DERECHOS DIGITALES
América Latina

DATA RETENTION AND REGISTRATION OF MOBILE PHONES

CHILE IN THE LATIN AMERICAN CONTEXT

MARIANNE DÍAZ

DERECHOS DIGITALES
América Latina

DATA RETENTION AND REGISTRATION OF MOBILE PHONES

CHILE IN THE LATIN AMERICAN CONTEXT

MARIANNE DÍAZ

Cover page: Violeta Cereceda and Constanza Figueroa.

Layout: Violeta Cereceda.

Editing: Vladimir Garay.

Junio 2017.

This report was made by Digital Rights (Derechos Digitales), with the funding of Privacy International and Ford Foundation. Digital Rights is an independent non-profit organization, founded in 2005 and whose mission is the defense, promotion and development of fundamental rights in the digital environment, from a public interest perspective. Among its main areas of interest is the defense and promotion of freedom of expression, access to culture and privacy.

Abstract [1]

Data retention and mobile phone registration measures constitute restrictions to the fundamental rights to privacy and freedom of communication. Being this the case, the measures must comply with a series of minimum requirements that guarantee the respect for international standards in the field of human rights. This study is done considering the regional and global trend that leads governments and service providers to accumulate an increasing amount of information about their users. A compared perspective is given analyzing the laws of Mexico, Brazil, Colombia, Peru, Argentina and Chile regarding data retention and registration of mobile phones, bearing in mind their international obligations and commitments in the inter-American framework, and in particular, to legislative projects that seek to change the current regulatory framework of telecommunications in Chile.

Key words: Data retention, privacy, communications, SIM registration, mobile telephony.

1 The author thanks Valentina Hernández and Paula Jaramillo for the information provided for the preparation of this research.

Table of Contents

5. Executive Summary

This report is the result of an examination of the current legislation on data retention and the registration of mobile phones in Argentina, Brazil, Mexico, Peru and Chile (with emphasis on the latter), in relation to the principles and parameters of human rights that govern restrictions on access to communications and freedom of expression.

There is a global trend of nations to regulate telecommunications more strictly, sustained on the fight against terrorism and organized crime, the response to this points to the fact that the uses of technology for the purposes of communication are protected by international human rights standards. As an example, anonymity, which is usually presented by states as a dangerous status that must be eradicated, assuming that it contributes to the perpetration of crimes, is seen by the United Nations as a guarantee of freedom of expression and free flow of ideas in modern society.

In the balance of this tension, the American Convention on Human Rights considers the minimum requirements that must be considered in any restriction on freedom of expression in the region. We accept, therefore, that there are limitations and that it is within the power of the states to regulate the cases in which these rights are restricted, nonetheless we postulate that said measures must meet five requirements: (1) legality, (2) search for an imperative purpose, (3) necessity, suitability and proportionality of the measure in relation to the purpose pursued, (4) judicial guarantees, and (5) satisfaction of due process.

Thus, we observe that the Latin American legislations regarding data retention and registration of SIM cards are inconsistent in the fulfillment of these parameters. In several cases, the measures are taken infringing the principle of legality, through an executive order, jeopardizing minimum guarantees of the democratic system. In other cases, access by public entities to data is allowed without the guarantee of a judicial order, which violates due process and places citizens in a state of defenselessness that seriously affects their human rights. As reported, a recent trend has included registration mechanisms on one of the numbers that identifies each mobile phone, such as the so-called IMEI.

It is clear, with the evidence we have available, that measures such as mandatory registration of SIM cards are not only disproportionate, but directly useless. Its alleged advantages of this measures have proved to have no basis in reality, after their application in various countries, especially in the African region. Likewise, both: the mandatory registration of SIM cards and data retention measures that lack minimum standards contribute to deepening an unbalanced relationship between users, mobile phone companies and the states, an imbalance that affects the ability of citizens to demand compliance with their fundamental rights. Based on this analysis, we elaborated a series of recommendations, not only to the Chilean State, but to the states in general, with the purpose of achieving this balance.

1. Mobile phone registration and data retention: scope and purpose

National security and the prevention and prosecution of crime are the most frequently used arguments to justify the increased surveillance of communications, including the accumulation of data on those communications. During the last two decades, a marked global trend points to the expansion and implementation of prescriptive regulations that force the requirement and retention of a greater amount of data from mobile phones users by the companies that provide the service (Gow and Parisi, 2008). The wave of implementation of mandatory SIM card registrations began in 2003, with regulations in Brazil, Germany and Switzerland (GSMA, 2013). By 2016 around 90 countries required mandatory registration for SIM card users (GSMA, 2016) .

For the most part, the authorities that implement these measures justify them on the need to use information as a tool in the fight against terrorism and organized crime (Kapellmann and Reyes, 2015). Also, although to a lesser extent, they are justified on the fight against theft and robbery of mobile devices, as well as the need to reduce the loss of resources in the mobilization of police personnel and emergency services in cases of prank calls (Eagle News, 2016).

The prepaid phone market makes up a high percentage of the entire mobile market, reaching up to 90% in countries such as Mexico (Gow and Parisi, 2008). This implies that, although at the moment of the greatest growth in the creation of these measures, conflicts had already risen in relation to the amount of personal data accumulated and managed as a result of them, the percentage increases on prepaid phones, considering the advancement of the technology that leads to the growth in the number of functions that these devices can fulfill, which allows to accumulate a much greater number of data, not only of the actual communication, but of the user's location, browsing history and countless other relevant information.

Despite the extent to which these types of measures are still being implemented today, there is also evidence of their elimination in some countries. The effective application of these measures in various countries of the globe has demonstrated the absence of a clear link between mandatory registration measures and the prevention of terrorism and organized crime (Privacy International, 2004). In the case of Latin America, Mexico modified its national criminal and telecommunications legislation in 2009, with the purpose of establishing the creation of the National Registry of Mobile Telephone Users (RENAUT), which obliged the providers of telecommunications services to keep a record in which each cellphone is clearly associated with a citizen, this record would be accessible at request of the Public Ministry, which would have access to data such as the geolocation of the device or the content of the communications. However, these provisions were repealed just three years later, since, instead of decreasing, the percentage of terrorist and organized crimes increased within the system's validity (GSMA, 2013).

Similarly, a study done in 32 countries in sub-Saharan Africa (Jentzsch, 2012) shows that the mandatory registration of SIM cards not only decreases the growth in the use of mobile phones

(an undesirable effect in countries that seek to increase their rates of access to telecommunications) but there is no convincing evidence that the implementation of such registry decreases the crime rates.

