND THE CARIBBEAN

The Internet is a decentralized global network that makes communication, information and learning easier. Basic democratic practices, such as discussing matters of public interest and participating in the political process, will be increasingly related to the digital world. This publication presents an overview of the most relevant issues in the area of Digital Law in Latin American countries, as a result of the Project “Digital Rights: Latin America and the Caribbean”, an International Newsletter coordinated in Brazil by Professor and Researcher of FGV, Eduardo Magrani. The project emerged in 2012 as an initiative of leading Latin American think tanks working on issues related to Internet regulation and governance interested in consolidating Human Rights in the digital world. The regulation of net neutrality, the regulation of copyright and the responsibility of intermediaries, restrictions on freedom of expression by electronic means and data protection policies are some of the themes that can be found in this work of selected articles. Being informed about these subjects is a fundamental requirement for promoting dialogue and consensus around these issues. This publication is intended to be a useful tool for a broad community of stakeholders interested in the Digital Law landscape in Latin America.

Agência Brasileira do ISBN

ISBN 978-85-63265-85-2



9 788563 265852