Lawful and unlawful surveillance in Mexican democracy

Vigilancia legal e ilegal en la democracia mexicana

■ **Diego Rivas y Chiara Mantovani**

Universidad Autónoma de Baja California (México) y Universidad Cetys (México)

NOTAS BIOGRÁFICAS

Diego Alfredo Pérez Rivas is full-time research professor at the Universidad Autónoma de Baja California. Bachelor's degree in Political Sciences at the National Autonomous University of Mexico (UNAM), Master of Law at the University of Salamanca (Spain), PhD in Philosphy at the Universidad Complutense (Spain), and postdoctorate in Philosophy at the University of Turin (Italy). Member of the National System of Researchers (SNI), category I. Research areas: political philosophy, theory of law and philosophy of science, as well as human rights and democracy.

Contacto: diego.alfredo.perez.rivas@uabc.edu.mx.

Chiara Mantovani is a lecturer at the Deparment of International Business of Cetys University (campus Ensenada). Bachelor's degree in Modern Languages at the University of Verona (Italy) and Master of Science in International Public Policy at University College London-UCL (UK). Research areas: impact of public policies, gender theories, philosophies and policies, as well as international economy and international marketing.

Contacto: chiara.mantovani@uclmail.net

Abstract

With the access to always more sophisticated and technologically advanced surveillance tools, it is crucial to develop progressive legislation to safeguard human rights and to ensure governments do not abuse their power by engaging in excessive state surveillance. This article investigates the use governments give to these surveillance instruments, focusing on Mexico. Firstly, we offer an overview of recent cases exposing governments' use of mass surveillance to repress critics. Secondly, we analyze what legislation is in place for data protection and privacy in some countries and how authoritarian governments employ surveillance methods to control their citizens. Thirdly, the Mexican legislation about data protection and access is presented. Fourthly, we describe how the Mexican authorities employ unlawful surveillance methods against critics with the complicity of telecommunications companies. Finally, we propose a few reforms to strengthen data and privacy protection in Mexico.

Resumen

Con la existencia de herramientas cada vez más sofisticadas y tecnológicamente más avanzadas resulta fundamental desarrollar leyes para defender los derechos humanos y asegurar que los gobiernos no abusen de su poder aplicando una vigilancia estatal excesiva. Este artículo investiga el uso que los gobiernos hacen de estos instrumentos con un enfoque especial sobre México. En primer lugar, se presentan algunos casos recientes que ilustran el uso de la vigilancia masiva por parte de ciertos gobiernos para reprimir sus críticos. Después, se analiza las leyes existentes en materia de protección de datos y privacidad en algunos países ilustrando cómo los gobiernos autoritarios utilizan métodos de vigilancia para controlar a sus ciudada-

nos. En tercer lugar, se describe la legislación mexicana sobre la protección de datos y el acceso a estos. En cuarto lugar, se explica cómo las autoridades mexicanas emplean métodos de vigilancia ilegal en contra de sus críticos, con la complicidad de las compañías de telecomunicación. Finalmente, se proponen algunas reformas con el objetivo de fortalecer la protección de datos y privacidad en México.

Keywords
Mexico, surveillance, metadata, privacy, data protectio

Palabras clave
México, vigilancia, metadatos, privacidad, protección de datos

Sumario

Contents

© 2017. *Revista Internacional de Comunicación y Desarrollo, 7*, 111-129, ISSN e2386-3730

A specter is haunting the world at the beginning of the XXI century: the specter of mass surveillance. Some of the political and economic forces born within the democracy have united their efforts to justify and legalize this specter. Telecommunication firms, web companies, opponents to privacy and civil rights, nationalists and national security paranoids have being engaging in harsh confrontations with the goal of establishing technological systems able to obliterate some fundamental rights of the democracy. Modeled on the surveillance systems adopted in authoritarian regimes, the new surveillance mechanisms implemented by some democracies have been, in some cases, made legal and in other cases have been used at the edges of the law.

On one hand, the value assigned to the data collected, organized and analyzed by telecommunication and web companies, has driven the idea that the opening of this market can generate wealth. On the other hand, the potential political use of this information in limiting or harming civil rights, gives rise to concern about the undesirable consequences deriving from the legalization of this market. Data storage and the free trade of data on the web are economic issues with relevant political implications, such as the right to privacy, the right to free speech, to free thinking and even to the presumption of innocence.

Currently, technology allows for the creation of intelligent algorithms able to analyze a great amount of data (big data). This data can be used in a variety of situations. It can be applied for the creation of targeted marketing strategies, in order to measure individuals´ behaviors regarding their beliefs and opinions, or for the elaboration of complex relations between a consumer group and voters. However, it can be also used to spy and monitor in real time.

What ethical and legal ramifications do these actions generate? How can they transform democracy? What type of lawful and unlawful tools are being used to implement this surveillance? These are some of the questions we will try to answer in this paper, with a focus on the Mexican case.

1. OVERVIEW

In April 2008, one of the first protests organized thorough a social network (Facebook) took place in Cairo (Egypt) against Mubarak government. Different media soon informed their audiences that the protest organizers had been localized by public officials thanks to the databases of the social network used to promote the protest (Farouk, 2012).

The administrators of the ¨April 6 Movement¨ Facebook group were tortured. In 2001, a manual used to organize the Egyptian revolution advised against using Twitter or Facebook to disseminate information due to the potential risks to the dissidents. Mubarak would very soon implement censorship and persecution policies in the web (Assange, 2013).

The events in Egypt started a debate that is still ongoing. On one hand, social networks played a crucial role in the organization of protests and civil demonstrations, and helped to strengthen the democratic mechanisms for the expression of ideas and for free association. The synchronized use of these technologies made possible for people from very different backgrounds to organize themselves and to create strategies aimed at fighting poor governance and state oppression. On the other hand however, these technologies facilitated the localization of the citizens taking part in the protests, highlighting the dangers of indiscriminate state access to this web-generated information.

These new technologies were a double-edged weapon. They could be used as an apt instrument for social organization and democracy, but they could also function as a repressive tool in the hands of governments hostile to the respect of human rights. In this way, under the pretense of protecting national security, the protesters' privacy and civil rights were violated.

In 2010, WikiLeaks revealed a series of classified governmental cables (*Collateral Murder, War Logs* and *Cablegate*) with the purpose of denouncing the systematic abuse carried out by the US army and government during a number of military actions (Bumiller, 2010). The Obama administration reacted by organizing a legal-political campaign to silence WikiLeaks. On the legal front, a grand jury composed by the Ministry of Justice and the FBI was created in order to determine if Assange could be prosecuted for conspiracy, on the basis of the 1917 Espionage Act. Among the strategies used against his person, according to Assange, there are murder instigation, direct censorship, freezing of his bank ac-

count, the persecution of his associates and the seizure of electronic equipment (Assange, 2013).

In this specific case, the dilemma between national security and transparency was resolved in favor of the State secret since the topics discussed were considered sensitive. Evidently, state surveillance is the true winner of this battle, which favored the creation of a new public enemy figure inside the collective imagination, i.e. a person whose crime is making public information that should not be considered classified nor dangerous under any political reason. Nevertheless, the real scandal had yet to happen.

In June 2013, the newspapers *The Washington Post* and *The Guardian* published a series of documents leaked by Edward Snowden with information on the massive espionage programs established by the US and its allies through the use of sophisticated systems such as *Tempora, PRISM, Xkeyscore* (Stöcker and Lischka, 2013). Similarly to Assange, the ex NSA tech consultant was accused of espionage for leaking documents considered of national security relevance. At present, Snowden is a political refugee in Russia. In this specific case, these leaked documents revealed the most hideous side of the antiterrorism policies established after the events of 9/11. As Rodríguez Prieto and Martínez Cabezudo (2016, pp. 132-133) affirm, Snowden's case exemplify how governments and corporations may give a fraudulent and dangerous use to technological advances in order to invade a person's privacy, exploiting the disciplinary and repressive possibilities offered by Internet.