Likewise, the implementation of user registers, or data or communication metadata is not exempt from failures. On many occasions, the mandates to retain data are not accompanied by clear standards regarding the handling, storage and safe disposal of such data, which, combined, can reveal highly specific details about the private life of any individual, including medical, financial and family aspects (Keane, 2015).

Consequently, the registration and retention of information associated with mobile communications raises a series of considerations concerning the privacy and intimacy of citizens, who may be affected by several factors: the acquisition, handling and storage of data, the possibilities of citizens to control the existing information about them in the hands of third parties, and the security and protocols surrounding the processing of such information (Kapellmann and Reyes, 2015).

As stated by the United Nations Rapporteur for Freedom of Expression (Kaye, 2015), the mandatory registration of SIM cards can provide governments with the ability to monitor the behavior of individuals beyond their legitimate interests, and hinder the access to communication tools that keep citizens away from the exercise of their fundamental rights.

It is worth considering, for example, that demanding identity documents or evidence from a permanent address can make it difficult for people belonging to marginalized groups to access telecommunications: low-income people, immigrants, women in precarious situations, transgender people, among other examples. Likewise, the existence of a mobile phone registry increases the costs of changing the provider for the user, since a new registration with a new provider would be needed, which in turn has an impact on privacy. The more faithful you are with a certain provider, the more detailed the personal profile becomes (Jentzsch, 2012). All these aspects have implications for the citizen's exercise of human rights in the context of mobile communications.

The American Convention contemplates the minimum requirements that must be contained in any restriction on freedom of expression, which must be evaluated in a systemic manner, but in particular there are five: (1) legality, (2) search for an imperative purpose, (3) necessity, suitability and proportionality of the measure in relation to the purpose pursued, (4) judicial guarantees, and (5) satisfaction of due process. These same standards are developed in the International Principles on the Application of Human Rights to Communications Surveillance, prepared with the consensus of civil society to determine the legitimacy of surveillance measures in the context of communications. Starting from these parameters, we seek to set limits to the natural situation of inequality in the relationship that arises between the state and service providers, on the one hand, and users, on the other.

2. Generalities

2.1. Retention of communications data

Although data retention practices in the field of telecommunications have become ubiquitous in recent years, human rights standards regarding the capture of data related to communications establish that any practice of this type constitutes a potential interference to the right to privacy. This applies to the retention of telecommunications data regardless of whether such data is subsequently consulted or used. The data, as a minimum unit of information, may not possess or provide a large amount of meaning by itself, but it gains great importance when considered with other sources of information that, added together, build a profile of the user, their interpersonal networks and behavior in society and the market.

As recognized by the UN Human Rights Council (UNHRC, 2014), the mere possibility that information about communications is captured interferes with the right to privacy and potentially has a silencing effect on freedom of expression. In this sense, it is up to the states to demonstrate that these interferences meet the minimum requirements, that is, they are not arbitrary or disproportionate. In the context of the Inter-American Human Rights System, measures that affect or restrict communications must be harmonized with international standards, as they affect fundamental rights. The mandatory retention of data by third parties, in which governments require telephone companies and internet service providers to store data and metadata from their clients' communications is not considered by the United Nations as necessary or proportional.

There is consensus in civil society that retention of data should never be required from service providers a priori, as it violates the right of individuals to express themselves anonymously (Privacy International, Access Now, and Electronic Frontier Foun -dation, 2014). We have seen, for example, that in 2014 the Court of Justice of the European Union declared the data conservation directive invalid, a regulation that sought to harmonize the provisions of the member states with respect to the conservation of data generated or processed by the providers of telecommunications services. The CJEU considered on that occasion that "by imposing the preservation of these data and by allowing access to the competent national authorities", the Directive constituted a serious and undue intrusion into fundamental right to respect for privacy and data protection of a personal nature. When assessing the Directive, the CJEU took into account the fact that it: 1) it covered every person, means of communication and data without any differentiation, limitation or exception, 2) did not set criteria that would ensure that only the competent authorities could have access to the data and that these would be used to prevent, detect or repress actions whose severity justified the interference, and 3) the Directive established a data retention period of between six and twenty-four months, without specifying which criteria should be used to terminate the period and thus ensure that it is limited to the strictly necessary time. These factors led the European Court to consider that the Directive did not have sufficient guarantees to ensure the protection of citizens' data against access and illicit uses, and against possible abuses by authorities or intermediaries (Court of Justice of the European Union, 2014).

Similarly, in 2014 the Paraguayan Senate began the discussion of a bill (popularly known as "Pyrawebs") that would require Internet service providers to keep their users' communications data for twelve months, as well as allow access to these data by the authorities through a court order. The data to be collected included details such as the duration of the connection, the identity of the parties and the geolocation of the users (Sequera, Alonso and Rodríguez, 2014). The Paraguayan organization TEDIC launched a campaign accusing that mandatory data retention as a disproportionate and invasive measure that creates huge potential for abuse by companies and governments, and constitutes a serious infraction to fundamental rights of people. Finally, the bill was rejected both in the Chamber of Deputies and in the Senate (Flores, 2015).

2.2. Mobile phone registry

2.2.1. SIM card registry

For purposes of the present investigation, we refer to mandatory registration of SIM cards as any procedure in which individuals must go through the process of registering a SIM card (subscriber identity model) for their mobile phone using their name (Jentzsch, 2012). A SIM card stores the International Mobile Subscriber Identity (IMSI), which is used to identify a specific user. The technology of a SIM card allows a user to change the device simply by removing it from one phone and inserting it into another, without the need to change anything else, and it contains a unique serial subscriber key (IMSI), as well as authentication information and encryption, temporary information related to the network, and two identification and blocking passwords (PIN and PUK) (Aririguzo and Agbaraji, 2016).

The mandatory registration of SIM cards is used to associate a specific microchip with a specific user and identified accurately. This type of procedure is similar to KYC procedures ("Know your customer") applied by banking entities to prevent money laundering activities. Processes of this type are characterized by collecting a certain amount of information related to the identity of a person and possibly contrasting this information against a total or partial list, for example, a list of politically exposed people, individuals with a criminal record or directly with the database of citizens registered as legal residents of a certain country.