On behalf of national security, the privacy of millions of people worldwide has been systematically violated through the use of IT systems able to process great databases for espionage purposes. The moral and political argument in support of these actions derives from the incessant and ongoing war against terrorism. In other words, national security triumphs over privacy.

1.1 METADATA

In the Dublin Core Metadata Initiative FAQ[1], metadata are defined consequently as "structured data about data". Metadata are a type of data that help the IT systems to classify and give meaning to the resources that are used to classify information. One of their main purposes is to help the system user, be it a person or a program, to access specific data without the need to consult each record.

Today we are used to interacting with apparently free digital services offered by various communication and web companies. Seduced by the apparently cost-free element of these digital services, users do not reflect usually on their real nature. In reality, data and metadata are the real goods being produced through these services, while the users is converted into a consumer of the product. This Copernican turn is possible thanks to the storage and management of the personal data on the web. Companies offer their services in exchange for a nearly complete access to all data provided by the user. It is in truth a commercial transaction between the companies' services and the users' personal information.

In our interactions with the available digital technologies, we generate a *digital fingerprint* that can be used to identify us through the analysis of the electronic devices we use to surf the web. The metadata that users generate in their interactions with their devices and the web are the language in which the digital fingerprint is written. This digital fingerprint is a personal users' record obtained by storing and analyzing data on the devices with Internet connection and their IPs about users' interactions with other users and with other systems, including photos, written and audio messages, emails, online shopping, location, personal communications, calendar, biometric data, search history, likes, cookies, etc.

In this sense, Rodríguez Prieto and Martínez Cabezudo (2016, pp. 135-138) introduced the concept of *linkdomination*, which is a type of domination based on the way information about ourselves is obtained thanks to our digital fingerprint. As such, state or corporation powers are able to intrude into our intimate sphere with just a click. In this way, governments and business world establish a cooperation that is not aimed at satisfying the necessities of the majority of citizens.

In this context it is crucial to ask: how is this information managed? Is it only used for ''legitimate advertising purposes'' or could its analysis with certain techniques constitute an invasion of privacy and personal freedom? Is the information provided only for the

[1] Full text available at: http://dublincore.org/resources/faq/

© 2017. *Revista Internacional de Comunicación y Desarrollo, 7*, 111-129, ISSN e2386-3730

commercial use of the companies, or could it be collected and analyzed by governmental agencies too? In the immediate future, will an information market arise in which sensitive data will be openly traded or will we witness instead the creation of a black market? What rules should prevail?

A number of recent studies have highlighted the great potentiality of the algorithms applied to metadata analysis, and have suggested a possible route to follow. A study by Kosinski-Stillwell-Graepel (2012) published in the *Proceedings of the National Academy of Sciences of the United States of America*, demonstrated that the likes we give on the social networks reveal sensitive data about our tastes and preferences with regard to sexuality, politics, religion and civil status. As such, these intelligent algorithms are able to know, via indirect ways, sensitive data on the individuals. A detailed analysis of users' interactions with Facebook content allows to identify with great accuracy their personal preferences.

Another investigation by Youyou-Kosinski-Stillwell (2014) has revealed that an algorithm is able to calculate the personality of an user better than a work colleague through the analysis of only 10 likes, while with 150 likes the algorithm creates a description more detailed than the user's siblings or parents. These algorithms are thus able to classify users and to predict their behaviors or to influence their perceptions. As such, they may be considered as potential technological risks. Hence, it is evident that these tools should not be entrusted in the hands of antidemocratic regimes or companies that violate the fundamental rights of their users.

In the near future, the development of new technological instruments will greatly extend the uses we can give to the information obtained through data and metadata analysis. In some specific cases, this information will provide not only personal data, but also accurate personality descriptions and predictions on our behaviors and on opinion trends. Numerous ethical and juridical issues arise from this situation. Probably, one of the most relevant issue consists in defining the ownership and legitimate uses of this data, to avoid their use in actions that harm the freedom and fundamental rights of people.

2. INTERNATIONAL CONTEXT

In order to evaluate Mexico's legislation and its government's legitimacy in the use of personal data and surveillance systems, it is relevant to insert Mexico case in the broader international context. In this section, we will present an overview of the laws and surveillance systems as applied by other countries. Firstly, we will analyze the cases of Iceland, Estonia and Finland, considered champions of data and privacy protection, and secondly we will focus on increasingly less democratic systems, which engage in legal and illegal mass surveillance to spy on their opponents or to control their citizens: Colombia, Venezuela, Turkey, Iran and China. With the aim to contextualize on a global scale the countries presented, we will use as a guide the *Freedom on the Net Index 2016* (FOTN), developed by the independent watchdog organization *Freedom House*. The index gives information on 65 countries worldwide and assess citizens' degree of freedom in accessing and using internet, by evaluating the obstacles to access, the limits or censorship imposed to web content and the violations of users' rights by the national governments. The scoring system goes from 0 (most free) to 100 (least free). This overview will be then useful to compare Mexico with these nations and uncover the similarities or differences in terms of data protection laws and of the application of mass surveillance and other monitoring systems.

In general, the report on the *Freedom of the Net* has found that Internet freedom has declined for the sixth consecutive year worldwide. In particular, social media and communications apps are being targeted by governments, as they are a rapid and secure way to disseminate information and are increasingly becoming the main communication tool used during anti-government protests, due to their encryption features which make obtaining data on users and content very difficult. As such, authoritarian governments are increasing their pressure on service providers to reveal users´ information, as well as using the content published on these social media to monitor and arrest critics and dissidents.

The report finds that in order to increase their control on their citizens and on these media, a number of governments, both democratic and nondemocratic, have passed laws

that reduce privacy and that allow for broader surveillance. Authoritarian nations are specifically using antiterrorism and national security laws to persecute individuals and organizations for writing about democracy, religion or human rights (Freedom House, 2016).

However, there are other countries that go against this trend. Both Iceland and Estonia, for example, have put in place strong legislation to ensure the protection of personal data and to increase the accountability of service providers and data controllers. Iceland leads with Estonia the FONT ranking with a score of 6, as one of the countries with the highest rate of internet access and the smallest violations of user rights

2.1 ICELAND

Data protection in Iceland is regulated by three main pieces of legislation: the *Data Protection Act* (2000), *the Rules on Electronic Surveillance* (2007), and the *Media Act* (2011). With the *Rules on Electronic Surveillance*, Iceland has implemented well-defined regulations to limit electronic surveillance in the workplace, in schools, and in other areas traversed by a limited number of people, and to protect individuals' privacy also when under surveillance. Surveillance is only allowed under court order, may be carried out only for explicit and legitimate reasons and must be proportional, in order to avoid excessive surveillance, and only if other, reasonable, and less intrusive means are not available to reach the same objectives.

The *Media Act* is a legislation of great relevancy created with the specific purpose of protecting the freedom of the press, both printed and online, by establishing legal protections for journalists and their anonymous sources, as well as for their editorial independence from media service providers' owners. As stated in article 1:

> ''The objective of this Act is to promote freedom of expression, freedom of information, media literacy, diversity and pluralism in media and to enhance consumer protection in this area. A further objective of the Act is to establish a coordinated regulatory framework for media services irrespective of the type of media employed''

Iceland government's commitment to preserving freedom of speech and to protecting personal data is made evident by the numerous policies and initiatives undertaken in last few years, of which the *Modern Media Initiative*, and the subsequent creation of the *Modern Media Initiative Institute*, is one of the most important. In 2010, still reeling from the 2008 financial crisis and as a response to the witch hunt surrounding the whistleblower website WikiLeaks, the parliament unanimously passed a resolution on modern media aimed at making Iceland a safe haven with legal protection for journalists, bloggers and whistleblowers from all over the world (Freedom House, 2016).