The mandatory registration of SIM cards usually has as its main purpose the regulation and control of anonymous transactions. In general, law enforcement agencies tend to be concerned about the apparent link between the anonymous mobile phone market and criminal and terrorist activities (Gow and Parisi, 2008). However, the real existence of this link is doubtful, being the case that two thirds of terrorists operate under their real identity, and 80% of the countries that have been most affected by terrorist activities already have national systems of identity (a third of which even use biometric technologies). There is no evidence that the implementation of such national identity systems has any influence on terrorist activity (Privacy International, 2004).

In countries such as Canada, where the collection of personal information by a service provider is subject to a reasonable opportunity test, requiring verification of identity by telecommunications companies is considered an invasion of privacy, since said information is not necessary to

provide the service and, consequently, it is considered as neither reasonable nor appropriate to require it (Gow and Parisi, 2008). Some researchers have argued that the compulsory registration of SIM cards would not only constitute an illegitimate invasion of users' privacy, but would especially affect a specific sector of the population that has prepaid cards for a series of reasons, among them, the lack of financial credit.

The central argument for implementing the registration of SIM cards and the collection of personal information as a result is that this practice would help the fight against terrorism, by making the anonymity more difficult. On the one hand, the lack of correlation between mandatory identification systems and the prevention of terrorism has been demonstrated for a long time (Privacy International, 2004); on the other hand, several researchers have argued that, in the face of closer scrutiny of the notion of "anonymity", it is clear that this condition is not an absolute, but a spectrum. Wallace (1999) defines anonymity as the impossibility of coordinating the characteristics of a person in order to establish their identity. On the other hand, Gary Marx (1999) has described seven categories of identity characteristics:

- Legal name
- Location
- Trackable pseudonyms
- Non-traceable pseudonyms
- Patterns of behavior
- Social or physical attributes
- Eligibility / non-eligibility symbols

In this sense, and following Gow and Parisi, in an anonymous prepaid contract, the telephone number serves as an "opaque identifier", which can be used to track calls and make payments, thus providing an extremely limited mechanism of anonymity, by becoming a piece of central information to coordinate other features that allow to determine the identity of the user. Anonymity, although central to the very notion of privacy and freedom of expression (Kaye, 2015), is not an absolute state that is achievable for a mobile phone user. Even in the ideal scenario (a customer activates a prepaid line using cash), several of the conditions indicated by Wallace to determine the identity of the user are maintained. Even an opaque identifier, such as a user's telephone number, provides the possibility of generating at least three pieces of information for identity determination.

The notion that collecting a greater number of pieces of information around the telephone activity of users would contribute to the fight against crime is part of the erroneous principle that sustains that people

who choose to get involved in criminal activities would do this by using phone lines registered by their name. In reality, it is most likely that criminals adopt an alternative tactic, either illicitly cloning third party SIM cards, using foreign SIMs in roaming mode or adopting satellite and Internet telephony technologies (Donovan & Martin, 2014).

Given that this assumption is false, the implementation of SIM card registration mechanisms usually translates into behaviors that compromise the privacy of citizens whose activities are

legal, thus affecting their basic freedoms through a cooling effect on freedom of expression (Donovan and Martin, 2014). In particular, the compulsory registration of SIM cards violates any potential for the exercise of anonymity, a restriction that discourages the free flow of ideas and information (OHCHR). In accordance with the Principles on Communications Surveillance, these types of measures applied to the general population are not proportional to international human rights principles, especially the right to express oneself anonymously, and states should avoid demanding the identification of mobile phone users.

Notwithstanding this, several Latin American countries have regulations that require or seek to require the creation of compulsory SIM card registrations, information that is added to the already existing data that the telecommunications companies retain by law to identify the users before the authorities.

2.2.2. IMEI registry

The IMEI (International Mobile Equipment Identity) is a number consisting of fifteen decimal digits that allows the identification of the brand and model of a mobile device, as well as its serial number. Through the IMEI code, a mobile operator can track the use of a specific devices very quickly, when used in the same mobile network (Aririguzo and Agbaraji, 2016).

The registration of IMEI is carried out through the collection of information of each active mobile device, by including in a database both the IMEI number and specific information about the user who owns the device. The main argument used to defend the imposition of mandatory registration measures of IMEI is usually the prosecution phone theft crimes. Thus, by knowing the IMEI number of a device that has been stolen, operators can trace their networks and identify the person who might be using the device, along with the SIM card being used, and can also block the device. They can deny access of said user to the system, either by blocking the SIM card (which prevents the line from being used) or by blocking the IMEI code (which completely disables the device for use with any SIM card). Those who propose this measure argue that the implementation of the IMEI registry would not only combat the sale of stolen phones, but would help fight other crimes, such as kidnappings.

Broadly speaking, the IMEI registration system works through one of two possible models: in the "whitelist" system, customers can use their devices only if they have been registered with the telecommunications company; if they are not registered, companies must deny the service until they are registered.

In the "blacklist" system, devices are considered legitimate by default, with the exception of those that appear on the list. This consists of a record of the IMEIs associated with mobile devices to which service must be denied, since they have been reported as lost or stolen. For this system to work, the list must be centralized through the different operators, so that those devices that have been reported do not work in any of the different networks (GSMA, 2017).

The implementation of an IMEI registration system under the whitelist model usually implies a moratorium of the registration of devices that where in operation prior to the enactment of the

law. This means that a cut-off date (or "blackout") is established in which all devices that have not been registered are disconnected from the service. This measure can cause serious risks to human rights; For example, in Kenya, in 2012, the authorities disconnected the telephone lines of around 1.5 million citizens, since the IMEI codes of their devices were not in the international database. In this case, the measure sought to combat the sale of counterfeit phones (copies of popular brands and models made with cheap materials), in order to "protect consumers of inferior phones, safeguard mobile payment systems and prevent crime" (Chebusiri, 2012).

By the application of this measure, hundreds of thousands of people were affected, not only on their ability to communicate freely, but also their only means of accessing and participating in the economy, since for many of them their mobile phones where their only way of communicating with clients, access the internet and even doing transfer payments. Going back to the case of Kenya, the international organization Article 19 pointed out that the measure was disproportionate and that, consequently, the principles of necessity, proportionality and legality, where not supported by the evidence, since it was possible to achieve the same goal through other measures.

Many who use "counterfeit" devices, particularly the poor who live in the periphery and in rural areas, are unaware that their devices are counterfeit. Most of them cannot distinguish the difference from a genuine artifact, and many of them buy them from registered distributors, under the presumption that the product is genuine. Some may not have the ability to buy or change their device due to the prohibitive costs associated with new purchases or changes (Article 19, 2011).

In most countries, the blacklist system for the registration of IMEI predominates. In Guatemala, for example, the Mobile Terminal Equipment Law (Decree 8-2013) was created in 2013, which established the obligation of mobile telephony operators to cancel lines when users have not been registered within a period of three years, which was completed on October 8, 2016. The standard simultaneously contemplates a SIM card registration (which includes all the client's basic personal data) and an IMEI record based on a blacklist system (denominated "Negative Database" by the law), containing the IMEI information of mobile devices that have been reported as stolen or lost. Other countries have adopted partial or fragmented whitelist systems: in Ecuador, since 2014, it is mandatory that all mobile phones that enter the country by air are registered in a database maintained by the Superintendence of Telecommunications of Ecuador (Supertel) and the National Customs Service of Ecuador (Senae). So that a device can be registered, the brand and model must be approved in Ecuador and not be reported for theft in Ecuador, Colombia, Peru and Bolivia (El Mercurio, 2014).

3. Colombia

3.1. Data retention

In Colombia, Decree 1704 governs the measure of data retention of communications in the context of the criminal investigation, while Law 1621 of 2013 does the same with respect to intelligence activities.

Decree 1704 requires service providers to safeguard information about their clients' communications that allows them to know their geolocation in real time. On the other hand, Law 1621 requires retaining the user's communication history, the technical identification data of the subscribers that are part of the communication and the geolocation data. In both cases, the data must be kept for a period of five years, and in both cases, the wording of the legal text is vague and imprecise, raising doubts about what "the communications history" means, or whether the obligation to retain data also extends to data derived from Internet browsing. Law 1704 refers to geolocation data, conceptualizing it as "specific information contained in its databases, such as sectors, geographic coordinates and power", which opens the possibilities of interpretation by the authorities or telecommunications companies.

3.2. Registration of mobile phones

Decree No. 1630, of May 2011, creates a national registry of mobile phones, through the adoption of two databases. The negative database contains the IMEI of the devices that have been reported as stolen or lost, both in Colombia and abroad, while the positive database includes the mobile equipment imported or legally manufactured in Colombian territory. The latter connects the IMEI with the identity of the user, who is required to provide the telecommunication operators with their full name, type and identity document number, address and telephone number. Operators are obliged to verify this information with different databases, including the national database of identity documents, the registry of marital status and credit history databases (Privacy International, 2017).

In the Colombian case, although there is no mandatory registration of SIM cards, the IMEIs are associated with a specific user. In addition, to ensure that all legitimate IMEIs are registered in the positive database, a verification system was implemented that requires service providers to detect and register each IMEI that generates activity in their networks, which is carried out through a metadata analysis called CDR. The information collected and analyzed includes the IMSI and IMEI codes, the date, time and characteristics of the activity, and the coherence of these data. After this analysis, all IMEI considered as "irregular" are blocked.

The creation of the IMEI registry has been criticized within Colombia, as civil society organizations consider the amount of information required to elaborate the positive database excessive, as well as to the possible risks in the handling of this data. Furthermore, the homologation of equipment prior to registration and acquired abroad has given rise to various inconveniences: at

the beginning, a payment was required, which left the option out of reach for most people and, subsequently, although this constraint was eliminated, the registration procedure still required a level of technical knowledge that affected the common user. Subsequent to this, the procedure was again modified to facilitate access to the population in general (Sáenz, 2016).

4. Brazil

4.1. Data retention

The Brazilian telecommunications agency, ANATEL, requires ISPs to retain connection records for a period of one year. This requirement is ratified by Law No. 12,965 / 24, commonly known as the Internet Civil Framework, which establishes that:

[W] hen providing an Internet connection, the corresponding independent provider system has the duty to store the connection records, in confidentiality and in a secure and controlled environment, for a period of one year, in accordance with current regulations. The connection registers make up the set of data concerning the start and end date and time of an internet connection, its duration and the IP address used by the terminal to send and receive data packets.

The same Law, in Article 15, establishes the obligation of the service providers to keep the records of access to Internet applications in confidentiality and in a controlled and secure environment, for six months. Both this period and the aforementioned period can be extended by means of precautionary motions, without any law establishing the maximum period for such extension. At the same time, internet connection service providers are required by resolution 614/13 to retain connection records and account information of their subscribers for at least one year.

On the other hand, the requirements for fixed and mobile telephony providers are even greater, since resolutions 426/05 and 477/07 establish that these must keep the data of telephone records available to ANATEL and other interested parties, for a period of at least five years, without indicating a maximum limit for retention. In the case of fixed telephony, it is not clear which data are included in the concept of "telephone registration", while regarding mobile telephony, the regulation refers to data on incoming and outgoing calls, date, hour, duration, price and account information of the subscribers.

These call records, in accordance with the provisions of the Law of Criminal Organizations in its Article 17, must be kept at the disposal of the authorities for the aforementioned period.

4.2. Registration of mobile phones

The above-mentioned Resolution 477/07 establishes minimum requirements regarding the personal data that users must provide to contract a mobile telephone service: their name, their identity document number, their tax identification number and their address. In 2016, this requirement was reinforced by the adoption of Law No. 16,269, of July 5, 2016, which establishes the mandatory registration of SIM cards at the time of their sale, a record that must contain the full name of the purchaser, address, ID number and tax identification number and the chip authentication number, all of which must be verified by presenting official documents, of which the product supplier must keep a copy.

Although the data required by this law is the same as that mentioned in resolution 477/07, the main difference lies in the fact that Law No. 16,269 establishes sanctions of up to 10,000 tax units, including the seizure of the provider´s inventory of available products at the time of application of the sanction, in case of recidivism.

Law No. 16,269 was presented as a tool to fight crimes such as false kidnapping and the use of cellphones by criminals from prison. However, beyond the lack of evidence of the link between the compulsory registration and the crime rates, it has been seen that the registration system hinders the access of tourists, who need to register in advance to obtain a Brazilian tax identification number before acquiring a telephone line for their stay (Costa, Casemiro and Pessoa, 2015).