2.2 ESTONIA

Estonia ranks as the freest country in terms of Internet access and data protection along with Iceland. In the last years it has undertaken reforms to increase its internet penetration rate and to transform its society in one of the most technologically advanced in the world (Freedom House, 2016). Estonia has implemented strong privacy protections and the right to privacy is enshrined in its Constitution (1992) in art. 26 as follows:

> ''Everyone is entitled to inviolability of his or her private and family life. Government agencies, local authorities, and their officials may not interfere with any person's private or family life, except in the cases and pursuant to a procedure provided by law to protect public health, public morality, public order or the rights and freedoms of others, to prevent a criminal offense, or to apprehend the offender''.

Moreover, the offense of violation of confidentiality of messages and the illegal disclosure of sensitive personal data and illegal use of another person's identity are sanctioned under the articles 156 and 157 of the Estonian Penal Code. The main piece of legislation concerning data protection is the *Personal Data Protection Act 2007* (PDPA), which implemented the EU Data Protection Directive 95/46 EC. Under this act, personal information considered sensitive, such as political opinions, religious or philosophical beliefs, ethnic or racial origin, sexual behavior, health, or criminal convictions, cannot be processed without the consent of the individual (Norton Rose Fullbright, 2014).

The *Criminal Procedure Code 2004* esta-

© 2017. *Revista Internacional de Comunicación y Desarrollo, 7*, 111-129, ISSN e2386-3730

blishes the requirement of a court order for ''wire-tapping'' during criminal investigations, which can be permitted for up to two months, with a renewal option. Surveillance for intelligence and counter-intelligence is instead regulated by the *Security Authorities Act 2001.* According to this law, acts that restrict the right to confidentiality of messages and to inviolability of home, family and private life as guaranteed under the Constitution can only be undertaken by the designated security authorities (the Estonian Internal Security Service and Information Board) and only to ensure national security and constitutional order. Such acts need a court authorization and are permitted for up to two months for the same period at a time. In any case, the citizen whose rights are restricted must be notified of the implementation of such measures (Privacy International, 2016).

Finally, the *Electronic Communications Act 2015* establishes the conditions for the interceptions of communications and access to data stored on communication networks by intelligence agencies or other authorities. Furthermore, Estonia created a parliamentary committee in charge of overseeing the surveillance actions and practices carried out by the security agencies, the Parliament Security Authorities Surveillance Select Committee (Privacy International, 2016).

Even though Estonia has one of the most advanced privacy protection regulations in place, some concerns have been raised concerning data retention practices in the country. *The Electronic Communications Act* requires Internet and telecommunications providers to retain a wide variety of communication metadata for one year, which carry information on the source, destination, time, duration and location of the communication. In 2014 the Court of Justice of the European Union (CJEU) found Estonia in contravention to the right to privacy and personal data protection as enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights, nevertheless to this day Estonia has not made any changes to its data retention provisions (Privacy International, 2016).

2.3 FINLAND

Finland represents an interesting case of a democratic country considering limiting the privacy of its citizens. Even though it is not assessed in the FOTN, Finland is one of the countries with the strongest privacy and users protection laws in place worldwide. However, at the moment, the Finnish parliament is discussing a relevant legislation that will go against the current privacy law, by considerably expanding the surveillance powers granted to the military and the national intelligence service.

In terms of privacy legislation, Finland, besides stating the right to privacy in its Constitution, has developed two central piece of legislation on the topic of data protection and monitoring: the *Personal Data Act 1999* and the *Information Society Code 2014*, which updated and incorporated ten existing laws into one. The first act set the legal framework for personal data protection, defining the data collector's legal responsibilities in ensuring data privacy, and sets the right for the individual to consult, update, rectify, or eliminate the data collected about themselves.

In the *Information Society Code*, the scope for data security and protection is extended to include entities that operate outside of Finland, but that use devices to communicate with the country, or provide online services for Finnish users. The *Code* also establishes protective measure for the users and for Net Neutrality, this means that Internet services may be restricted only under specific circumstances, and that all data on the Internet must be treated equally, and that nor priorities nor benefits can be applied to data traffic, which must flow without any discrimination based on user, content, website or platform, etc. (Rodríguez Prieto, Martínez Cabezudo, 2016, p. 127).

Finally, with regards to the user privacy, the *Code* introduces the new concept on ''intermediary''. All service providers for electronic communications are considered an intermediary, and as such are responsible for guaranteeing the confidentiality of communications and data, including communications that take place outside public communication networks. For example, instant messaging applications and social networks are considered, under this extended definition, as intermediaries.

In terms of Internet surveillance, Finland is currently discussing a legislative proposal which, if approved by the parliament, will give to the national security intelligence services broader power in intercepting online data for

military and civilian intelligence purposes, even without the suspicion of a crime being committed. This proposal has been denounced by the Finnish association Electronic Frontier Finland, member of EDRi (European Digital Rights organization), as being a worrisome step towards the debilitation of the constitutional protection of the secrecy of communications, and which may open way to unprecedented mass surveillance programs (EDRi, 2015).

2.4 COLOMBIA

Among the countries classified as partly free we find Colombia, with a score of 32. Even though the FOTN report finds that internet freedom has increased in Colombia, concerns are raised over excessive and illegal surveillance by the state. In terms of legislation, the article 15 of the Colombia Constitution (2005) establishes the rights to privacy, good name or reputation and data protection.

Two major acts supplement the content of this constitutional article on data protection and processing by public or private entities: the *Law 1581* of 2012 and the *Decree 1377* of 2013. The first text articulates comprehensive personal data protection regulations concerning personal data stored in any private or public databases. The owner of the data must give prior informed consent to any use given to their personal data, including their collection and transfer. These rules apply also to data collectors not located in Colombia, but that are subject to the Colombian jurisdiction under international standards and treaties (Norton Rose Fullbright, 2014).

The *Decree* 1377 is a secondary regulation on data protection and regulates the forms in which data subjects' consent may be obtained, the rights for data subjects' to access, update, rectify, suppress and revoke their authorization, the processing of sensitive data, the obligation for data controllers to implement a personal data processing policy and notices, and the transfer and transmission of personal data to third parties and abroad (Rodriguez, 2013).

Despite these regulations, Colombia maintains to this day criminal penalties for defamation, which include incarceration and heavy fines, and which have been used against online speech and as an intimidation tool against journalists and bloggers (Freedom House, 2016).

Notwithstanding the privacy protection rules in place, Colombia's record on privacy, surveillance and human rights has recently come under scrutiny of the United Nations, impulsed by fresh scandals on illegal spying involving the National Police and which has led to the resignation of the Chief of the National Police (Rice, 2016). The organization *Privacy International* published in 2015 a study on the mass surveillance system put in place by the Colombian government to monitor its citizens' communications in the last twenty years, in which it highlights serious issues in terms of unchecked and excessive application of surveillance, and of system vulnerabilities that make it susceptible to abuse (Privacy international, 2015).

The report identifies three mass surveillance systems used by various state agencies, able to intercept and collect data on hundreds of millions of phone and internet communications (audio and written) in an automatic way by being connected to the nation's telecommunications operators: *Esperanza, PUMA* (Single Monitoring and Analysis Platform) and the *IRS* (Integrated Recording System). Especially *PUMA* and the *IRS* are found to be used ''either unlawfully or with dubious legal justification'' (Privacy International, 2015, p. 8).

Finally, it is crucial to highlight that the Colombian law does not authorize this type of mass and automated surveillance made possible by systems such as *PUMA* and the *IRS*. As such the report concludes that in Colombia some state agencies are secretly building their own surveillance systems without sufficient scrutiny and without lawful basis (Privacy international, 2015).

2.5 VENEZUELA

Venezuela is classified as 'partially free' as well with a score of 60. Freedom of the internet has been increasingly diminishing in this country, especially due to the deteriorating economic and political situation. According to FOTN, it is on the verge of being classified as a 'not free' country in terms of access to the internet and users' privacy protection.

Venezuela does not have a general legislation regulating data protection nor any authority in charge of this protection, but general principles can be find in its Constitution (2009). The Constitution offer a framework

© 2017. *Revista Internacional de Comunicación y Desarrollo, 7*, 111-129, ISSN e2386-3730

for data protection by safeguarding the honor, the private life and intimacy, and reputation of people. In particular, article 28 states the right to access, update rectify or destroy personal data.