In 2013, ANATEL issued a series of measures with the purpose of denying mobile telephony services to counterfeit devices (called "xing-ling") as of January 2014. By that time, it was estimated that these devices represented more than 12% of the entire market (Carneiro, 2013), around 34.5 million mobile devices. However, the effective implementation of this measure has been at least problematic, as it is a gigantic and complex data bank. Thus, ANATEL has postponed the measure, which only entered into an "experimental phase" in 2016.

In this context, the Institute of Technology and Society of Rio, together with the international organization Access Now, forwarded their concerns regarding the implications of this measure on human rights to ANATEL. Since most of these users have acquired the devices acting in good faith, denying them access to the Internet and communications violates their right to freedom of expression and access to information. In addition, this type of measure disproportionately affects the most impoverished users, who usually have less expensive devices, and for whom their replacement or acquisition of a new phone would be practically impossible.

5. Peru

5.1. Data retention

Legislative Decree No. 1182 of July 2015 (popularly known as the Stalker Act) established a mandate to retain data "derived from telecommunications" for three years. This mandate provides details regarding the communications whose extension and scope is not specified by the regulations at the disposal of the police agencies, although it does require the prior existence of a judicial authorization. However, this law has been criticized by civil society, since it was created directly by the Executive Power through an exceptional mechanism and without prior debate (Morachimo, 2015). Likewise, this Legislative Decree is not sufficiently clear when describing which data is included in the generic concept of "data derived from telecommunications", an ambiguity that human rights organizations have assessed as dangerous.

At the same time, Law No. 27,336 had already established an obligation under which the entities under the control of the Private Investment Supervision Agency in Telecommunications should keep the source records and the billing details of the services provided for a minimum of three years.

Moreover, the Peruvian Criminal Procedure Code, Article 230, states that telecommunications service providers are obliged to provide geolocation information for mobile phones, as well as the intervention, recording or registry of communications, immediately, in real time and without interruption, when ordered by a court. On the other hand, since Decree 1182 came into effect, the court order is no longer necessary, since the police agencies may require the operators the access to geolocation data of their users in real time, without any prior authorization.

5.2. Registration of mobile phones

Since 2015, companies that provide mobile telephony services in Peru are required to verify the identity of their users of prepaid services at the time of contracting. The obligation of this verification came into effect in January 2017, and is carried out through biometric identification systems connected to the database of the National Registry of Identification and Civil Status. This information is centralized by OSIPTEL in the National Registry of Mobile Terminals, which in turn contains the information of all users who have contracted services in any form (OSIPTEL, 2015).

Thus, the Regulation of Law No. 28,774 establishes that service providers must have a Private Registry of Subscribers, which must include the name and surname of each user, their identification number (DNI, ID card, immigration or Unique Taxpayer Registry), the phone number and the brand, model and series of the mobile device, even when the equipment has not been commercialized by the company in question. In addition, the Regulation obliges telecommunication service providers to implement an automated system that allows them to register a subscriber that uses his SIM card in a different device different from the one registered. Likewise, they must give OSIPTEL the records of the mobile terminals that are reported as stolen, lost or recovered.

On the other hand, in January 2017 Legislative Decree No. 1338 was promulgated in Peru, by which the National Registry of Mobile Terminal Equipment for Security (RENTESEG) was created, with the alleged purpose of "preventing and fighting theft, robbery and illegal trade in mobile terminal equipment." This decree creates a system of black and white lists, determining that only the teams incorporated in the whitelist are enabled to operate in the network, and that the devices reported as lost, stolen or inoperative would be disabled. When activating a mobile device, the IMSI and the IMEI are thus associated with the specific identity of the authorized user for a certain device. With the entry into force of this decree, companies providing telecommunications services are obliged to verify the identity of the user at the time of contracting the service, through the system of biometric verification of their fingerprint.

6. Argentina

6.1. Data retention

Although Argentina does not have law that explicitly establishes the obligation to retain data, the regulation on the quality of telecommunications services includes the obligation of service providers to guarantee the access to any information that the authorities consider relevant to the performance of evaluations of service quality. As a consequence, Article 8 of this Regulation obliges telecommunications companies to keep their system´s data, for a minimum of three years.

Likewise, Law No. 25,873 and its corresponding regulatory decree established the obligation of the telecommunications service providers to register the filial and domiciliary data of their clients, as well as the traffic records of their communications, and systematize them at the disposal of the Judicial Power and the Public Ministry, for a period of ten years. However, this law was declared unconstitutional for violating the principles of necessity, legality and proportionality.

6.2. Registration of mobile phones

In November 2016, through the Joint Resolution No. 6-E / 2016, the Argentine Ministry of Communications and the Ministry of Security created the User Identity Register of the Mobile Communications Service. Under this regulation, it is sought to promote the naming of all telephone lines existing in the country, responsibility that lies with the operators of the telephone service. Given that, in practice, postpaid lines are already associated with a registered holder, the objective of this regulation is to generate a record of the prepaid lines. The first problem presented by this regulation is of a formal nature and lies in the fact that this provision has been issued by administrative means; it should be remembered that one of the main requirements of legal restrictions on fundamental rights is that they must go through the ordinary legislative process.

In addition to the registration of telephone lines, in 2016 ENACOM enabled a website where Argentine users can consult the GSMA database, containing an international blacklist of the IMEI codes of stolen or lost cellphones. The devices which IMEI is on that blacklist will be denied service by the operators, so that the list serves as a tool through which a user can know if a certain device will work in the mobile network before acquiring it (Sametband, 2016). Consequently, it is clear that the system has certain limitations, since the user needs to have the mobile device in hand, or in any case the IMEI code of the device, before making the transaction.

In this context, the vagueness of resolution 6-E / 2016 when determining which data should be requested for registration purposes is particularly worrisome, since it leaves this important decision in the hands of the service operators. Although it is proposed as a record of the telephone lines, and not the devices, the set formed by both regulations has been presented as a single system, and the Minister of Security declared that "[i]f a new chip is connected to a telephone in the list, the line then must be discharged." The norm, moreover, is insufficiently clear with respect to the reasons that the Public Prosecutor's Office or the Judicial Power may claim to regain access to the Registry, as well as the terms of said access (ADC, 2016).

7. Mexico

7.1. Data retention

The Federal Telecommunications and Broadcasting Law obliges companies providing telecommunications services to conserve the metadata of their users' communications for two years. In opinion of the Supreme Court the request for these data must be preceded by a judicial order. The National Code of Criminal Procedures allows the geographic location of communication devices in real time, although it establishes that the intervention of communications and extraction of identification data will require judicial order. Likewise, the Code establishes that service providers will be obliged to deliver to the Public Prosecutor's Office, following a court order, the data stored with respect to their users in the field of service provision. This Code does not establish any type of parameter or limit with respect to what data the service provider must keep, for how long or under what standards or criteria.