Venezuela's legislative efforts seem directed, however, to limit freedom of speech and to control online content. With the amendment to the *Law on Social Responsibility in Radio, Television and Electronic Media* of 2010, Venezuela introduced generalized prohibitions and sanctions to censor potential dissenting messages that may promote anxiety among the population, alter public order, disregard legal authorities, or promote the violation of existing laws. Furthermore, service providers and websites are now considered liable for content posted by a third-party and are required to implement mechanisms to restrict prohibited content, under risk of heavy fines and of temporary suspension of operations (Freedom House, 2016).

A report published by the *Global Information Society Watch* in 2014 found that Venezuela is applying mass surveillance systems to spy on its citizens, and that it has violated their human rights during the monitoring of their communications (GISWatch, 2014).

Some of the measures that are being implemented are: the interception of individual citizens' emails and of telephone calls of members of the opposition, real time monitoring of citizens' digital activities and social networks especially through the intervention of the CESPPA (Strategic Center for Security and Protection of the Nation), attacks on Twitter accounts and websites hosting anti-government content, and censoring of broadcast programs and websites critical of the government. Furthermore, Venezuela has made mandatory the SIM card registration and placed data retention requirements on telecommunications companies (GISWatch, 2014).

Finally, the interdisciplinary research laboratory Citizen Lab at the University of Toronto found that a program capable of filtering, censorship and surveillance called *PacketShaper* and produced by the company Blue Coat Devices, is present on government networks in Venezuela, which is just one of the client among other countries with a historic track of human rights violation, surveillance and censorship, such as Afghanistan, China, Saudi Arabia, etc. (Marquis-Boire, et al, 2013).

2.6 TURKEY

Turkey is the first of the countries in the FOTN ranking to be categorized as not free, with a score of 61 over 100. Since 2011, Turkey has established a content filtering system and applied censorship against websites and social networks. The measures to control and monitor citizens' communications and digital activities have been tightened since 2013, when peaceful protests broke out against the authoritarian policies of government and spread across the country, initially sparked by the wish to defend Taksim Gezi park in Instanbul. The protesters were in their majority young people which organized themselves and communicated through social media, especially Twitter. Eventually, the protest was repressed with violence and the social media attracted the interest of the authorities due to their instrumental role in organizing the uprising and in disseminating information (Tavmen, 2014).

Since then, mass surveillance and state control of broadcasting and internet information outlets has been a priority for the Turkish government. Even though Turkey protects the freedom of expression in its constitution and adopted its first law on Data Protection in 2016, modeled on the EU's directives, in reality censorship of critical positions is widely applied. Numerous serious violations on the right of privacy and of freedom of speech are taking place, sometimes within the legal framework created, which however does not comply with international human rights standards (Tavmen, 2014).

An example is the *Law 5651 on Regulating Broadcasting in the Internet and Fighting Against Crimes Committed through Internet Broadcasting* of 2007, which is being used to censor webpages without the need of a court order. Numerous websites have suffered blackouts, Wikipedia being one of the most recent in April 2017 (Zeldin, 2017). However, also Twitter, Facebook and YouTube have being temporally blocked in various occasions until the content deemed prohibited was removed, and journalists and bloggers have been monitored or arrested for their critical writing (FOTN, 2016). According to the Turkish Free Journalists' Initiative, there are currently 180 journalists imprisoned in Turkey (SCF, 2017). On 11 January 2010, the Representative of the Organization for Security and Cooperation

in Europe on Freedom of the Media published a Report on the Turkish Internet Law and its use in mass website blocking. The report recommended to Turkey to bring the *Law 5651* in line with international standards or to abolish it completely (OSCE, 2010).

Finally, Turkey has been identified as a client of Blue Coat Devices as well, and the surveillance program *PacketShaper* has been found on government networks (Marquis-Boire, et al, 2013).

2.7 IRAN

Iran lacks a specific law on data privacy as well. There are however some provisions contained in other laws that regulate data protection such as the *Law on Electronic Commerce (LEC)* of 2004, the *Law on Computer Crimes (LCC)* of 2009 and the *Law on Publicising and Access to Data (LPAD)* of 2010. In specific, the article 58 of LEC established that the storing, processing and distributing of private data messages containing information on tribal or ethnic origins, moral and religious beliefs, and ethical physical, psychological or sexual condition of people is allowed only with the explicit consent of the individual (Norton Rose Fullbright, 2014).

According to the FOTN report, the Iranian cyberspace is under strict control, and all web content and platforms are subjected to arbitrary requests by the Iranian authorities to access users' data. Tens of thousands of websites suffer restricted access, especially international news and human rights sources, while Facebook and Twitter are blocked in the whole country. Furthermore, many activists have been arrested and incarcerated for their online activities.

In 2015, in view of the election, the Elections Security Headquarters was installed in order to monitor the cyberspace and in 2016 the Supreme Council on Cyberspace ruled that all instant messaging applications had to move all data on Iranian users to servers located inside the national territory, making it easier for the government to pressure foreign companies on providing their users' data (Freedom House, 2016).

In 2014, the government also launched the Operation Ankboot or project Spider, a mass surveillance operation aimed at identifying and eliminating Facebook pages and activities that according to the authorities spread corruption and western-inspired lifestyles. Operation Ankaboot was acknowledged by officials in 2015, when the IRGC Center for Investigation of Organised Cyber Crimes informed in a press release that 130 Facebook pages had been shut down, twelve individuals arrested and twenty-four detained (Shams, 2015).

2.8 CHINA

The last position of the FOTN ranking is held by China, with a score of 88. According to the report published by the Open Net Initiative (ONI, 2012, p. 271), China is ''one of the most pervasive and sophisticated regimes of Internet filtering and information control in the world''.

In terms of data protection, China does not have a comprehensive legal framework in place, but rules and regulations can be found across different laws, such as the *General Principles of Civil Law* and the *Criminal Law*. In 2012 the *Decision on Strengthening Online Information Protection* was promulgated with the goal to protect online information and citizens' rights, as well as those of other legal entities and organizations, and to safeguard national security (Norton Rose Fullbright, 2014).

The same year the *Information Security Technology Guidelines for Personal Information Protection* created specific requirements for the collection, processing, transmission and deletion of personal data. Nevertheless these guidelines cannot be enforced legally, and their application remains discretionary (Norton Rose Fullbright, 2014). The most recent law issued on the topic of data protection is the 2017 *Cybersecurity Law*. This law establishes new security and data protection obligations on network operators as well as restrictions to personal data transfer outside China (DLA Piper, 2017).

Notwithstanding the legal protections in place for data privacy, China state regulations require from service providers and private actors complete collaboration in terms of monitoring and filtering online content, as well as keeping a record of personal user information and online activities, which must be made available to the authorities upon request. For example, email and Internet service providers are required to keep a record of personal information, e-mail addresses, domain names users have accessed, content published and

time of publication for at least 60 days (ONI, 2012).

Internet cafes have also become a monitoring tool for the Chinese authorities. These cafés are required to install filtering software and record user information and complete session logs. In Tibet, moreover, Internet cafés have been ordered to install surveillance software since 2010. Monitoring and storing of user information and activities is carried out also by the biggest telecommunications companies, such as China Mobile Communications Corporation (China's largest mobile phone company), Tencent, and Skype, as well as by instant messenger apps, such as QQ, China' s most popular instant messenger. All the information collected by these service providers are given to the authorities if requested (ONI, 2012).

In order to increase its control on its citizens' online activities, the Chinese government amended the 1988 *Law on Guarding State Secrets.* According to the amendment all ICT companies are required to comply with measures to protect state secrets, which are loosely defined as matters of national security interest. In case of state secret leaks on the Internet, the companies must maintain and disclose their records to the relevant authorities and cease immediately the transmission of the leaked information. Due to the loose definition of state secret, this law has been used to target journalists, activists, and dissidents,which has led in some cases to their arrests. For example, the journalist Shi Tao was arrested after Yahoo! revealed to the authorities that he was the person behind an email sent to a US prodemocracy group on the topic of the 15th anniversary of the 1989 Tiananmen Square crackdown (ONI, 2012).