For its part, the Federal Telecommunications Law delimits a very broad spectrum of data related to communications that must be kept by service providers, in order to deliver them to the authorities when they are required. Among these data are:

- the type of communication (voice transmission, voice mail, conference, data),
- supplementary services (including call forwarding or transfer), messaging or multimedia services (including short message services, multimedia and advanced services);
- necessary data to track and identify the origin and destination of mobile telephony communications:
- destination number, modality of lines with a contract or tariff plan, as in the modality of prepaid lines;
- necessary data to determine the date, time and duration of the communication, as well as the messaging or multimedia service;
- the date and time of the first activation of the service and the location tag (cell identifier) from which the service was activated;
- the digital location of the geographical positioning of the telephone lines.

7.2. Registration of mobile phones

Between 2009 and 2011, the Mexican Federal Telecommunications Law contemplated a policy of registering mobile telephony users through the National Registry of Mobile Telephony Users (RENAUT). This registry was created by means of a resolution of the Federal Commission of Telecommunications, with the purpose of holding the service providers accountable to collaborate with the authorities in the prosecution of crimes committed by the users. In practice, the RENAUT associated each mobile phone user with its national identification number (Unique Population Registration Code, or CURP). Article 44 of the Telecommunications Law of 2009 obliged concessionaires of public telecommunications networks to keep a record of their users' data

(both in prepayment as in postpaid) that should include, as a minimum, the modality number of the telephone line, the full name, address, nationality, number and other official identification data and the printing of the user's fingerprint. This same article established that the concessionaires had the obligation to preserve the photostatic or electronic copies of the documents that would serve as support for said registry.

Despite the fact that this legislation sought to establish mechanisms to improve communications between telecommunications concessionaires and the authorities called to fight crime, the law was reversed only two years after its enactment, after lawmakers of the RENAUT admitted that it had not helped the prevention, investigation and prosecution of the crimes it sought to combat, since in 2010, the first year of registration, the number of kidnappings rose by 8% compared to 2009 (Torres Mercado , Castro Trenti, and González Alcocer, 2011). Likewise, before the implementation of the registry, around 4,400 extortion calls were carried out per day, a number that increased by more than 40%. In the Mexican case, after the failed that RENAUT turned out to be, it was understood that the claim that a mobile phone registry should lower crime rates was based on the assumption -the error- that criminals would use registered devices under their own names.

As other studies have pointed out, the registration of a mobile phone through a unique identification number, such as the CURP, does not guarantee that the data is true or remains valid, especially when no incentives were established for people to maintain their updated data. In the Mexican case, on the contrary, the obligation to register the devices generated incentives for the theft of mobile equipment. These factors, coupled with the enormous ease of defrauding the registration system, creating inconveniences for innocent users, led Congress to repeal the National Registry of Mobile Telephony Users in 2012, just two years after its entry into force, determining that it had not contributed "to the prevention, investigation and / or prosecution of related crimes". Among other arguments, it was pointed out that the measure not only did not guarantee the veracity of the data, but could lead to falsely accusing a person who had been the victim of identity theft. In this sense, it was assessed that it was possible that the policy had encouraged criminal activities such as the theft of mobile phones or the cloning of SIM cards. Together with the elimination of the RENAUT, the data collected because of its implementation was eliminated, together with the backing of the verification data contemplated in the aforementioned article 44.

Currently, Mexico maintains a blacklist system of IMEI codes; users can report a device as stolen or lost, and companies providing mobile phone service are required to maintain a database and settle agreements that allow them to exchange information about devices reported as stolen or lost, so that the activation of devices that show IMEI codes in said database is denied (Instituto Federal de Telecomunicaciones, México).

8. Chile

8.1. Data retention

In Chile, the statute on data retention is dispersed among various regulatory bodies.

According to the General Telecommunications Law (Article 24H) the service providers have obligations, among which is to protect the privacy of its users and comply with general duties of confidentiality. This obligation is restated by the Regulation of Telecommunications Services (decree 18 of 2014), which in its Article 50 states that Internet service providers will seek to preserve the privacy and security of users in the use of said service. However, the breadth and vagueness of this obligation forces us to ask ourselves what we should interpret for privacy and security in the context of this regulatory framework.

In contrast to the general and diffuse nature of the General Telecommunications Law and bylaws, criminal legislation offers more specific regulations on the matter. The aforementioned article 222 establishes that the judge will be competent to order, at the request of the Public Ministry, the interception and recording of phone or other communications of a person, when there are well-founded suspicions, based on certain facts, that said person has committed or participated in the preparation or commission, or will currently prepare the commission or participation in a punishable act worthy of crime.

The Code of Criminal Procedure (hereinafter referred to as CPP) requires that, in the case of requesting the intervention of telephone communication, a series of prerequisites must be met so that the judge authorizes the measure. These requirements, as seen in the text of the law, are exhaustive compared to the requirements of other measures considered in the same regulation (for example, those related to the interception of correspondence), thus generating a disparity regarding the intervention of communications made through a mobile device when these are considered correspondence or when they are considered phone communication. Thus, a judge will require fewer requirements to intervene an email than to intervene a call, which indicates that the rule did not foresee the advancement of technology, bearing in mind that mobile phones and similar devices gather more information than any other communication mechanism.

This means that the telephone companies are obliged to provide the officials in question with the facilities necessary for such a measure to be carried out at the required time. For this purpose, providers must maintain an updated list, with a reserved nature and at the disposal of the Public Prosecutor, which contains their authorized ranges of IP addresses, as well as a minimum one-year registration of the IP numbers of the connections made by their subscribers. It is in this provision that the first serious failure in the drafting of the law is evident, since it does not indicate a time limit regarding the maximum time by which suppliers can store the data collected, a circumstance that disclaims the proportionality of the measure. The current Chilean legislation on personal data does not establish temporary limits with respect to their retention, and also omits to prescribe parameters related to the minimum conditions and security standards for the storage of the data, as well as its final elimination.