Finally, China has been building and implementing at least since 2006 its *Golden Shield Project*, which is a digital surveillance network with nationwide coverage. Video surveillance, security cameras, online monitoring and filtering, use of identification cards with scannable computer chips and photos, obligatory real-name registration for mobile and online accounts and in internet café are all part of this huge surveillance network. It is estimated that there are around 30 millions security cameras installed in Chinese cities, as well as around two million people monitoring public opinion online. Moreover, numerous cyberattacks originating from China have been conducted against human rights groups, civil organizations, activists' email accounts and journalists working on issues related to China (ONI, 2012).

In addition, Citizen Lab has uncovered evidence that China is also a customer of the surveillance software company Blue Coat Devices and has purchased the *PacketShaper* appliances to monitor and filter data (Marquis-Boire, yet al, 2013).

In conclusion, this section offered a brief overview of some data protection legislation in place worldwide and of the use governments, both democratic and authoritarian, make of personal data and information that can be collected online in order to monitor and control, with varying degrees, their citizens' activities, especially if they are critic of the established power. In general three main elements can be identified: firstly there is a tendency, even in democratic countries, to apply mass surveillance strategies under the pretension of protecting national security interests, used as a justification to restrict citizens' rights and infringe upon their privacy. Secondly, governments are buying surveillance software from companies selling internationally to some of the most repressive regimes in the world, and a 'surveillance' market appears to be growing and thriving thanks to the current global situation of instability and democracy erosion. Thirdly, the pressure on telecommunications and internet services to provide personal data is increasing, and often these companies bow to the pressure, becoming thus complicit with the unlawful requests of these repressive governments.

3. MEXICAN LEGISLATION

The Freedom of the Net report categorizes Mexico as a 'partially free' country, with a score of 38, below Brazil, Colombia, Nigeria, Kyrgyzstan and South Korea. In terms of legislation, the 2008 reform of article 16 of the Mexican constitution states that ''no one may be disturbed in his person, family, home, papers or possessions, except by written order of a competent authority, duly grounded in law and fact which sets forth the legal cause of the proceeding''. In this article, it is also affirmed that all people have the right to the protection of their personal data as well as to their access, rectification and elimination. The constitutional document is very specific and

assigns only to the federal judicial authority the power to authorize the monitoring of any private communication. It also affirms that the court order must explicitly state the legal causes for the surveillance request, as well as the type and duration of the monitoring allowed and the people involved. Moreover, the use of this legal surveillance is not allowed in electoral, fiscal, trade, civil, labor and administrative cases, and in the communications between a person detained and their lawyer.

The Federal Institute for Access to Public Information (based on the art. 15, 16 and 37, section III of the *Federal Law on Transparency and Access to Governmental Public Information 2006,* and art. 28 and 64 of the *Federal Institute Rules 2014) issued the Guidelines for the Classification and Declassification of Information by Federal Public Administration Agencies and Entities 2003. Article 32 states:*

> ''The information on personal data of an identified or identifiable natural person will be confidential when concerning: ethnic or racial origins, physical, moral and emotional characteristics, affective and family life, private address and phone number, wealth, ideology, political opinion, religious or philosophical beliefs, physical and mental health, sexual orientation, and equivalent data that regard their privacy, such as genetic information''.

The *Federal Law on the Protection of Personal Data held by Private Parties 2010 partially* develops the constitutional art. 16 by specifying the rules for data storage and use only for natural persons and private legal entities. This law defines personal data as: ''any type of information concerning a natural person, identified or identifiable''. *Personal sensitive* data are instead defined as:

> "Personal data that concern the most private sphere of the individual, or data that, if misused, may cause discrimination or serious danger to the individual. In particular, data are considered sensitive when they may reveal information on racial or ethnic origins, current and future health state, genetic information, religious, philosophical and moral beliefs, trade union membership, political opinions, sexual orientation''.

Additionally, the law regulates the transparency of privacy notices with regards to the identity and address of the data collector, the objectives of the data processing, the limitations for data use and disclosure, the means to access, rectify, eliminate or object, and the procedures to communicate changes in the privacy notice policies.

In reality, Mexican law considers only mechanisms for unilateral regulations or agreements, in which the user has no possibility of actively participating in the formulation of these rules. This is the case specifically for Facebook and Whatsapp: in their user contracts there is a clause stating that the user agrees to move any legal dispute to a court in California. In the latest *Statement of Rights and Responsibilities* of Facebook, updated to 30th January 2015, it is stated:

> "You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in the U.S. District Court for the Northern District of California or a state court located in San Mateo County, and you agree to submit to the personal jurisdiction of such courts for the purpose of litigating all such claims. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions''[2].

With the aim to avoid the misuse of this information by the authorities as a tool to harm their citizens' fundamental rights, the UN *resolution Right to Privacy in Digital Age* of 18th December 2013, advises the States to create ''domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data''. From this point of view, Mexico does not comply with international standards for privacy protection, since the country does not have any civil or independent oversight mechanism.

In addition to this resolution, the Joint Declaration of the UN Special Rapporteur on the right to freedom of opinion and expression together with Rapporteur of the Inter-American Commission on Human Rights of 21st June 2013, note that:

> "Every person has the right to access information under State control. This right includes information related to national security, save for specific exceptions established by the law,

[2] The complete text is available at: https://www.facebook.com/legal/terms

© 2017. *Revista Internacional de Comunicación y Desarrollo, 7*, 111-129, ISSN e2386-3730

> with the condition that these exceptions are necessary in a democratic society... the States must disseminate, at least, information on the legal framework in place for the surveillance programs, on the entities in charge of implementing and overseeing these programs: the procedures for the authorization, for the selection of objectives and for data management, as well as information on the use of these surveillance techniques, including aggregated data on their scope. In any case, the States must establish independent oversight mechanisms able to ensure the transparency and accountability of these programs".

The *General Law on Transparency and Access to Public Information 2015* states in its article 70 that telecommunication companies must provide information for statistics purposes on the monitoring of private communications, on the access to the telecommunication records and geolocalization in real time. Furthermore, the law establishes that the statistical information on surveillance monitoring must be proactively published by the competent authority and on the *Platform for National Transparency*, and updated at least every three months.

The Guidelines for Collaboration on Security and Justice 2015 issued by the Federal Institute for Telecommunications (IFT) impose responsibilities for licensed companies and for competent authorities with regards to transparency. Companies and entities involved in surveillance actions are under obligation to provide two annual reports to the IFT, which must be accessible to the public. Nevertheless, the deadline for the delivery of the report has been postponed from November 2016 to May 2017, and as such, official data on these operations are still not available.

In this context, it is useful to analyze the types of surveillance regulated by the Mexican legislation. The modalities allowed are the following:

1. Geolocalization in real time through mobile devices: the *Federal Telecommunications and Broadcasting Law 2014* (art. 190, section I); the *Federal Code of Criminal Procedure 2016* (art. 303) and the *Guidelines for Collaboration on Security and Justice* by the IFT (Ch. III). The action of amparo 964/2015 emitted by the Supreme Court of Justice of the Nation (SCJN) affirmed that this modality can be implemented exclusively in cases in which ''a danger to the life or integrity of a person may exist''.

2. Monitoring of private communications: *Political Constitution* (art. 16) and the *Federal Code of Criminal Procedure* (art. 291): ''monitoring of private communications encompasses the whole communications system or programs fruit of the technological evolution, which allow the exchange of data, information, audios, videos, messages, as well as electronic files which record, retain conversation content or data that identify the communication, and can be provided in real time''. *The General Law to Prevent and Punish Crimes of Kidnapping 2016* (art. 24), *the Federal Law against Organized Crime 2017* (art. 48-55), the *Law on National Security 2005* (art. 33-49), the *Code of Military Criminal Procedure 2016* (art. 287).