Although the wording of the legal text is at least ambiguous concerning the extent and scope of the data to be collected by service providers, the Public Prosecutor's Office, through the Official Letter FN No. 060-14 ("General instruction that impart criteria applicable to the investigation stage in the criminal process ") confirms that these companies do not limit themselves to keep track of IP numbers, but also collect other metadata, including, for example, the data related to the traffic of calls and messaging services:

Prosecutors, when making a request to the respective Court, must indicate the scope of the interception they are bidding, for which they will expressly indicate if the interception requested is only of voice, or in addition, they require that the court authorizes obtaining calls traffic, the information coming from the messaging services or other forms of telecommunication that are possible to intercept, according to the technical capacities of the operators.

Decree 142 (Regulation on Interception and Recording of Telephone and Other Telecommunication Communications) establishes the mechanisms for executing the intervention and registration of communications, stating that these must be carried out in the terms determined by a judicial order, and that the procedure must respect the privacy and security of communications that fall outside the scope of the measure. This norm establishes a minimum term of six months for the conservation of the IP data of the users; however, as it is a regulation, the legal mandate contained in the CPP prevails, where the minimum term is one year.

None of the abovementioned regulations establishes a time limit for the retention of data, nor minimum standards regarding its conservation, security and deletion. In general, the consensus regarding the current Chilean legislation on personal data is that protection is weak and insufficient (Viollier, 2017). Rather than offering protection to the rights of individuals, it creates a regulatory framework for the market of personal databases. In the absence of safeguard mechanisms and standards for the conservation of data, current legislation allows them to be sold, even across borders, without the user's consent. On the other hand, the absence of effective sanctions and the lack of a control authority also weaken the protection that this law could offer.

Chile is currently preparing a bill on personal data, a project that has been awaited and negotiated for a long time, and that probably will not get to see the light due to a current legislative agenda focused on electoral issues (Viollier, 2017b). This project would introduce various changes to the existing protection of personal data, among them, the right to the portability of personal data, which would allow citizens to request a copy of the data that concerns them, and creates a special procedure for the exercise of access and rectification rights. In this sense, the project pursues a more stringent protection to the requirement of prior consent by the owner of the data, a requirement that is treated rather laxly by the current law.

On the other hand, the project limits the current concept of personal data, excluding those data that are not identifiable by "reasonably used means". This ambiguous concept is, at least, dangerous, as it opens spaces for the abusive treatment of data that may be considered "unqualified" for the protection granted by law.

On the other hand, the current law does not include a time limit of data retention, and the current text of the project preserves this problem while trying to solve it, stating that "[t] he personal data

must be kept only for the necessary period of time to fulfill the purposes of the treatment. " This parameter does not differ from the current text, which states that "[t] he personal data should be eliminated or canceled when its storage has no legal basis or such legal basis has expired." These programmatic norms do not respect the principle of proportionality and constitute insufficient and diffuse limits, which leaves spaces for abuse by public and private organizations as well as companies providing the service.

8.2. Registration of mobile phones

In March 2017, Chile implemented an IMEI code pre-registration policy, that is, a whitelist system that requires mobile devices to appear in the registry before being activated. Until now, Chile had managed a blacklist registry, which allowed users to report the devices when they were stolen, so that mobile operators can proceed to block them. The new regulations, called the Cellular Labeling Law, require that users who acquire mobile devices outside of Chile get to an office authorized by the Chilean Undersecretariat of Telecommunications (Subtel), where the IMEI code will be registered, along with other data such as the operating system of the device. This last measure will become effective as of July 2017. The database, as it is described in the law, does not contemplate registering the user's name or other information related to this, such as address; however, the effort necessary to cross that information with the information relative to the ownership of the telephone line is negligible.

In this regard, at the time of writing these lines, several bills are being discussed in Chile concerning the registration of SIM cards for cellphones, which are intended to be added to existing regulations on data recording and preservation in the field of telecommunications and in the criminal procedural scope.

The first of these bills (Bulletin No. 9767-15) entered the Chamber of Deputies on December 9, 2014. In this text, mobile telephone operators are required to register the personal data of those customers who acquire a line in the prepaid mode. The text reveals that its central purpose is to reduce the number of prank calls that affect the emergency number of Chilean police and, secondly, to prevent criminal acts related to the placement of explosive devices. Legislators argue that both circumstances could be avoided in case there is a record that does not allow the anonymity of those who perpetratesuch acts, given that, as affirmed, this would allow the perpetrators to be prosecuted more appropriately. It is important to point out that this text takes as a precedent the already mentioned Directive of the European Union, which, as we point out, was left without effect by the European Court because of its severe problems regarding the protection of human rights.

The text of this bill contains just five articles, which contemplate the obligation of mobile phone operators to keep the SIM card registry of the prepaid devices to which they provide service, a record that must contain the first and last name of the user, their nationality and their ID card number. According to this project, the registry should be sent to the Undersecretariat of Telecommunications every six months, as well as delivered to the police authorities and the Public Prosecutor's Office if they request so, with the purpose of investigating and prosecuting acts constituting a crime. Likewise, fines of ten to fifty tax units are established in the event that com-

panies fail to comply with these requirements. This extremely concise proposal, omits to indicate parameters for the conservation of these data, including a maximum time of conservation. On the other hand, it does not establish sanctions associated with non-compliance with the registration obligation, despite the fact that in its explanatory part it states that the SIM is intended to be blocked if the relevant registration is not carried out.

Meanwhile, two bills involving mobile device registration rest in the Senate, referring to the same issues as the aforementioned project, but separately. In 2014, members of the Upper House presented a project about prank and futile telephone calls made to emergency services, and in 2015, the discussion of a second parliamentary motion related to the collection of prepaid service user data began. Both consist of modifications to the existing General Telecommunications Law.

The first of these two projects (Bulletin No. 9597-07) intends to impose telecommunications service providers the obligation to deliver the information of its users to both the Chilean Police and other emergency services, with the purpose of sanctioning the improper use of calls to these services. Among the fundaments of this project it is argued that 80% of calls to the emergency service "133" consist of informal communications, pranks and reports of false incidents, arguing that the reason for this phenomenon is the lack of sanction of such behaviors. This project does not propose the collection of additional data from users, but makes it clear that the data with which companies currently count (such as the geographical location according to the device's connection cell) are sufficient to identify users. Thus, it only contemplates that providers must provide the authorities with these data in relation to citizens who make use of emergency services.

The second project (Bulletin No. 9894-15) establishes the obligation to collect data from users of prepaid phone services, in view to their individualization, that is, it constitutes a regulation for mandatory registration of mobile devices.