3.Obligatory retention of metadata on communications: the *Federal Telecommunications and Broadcasting Law 2014* (art. 190, section II): retention of telecommunications data traffic for 24 months.

The agencies authorized to access and to monitor the data, under court order, are:

1. The Attorney General of the Republic (PGR) and the attorneys of federal entities: the *Federal Code of Criminal Procedure,* art. from 292 to 302. When investigation of a crime is deemed necessary.

2. The Federal Police (PFP): the *Law of Federal Police 2009* (art. 48-55): in the cases in which enough evidence is uncovered to prove the existence of specific crimes. Some example are espionage, sabotage, terrorism, rebellion, treason, genocide, foreign interference in domestic affairs, actions against state powers or against military, naval or air operations, actions against diplomatic or counterintelligence personnel, as well as the destruction or damaging of strategic infrastructure.

3. The Center for Investigation and National Security (CISEN): the *Law on National Security 2005* (art. 33) states that private communications monitoring is allowed when national security is threatened, as defined in art. 5 of the same law.

The federal regulation establishes moreover that all metadata on communications, i.e. the information on citizens' personal communications, must be stored by the service providers for 48 months (*Federal Telecommunication and Broadcasting Law 2014*, art. 190, section II). Additionally, it sets the rules for the direct monitoring of personal communications and geolocalization in real time, opening the way to a type of indiscriminate surveillan-

ce (art. 190, sections I, II).

The regulation also enhances the surveillance mechanisms available to service providers as well as to the federal agencies authorized to data access (PGR, federal attorneys, PFP and CISEN). However, it does not clearly articulate the rights of the citizens nor the mechanisms in place for their protection. This is a relevant omission that strengthens state surveillance capacity at the expense of the protection of citizens' digital rights.

Data provided by federal authorities shows that of all requests to access stored data, only 1.09% came with the required federal juridical permission, and consequently most of the surveillance actions were taken under dubious ethical and juridical conditions. Additionally, telecommunications companies refused only 8.29% of all the requests. This situation is especially worrisome in federal entities such as Chihuahua and Veracruz, where there is a concentration of geolocalization requests, since these states have been the place of systematic fundamental rights violations, such as murder and disappearance of journalists (R3D, 2016b).

4. ILLEGAL SURVEILLANCE

Mexican law is very permissive towards the faculty state agencies have to monitor citizens. Furthermore, various civil organizations have denounced that most of the state surveillance actions do not comply with the desirable requirements of international standards. In many cases, these actions do not even comply with the procedures established by the national law. This means that most of the surveillance practices are undertaken without the required legal procedure, and are consequently applied outside the law.

Investigations carried out by the civil organization *Red en Defensa de los Derechos Digitales* (R3D, Network for the Defense of Digital Rights) are an excellent example of these types of complaints. In its first report of 2016 (R3D, 2016a), the organization evaluated the compliance of telecommunications companies with current regulations, and discovered that these companies were lacking in numerous aspects. The report analyzed the following elements: (1) Privacy policies, (2) Prior judicial authorization, (3) User notification, (4) Transparency, (5) Commitment against mass surveillance, and (6) User right to personal data access[3].

As the table shows, the most important telecommunications companies present serious shortcomings in their internal procedu-

Table 1. Privacy protection in Mexican telecommunications companies

	1	2	3	4	5	6	TOTAL
AT&T	75%	75%	0	75%	75%	0	60%
Axtel	0	0	0	25%	0	NA	5%
Izzi	0	0	0	0	0	NA	0
Megacable	25%	50%	0	25%	0	NA	20%
Movistar	50%	50%	0	25%	50%	0	35%
Telcel	0	0	0	25%	25%	0	10%
Telmex	0	50%	0	0	25%	NA	15%
Total play	0	0	0	0	0	NA	0

Source: R3D (2016a).

[3] Privacy policy (1.1 Privacy policy and information available in Internet; 1.2 Privacy policy establishes what information can be collected and stored; 1.3 Data retention time restrictions in place; 1.4 Presence of public document on state procedure to data access; 1.5 Public document lists types of data that can be provided, legal requirements and conditions to data access; 1.6 User notification when changes are made to the privacy policy). Judicial authorization (2.1 Prior judicial authorization is required to make public the document; 2.2 Public requirements and federal judicial court order is required to provide metadata; 2.3 Requests have been rejected for not complying with legal requirements). User notification (3.1 Notification to affected user; 3.2 Public promotion of user notification mechanisms to public institutions). Transparency (4.1 Publication during the last year of transparency report; 4.2 Transparency report is available in Internet; 4.3 Presentation of the report to the Federal Institute of Telecommunications). Commitment against mass surveillance (5.1 Publication of judicial controversies due to illegal or disproportionate requests; 5.2 Publication of public stance in favor of human rights and privacy; 5.3 Existence of judicial actions or regulatory entities for user data protection; 5.4 Participation in any sectoral or multisectoral mechanism for human rights promotion, respect and protection). User right to personal data access (6.1 Data are provided on user request; 6.2 Online format that is accessible and within time frame established by law).

res in terms of complying with national regulations. With the exception of At&T, the majority of big companies do not reach the 50% threshold for desirable implemented actions.£

With regard to the privacy policies, only two companies (At&t and Movistar) state the type of information collected on the users and their communications, while only three (At&t, Movistar and Megacable) have implemented a clear procedure on their collaboration with authorities.

The most worrying data, though, concern the prior judicial authorization element. Only At&t and Telmex require explicitly a judicial authorization for giving access to communications monitoring, while no company requires this permission in order to provide access to metadata. On the contrary, companies such as Axtel y Telcel have been fully collaborating with the authorities and have not denied any request, notwithstanding the absence of a judicial authorization or rationale.

From the point of view of user notification, none of the companies analyzed has in place any mechanism to safeguard the user right to know if they have been or are monitored. In terms of transparency, At&t is the only company that published a report on the access to user data, thus respecting the national regulations. However, the report is only in English and does not specify the source, the reasons nor the scope of the data access requests.

Finally, for what concerns the companies' commitment to human rights, only At&t has undertaken judicial actions to protect its users' rights in two cases. Four companies have instead expressed in a public document their corporate responsibilities towards users' rights, however no real actions were taken to protect them. In addition, it is relevant to highlight that with regards to the user's right to personal data access, none of the companies completely safeguards it.

The second report of 2016 published by R3D is called *The surveillance State: out of control*. In this report, the organization reports numerous inconsistencies in the authorities' actions. In 2013, telecommunications companies denied only 54 of the 872 requests made by various governmental entities to monitor private communications. In 2014, 1165 requests were made, of which 52 were denied. Finally, in 2015, there were 1144 requests and 62 were rejected. In addition to these data, there is another element especially troubling: the data reported by the entities that monitored private communications and the data collected by the supervisory body, the Council of the Federal Judiciary, do not match. In particular, there is a considerable mismatch with regards to three relevant entities: (1) the Centre for Investigation and National Security reports 2002 requests, while according to the Council of the Federal Judiciary the requests were 654, (2) the Federal Police reports 225 requests and the Council 289, (3) the Attorney General of Mexico reports 866 requests, while the Councils estimates they were 2392.

In the case of Mexico, it is especially crucial to underline that the authorities have persistently implemented surveillance specifically in the federal states with more assassinations and disappearances related to freedom of expression issues (Veracruz, Chihuahua, Puebla, Nuevo León, Tamaulipas). The case of Veracruz is exemplar: its ex-governor, Javier Duarte de Ochoa, ran abroad to escape from the justice and has been accused by numerous civil society leaders to have violently persecuted his opponents while in power. Under Duarte's government, the Veracruz Public District Attorney Office made 224 requests to access data in 2013, which rose to 780 in 2014 and to 802 in 2015.

Other relevant data from the latest report show that 98.91% of the requests were submitted without any judicial authorization. In some cases, the requests came from public entities lacking the legal faculty of making such requests. Examples of these public entities are some local courts, the Electoral Institute of Mexico City, the government of the state of Mexico, the Secretariat of Finance and Public Credit and the Secretariat of Communications and Transports (R3D, 2016b, p. 60).

Besides the monitoring of communications, the Chihuahua Public District Attorney, the Attorney General of the Republic and the Veracruz Public District Attorney were the entities that submitted the highest number of requests for geolocalization in real time between 2013 and 2015. Respectively these entities made 6674, 4005 and 1033 requests. Of all the requests, 99.17% did not have any judicial authorization. Additionally, only 8.73% of surveillance actions led to prosecution. In the case of Veracruz just 0.38% of these actions led to prosecution, and in Chiapas only 0.52%, while in Baja California, Tlaxcala, Zacatecas and Guerrero none of the surveil-

llance acts resulted in a prosecution (R3D, 2016b, pp. 72-73).

The results of these investigations suggest that the majority of surveillance actions in Mexico are implemented inside a context that is extremely harmful to the citizens. Firstly, national law is not in line with international standards. Secondly, telecommunications companies do not fully comply with the law to protect their users' rights. Thirdly, authorities access data and citizens' communications without judicial authorization. Finally, surveillance actions do not lead to the prosecution of the citizens monitored. As the report *The surveillance State* indicates ''investigating authorities use surveillance tools against people when there is no evidence on their participation in any crime'' (R3D, 2016b, p. 74).

Next to this type of excessive state surveillance, in Mexico malware software are being used to monitor targeted citizens without the need to rely on the complicity of telecommunications companies. In July 2012, various sources leaked documents revealing that the Mexican secret services had paid $300 millions to buy spyware designed to intercept citizens' landline and mobile communications. This type of software is able to record conversations, store text messages, emails, search history and contact lists, moreover it can turn on the cameras and mobile phones of the users. These leaks would then be confirmed by the Mexican army and in 2013 information appeared which confirmed that the software *FinFisher* had being used with the same objective (Freedom House, 2016, p. 602).

In 2015, a substantial document leak from the *Hacking Team* company revealed that Mexico was one of their most important clients worldwide; in fact this Italian company dedicated to designing and selling surveillance appliances had signed 14 contracts with various Mexican state and federal agencies. Even though these types of contract are at the edges of the law, the state entities that implement these surveillance systems increase year after year (Freedom House, 2016, p. 601).

Investigations by the Toronto-based interdisciplinary laboratory Citizen Lab uncovered evidence that software developed by the Israeli company NSO Group Technologies were used to infect citizens' devices engaged in relevant activism work. An example is the espionage against a well known scientist and two social leaders campaigning against obesity in 2016[4]: Dr. Simon Barquera, Alejandro Calvillo and Luis Encarnación. These people were working for the implementation of a tax on sugary beverages in Mexico and were infected with a malicious malware to spy them (Scott-Railton, et al, 2017a). This specific case shows that the surveillance measures implemented by the government may be used to persecute civil society members with completely illegitimate reasons.

A recent case that highlights the illegitimate and unlawful use given to this type of surveillance was made public the first semester of 2017. Another Citizen Lab report revealed that more than 76 messages were sent to journalists, lawyers and one underage person with the purpose of infecting their devices. The citizens targeted by this state espionage attempt were people involved in investigations aimed at denouncing the Mexican president's corruption acts, as well as the authority abuse by various state agencies and the systematic violation of human rights. The child monitored is the son of the journalist Carmen Aristegui, who has being subject to a systematic persecution policy for her numerous revelations on corruption acts, nepotism, the plagiarism of his university thesis by the actual president, the alleged alcoholism of the ex-president Calderón and the uncovering of an alleged child abuse network within the Mexican clergy (Scott-Railton, et al, 2017b).

Besides the illegal espionage against civil society members involved in journalism, another report highlighted that three politicians of the opposition party, *Partido Acción Nacional*, were victim of the same surveillance system (Scott-Railton, et al, 2017c).

The malicious use of this illegal software by public organisms was applied also against the international investigation group formed to review the case of the 43 students disappeared in 2014. These attempts at device infection happened shortly after the group denounced that they were being subject to illegitimate interferences by the federal government, during the redaction of the group final report (Scott-Railton, et al, 2017d). Citizen Lab investigations confirm that at least 19 citizens have been spied with the Israeli company's software, including activists, scientists, public officials and their relatives.

In addition to these cases, there have been demonstrated espionage attempts with the

© 2017. *Revista Internacional de Comunicación y Desarrollo, 7*, 111-129, ISSN e2386-3730

software Pegasus created by the NSO Group against the lawyers of three Mexican women assassinated in 2015 for political reasons: one of the victims, Nadia Vera, was a government critic and women's rights advocate. The espionage objectives were Karla Micheel Salas and David Peña, both lawyers specialized in the defence of human rights. The murdered women were victim of a professional attack in a flat in Mexico City, while they were visiting the journalist Rubén Espinosa, who had been threatened by the Veracruz government during Javier Duarte's mandate, and who was killed as well (Scott-Railton, et al, 2017e).

5. CONCLUSIONS

As mentioned, Mexico is classified as partially free in the *Freedom of Internet* report and the situations described in the above section cast a light on the reasons behind this classification. In general, it can be affirmed that Mexico is applying excessive state surveillance against its citizens, in a context of unclear or lacking regulations, which allow for illegitimate monitoring of private communications by various government agencies, often without evidence of a criminal act being committed by the person under surveillance, nor tangible results, since the vast majority of these actions do no lead to a prosecution.

Furthermore, there is strong evidence that illegal surveillance software and malware are employed to monitor and infect the devices belonging to critics of the established power, such as journalists, activists, lawyers, researchers and members of the opposition parties.

In this state of legislative confusion and non compliance, the indiscriminate access to citizens' personal data is further facilitated by complicit telecommunications companies, which fully collaborate with government authorities, thus neglecting the protection of their users' rights.

The international context described in this article, allows us moreover to draw a comparison between Mexico and the countries analyzed. It is clear that Mexico is making use of mass surveillance methods similar to those implemented by the more authoritarian governments: firstly, excessive state surveillance is employed, creating a situation in which any citizen may be considered a potential criminal. In this way, the right to the presumption of innocence that should apply to every person is seriously undermined. Secondly, the loose definition of national security permits to unduly expand the scope of action of government and intelligence agencies in terms of data access and monitoring. Thirdly, the targets of this state surveillance are often dissidents or critics of the government. Finally, illegal software and malware are employed especially against the targets mentioned.

Hence, it is evident that such unlawful and pervasive surveillance, as implemented by government entities against their own citizens, should be considered as undesirable in a democratic country.

In conclusion, to answer the question about what rules should prevail in a democratic country in order to avoid indiscriminate mass surveillance, we identify the following elements:

1. The creation of an independent organism to protect citizens' digital rights and to oversee telecommunications companies' and public authorities' compliance with the current legislation.

2. The formulation of clear rules that enhance transparency in the surveillance actions implemented by companies and public entities. Moreover, the publication of transparency reports should be proactive and they should be easily accessible on these entities' websites.

3. The establishment of special courts in charge of solving potential disputes.

4. The formulation of clear rules about who is allowed to access data and to monitor communications, by what types of means, and in what circumstances.

5. The requirement of prior judicial court order to access any data or communications, as well as of the obligation to notify the person affected by such measures.

6. The defense of the presumption of innocence, by applying the principles of necessity and proportionality to surveillance actions.

7. The explicit prohibition of espionage with illicit means and the creation of criminal responsibilities for those who buy illegal software with public money.

›Referencias Bibliográficas

- Assange, J. (2013). *Internet è il nemico*. Milano: Feltrinelli.
- Bumiller, E. (2010, April 4). Video Shows U.S. Killing of Reuters Employees. *The New York Times*, Retrieved from: http://www.nytimes.com
- CIDH. Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión. 21 June, 2013. Retrieved from: http://www.oas.org
- DLA Piper, (2017). Data Protection Laws of the World: China. DLA Piper Intelligence. Available at: https://www.dlapiperdataprotection.com
- EDRi (2015, October 6). Finland: New surveillance law threatens fundamental rights. European Digital Rights (EDRi). Retrieved: https://edri.org
- Farouk, Y. (2012). La revolución de Egipto: muy pronto para concluir, a tiempo para excluir. *Foro Internacional*, 52 (2), 345-360.
- Freedom House (2016). *Freedom on the Net 2016*. Washington: Freedom House.
- General Assembly resolution 68/167. *The right to privacy in the digital age, A/RES/68/167* (18 December 2013). Retrieved from: http://undocs.org/A/RES/68/167
- GISWatch (2014). *Global Information Society Watch 2014: Communications surveillance in the digital age.* Global Information Society Watch.
- Kosinski, M., Stillwell, D., Graepel, T. (2012). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, 110(15), 5802–5805. doi: 10.1073/pnas.1218772110
- Kramer, A., Guillory, J., Hancock, J. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences of the United States of America,* 111(24), 8788–8790. doi: 10.1073/pnas.1320040111
- Marczak, B., Scott-Railton, J. (2016). *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. Toronto:* Citizen Lab, Retrieved from: https://citizenlab.ca
- Marquis-Boire, M., Dalek, J., McKune, S., Carrieri, M., Crete-Nishihata, M., Deibert, R., Khan, S.O., Noman, H., Scott-Railton, J., Wiseman, G. (2013). *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools.* Toronto: Citizen Lab, Retrieved from: https://citizenlab.ca
- Norton Rose Fullbright (2014). *Global Data Privacy Directory.* Norton Rose Fullbright LLP
- OECD (2017). *Obesity Update 2017*. Washington: OECD
- OSCE (2010). *Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship.* OSCE
- ONI (2012). *China: country profile.* OpenNet Initiative.
- Privacy International (2016). *The right to Privacy in Estonia: Privacy International Submission to Human Rights Committee.* Privacy International
- Privacy international (2015). *Shadow State: Surveillance, Law and Order in Colombia – Special Report.* Privacy International
- R3D (2016a). *¿Quién defiende tus datos? Reporte de evaluación de empresas de telecomunicaciones ante las medidas de vigilancia*, México: Red en Defensa de los Derechos Digitales.
- R3D (2016b). *Reporte: El Estado de la Vigilancia. Fuera de Control*, México: Red en Defensa de los Derechos Digitales.
- Rice, M. (2016, March 8). Colombia's new spying scandal: Time for real change. *Privacy International,* Retrieved from https://www.privacyinternational.org
- Rodriguez, I. V. (2013). New Colombian Regulations have been Enacted - Obligations created by Colombian Decree 1377/2013. *Nymty,* Retrieved from: https://www.nymity.com
- Rodríguez Prieto, R., Martínez Cabezudo, F. (2016). *Poder e Internet: un análisis crítico de la red.* Spain, Madrid: Cátedra.
- SCF (2017, September 5). ÖGİ: 30 Journalists Detained, 14 Journalists Arrested By Turkish Government In August. *Stockholm Center for Freedom*, Retrieved from https://stockholmcf.org/
- Scott-Railton, J., Marczak, B., Guarnieri, C., Crete-Nishihata, M. (2017a). *Bittersweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links.* Toronto: Citizen Lab, Retrieved from https://citizenlab.ca
- Scott-Railton, J., Marczak, B., Razzak, B.A., Crete-Nishihata, M., Deibert, R. (2017b). *Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware.* Toronto: Citizen Lab, Retrieved from https://citizenlab.ca
- Scott-Railton, J., Marczak, B., Razzak, B.A., Crete-Nishihata, M., Deibert, R. (2017c). *Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware.* Toronto: Citizen Lab, Retrieved from https://citizenlab.ca
- Scott-Railton, J., Marczak, B., Razzak, B.A., Crete-Nishihata, M., Deibert, R. (2017d). *Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware.* Toronto: Citizen Lab, Retrieved from https://citizenlab.ca
- Scott-Railton, J., Marczak, B., Razzak, B.A., Crete-Nishihata, M., Deibert, R. (2017e). *Reckless IV: Lawyers For Murdered Mexican Women's Families Targeted with NSO Spyware.* Toronto: Citizen Lab, Retrieved from https://citizenlab.ca
- Shams, A., (2015, May 14). The State of Surveillance in Iran's Cyberspace. *Azad Tribune,* Retrieved from https://www.article19.orgn
- Stöcker, C., y Lischka, K. (2013, August 1). New Leaks Show Near Total NSA Surveillance. *Spiegel online*, Retrieved from http://www.spiegel.de
- Tavmen, G. (2014). *Internet rights that went wrong in Turkey: Special Report.* Global Information Society Watch.
- Youyou, W., Kosinski, M., Stillwell, D. (2014). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences of the United States of America*, 112(4), 1036–1040. doi: 10.1073/pnas.1418680112
- Zeldin, W. (2017, May 3). Turkey: Government Blocks Wikipedia. *Library of Congress,* Retrieved from http://www.loc.gov

© 2017. *Revista Internacional de Comunicación y Desarrollo, 7*, 111-129, ISSN e2386-3730

›Referencias Bibliográficas

Mexican Legislation

▪ Code of Military Criminal Procedure, Mexico (2016). Retrieved 22 September, 2017 from http://www.diputados.gob.mx

▪ Federal Code of Criminal Procedure, Mexico (2016). Retrieved 22 September, 2017 from http://www.diputados.gob.mx

▪ Federal Law on Transparency and Access to Governmental Public Information, Mexico (2006). Retrieved 22 September, 2017 from http://www.dof.gob.mx

▪ Federal Law on the Protection of Personal Data held by Private Parties, Mexico (2010). Retrieved 22 September, 2017 from http://www.diputados.gob.mx

▪ Federal Law against Organized Crime, Mexico (2017). Retrieved 22 September, 2017 from http://www.diputados.gob.mx

▪ Federal Telecommunications and Broadcasting Law, Mexico (2014). Retrieved 22 September, 2017 from https://www.gob.mx

▪ General Law on Transparency and Access to Public Information, Mexico (2015). Retrieved 22 September, 2017 from http://www.diputados.gob.mx

▪ General Law to Prevent and Punish Crimes of Kidnapping, Mexico (2016). Retrieved 22 September, 2017 from http://www.diputados.gob.mx

▪ Guidelines for the Classification and Declassification of Information by Federal Public Administration Agencies and Entities, Mexico (2003). Retrieved 22 September, 2017 from http://dof.gob.mx

▪ Guidelines for Collaboration on Security and Justice, Mexico (2015). Retrieved 22 September, 2017 from https://www.gob.mx

▪ Internal Rules of the Federal Institute for Access to Public Information, Mexico (2014). Retrieved 22 September, 2017 from http://www.dof.gob.mx

▪ Law of Federal Police, Mexico (2009). Retrieved 22 September, 2017 from http://www.dof.gob.mx

▪ Law on National Security, Mexico (2005). Retrieved 22 September, 2017 from http://www.diputados.gob.mx

▪ Political Constitution, Mexico (2017). Retrieved 22 September, 2017 from: http://www.diputados.gob.mx

▪ SCJN. Segunda Sala. Amparo en Revisión 964/2015. Sentencia de 4 de mayo de 2016.

Other legislation

▪ Colombian Constitution, Colombia (2005). Retrieved 2 September 2017 from: https://www.constituteproject.org

▪ Estonian Constitution, Estonia (1992). Retrieved 2 September 2017 from https://www.president.ee

▪ Information Society Code, Finland (2015). Retrieved 2 September 2017 from http://www.finlex.fi

▪ Media Act, Island (2011). Retrieved 2 September 2017 from https://www.pfs.is

▪ Personal Data Act, Finland (1999). Retrieved 2 September 2017 from http://www.finlex.fi

▪ Rules no. 837/2006 on Electronic Surveillance, Iceland (2006). Retrieved 2 September 2017 from http://www.ilo.org

▪ Venezuelan Constitution, Venezuela (2009). Retrieved 2 September 2017 from https://www.constituteproject.org