This project focuses on the registration of prepaid phones, thus framed in a regional and global trend that aims to assimilate the flexibility of this type of service (given the absence of a contract and certain formalities that the postpaid service implies) with anonymity, and the latter with the will and facility to commit a crime. Thus, in the foundations of this project it is pointed out that in Chile there are currently more than sixteen million prepaid phones, equipment that must also be registered if the standard is approved. However, the law states that it seeks to interfere as little as possible in the characteristics and flexibility of the prepaid service, focusing primarily on the diversity of commercial premises where a SIM card can be purchased.

Thus, the data to be requested for the creation of this record is the user's full name, address, identity card or passport number, as well as the technical data of the device and the SIM card.

The most important difference between these projects lies in their purposes. While the project related to the prank and fake calls seeks to address a specific problem through proportional measures which does not involve the collection of additional data. On the other hand,the House of Representatives project seeks nothing but the elimination of anonymity in mobile communications, a measure that would not only affect the free flow of information, but would also harm the most vulnerable sectors of the population. Although the project itself affirms that it seeks to interfere as little as possible in service provision schemes, it is inevitable that a measure of this type will affect

its operation. The mandatory registration of SIM affects the market in various ways, including a decrease in active SIM cards and therefore in the number of users, a rise in transaction costs associated with the change of telephone company, an increase in the information available in the hands of telecommunications companies (which results in the profiling and merchandising of these data); all these costs will be passed on to the end user.

9. Conclusions

Following the mentioned principles, which should govern the application of measures that restrain the free transit of communications, the first thing we must point out is that a priori data retention measures should never be required, as they entail the management of enormous amounts of information on the communications of all users, generally under the justification of pursuing crimes that are only committed by a fraction of them. As the UN Human Rights Council has pointed out, measures of this nature are never necessary or proportional (UNHRC, 2014).

The same applies to the compulsory registration of SIM cards, a practice that violates the right of individuals to express themselves anonymously, as well as severely affecting access to communications by a significant fraction of the population. In this sense, David Kaye, Special Rapporteur for the promotion and protection of the right to freedom of expression of the United Nations, has pointed out that measures such as the compulsory registration of SIM cards:

[D] irectly undermine anonymity, particularly for those who access the internet only through mobile technology. The mandatory registration of SIM cards can provide governments the ability to monitor individuals and journalists beyond any legitimate government interest.

A second concern about this type of measures lies in the possibilities of transmission and exchange of these data to be crossed or combined with other information bases. For example, in protest contexts it is possible to apply simulators of mobile telephony towers and thus extract information from citizens who are present, which can then be crossed with user databases to identify them without a trace. This risk is even worse in the case of countries that use biometric technologies.

On the other hand, as we analyzed at the beginning of this report, following the categories of identity of Gary Marx, the data that are already in the hands of telecommunications companies are more than sufficient in most cases to fully identify a user, without the necessity to store or collect a greater amount of information.

Continuing with the application of the principles, we find other conflicts in the legislations analyzed. In those countries where measures of data retention or SIM card registration are taken by administrative means, the principle of legality is violated. This is the case of Argentina, whose mandatory registration of SIM cards was created through a joint ministerial resolution, and is also the case of Peru, where the mandate to retain telecommunications data was created by a legislative decree.

Finally, the existence of judicial guarantees is an indispensable requirement, on the understanding that access to these data by the investigative and police bodies must be done on a case-by-case basis and prior a court order.

In terms of data retention, Peru currently allows, by virtue of Decree 1182, that police bodies require operators to access geolocation data of their users in real time, without any prior authorization (Morachimo, 2015). However, in terms of registration of SIM cards, it is the usual

practice enshrined in these regulations that telecommunications companies deliver this data in a preventive and periodic manner to an administrative body, without in general establishing any possibility on the part of the user exercise control over these data.

In this sense, we could not make recommendations to the Chilean State regarding the possible creation of a compulsory SIM card registry: it is our opinion that the possible negative consequences of implementing a measure of this nature far outweigh its possible advantages. However, in general terms with regard to existing regulations in Latin America, we recommend states to:

- Ensure that regulations that seek to regulate access to telecommunications comply with the ordinary legislative process.
- Establish clear and precise maximum terms of conservation and registration of communications, which should be brief, taking into account the magnitude of the violation of the fundamental rights that this measure means and its proportionality with the end achieved.
- Establish security protocols for the storage, handling and communication of the registered information, which contemplate precise technical requirements, according to the sensitivity of the information in question.
- Establish sanctions that allow the effective application of these standards to those who fail to comply with them, as well as those who violate the confidentiality duties or use this data for a purpose other than the one with which they were registered.
- Establish guarantees of prior and mandatory judicial control through which the judicial body can guarantee compliance with the suitability, necessity and proportionality requirements of the measure.

References

ADC (2016): "Preocupaciones acerca del Registro de Identidad de Usuarios de celulares". Consultado en: https://adcdigital.org.ar/2016/11/11/preocupaciones-acerca-del-registro-de- identidad-de-usuarios-de-celulares/https://adcdigital.org.ar/2016/11/11/preocupaciones- acerca-del-registro-de-identidad-de-usuarios-de-celulares/

Antonialli, D., & de Souza Abreu, J. (2016). Vigilancia estatal de las comunicaciones en Brasil y la protección de los derechos fundamentales. InternetLab. Consultado en https:// necessaryandproportionate.org/es/country-reports/brazil

Argentina (2016). Ministerio de Comunicaciones y Ministerio de Seguridad: Resolución Conjunta 6 - E/2016. Consultado en: https://www.boletinoficial.gob.ar/#!DetalleNorma/153684/20161110

Aririguzo, M., y Agbaraji, E. (2016), Mobile phone registration for a developing economy: gains and constraints. European Journal of Basic and Applied Sciences, Vol. 3 No. 3, 2016. Consultado en http://www.idpublications.org/wp-content/uploads/2016/05/Full-Paper-MOBILE-PHONE-REGISTRATION-FOR-A-DEVELOPING-ECONOMY-GAINS-AND- CONSTRAINTS.pdf

Article 19 (2011), Kenya: Free expression standards should guide fight against "counterfeit" mobile phones. Consultado en: https://www.article19.org/resources.php/resource/2762/en/kenya:-free-expression-standards-should-guide-fight-against-%E2%80%9Ccounterfeit%E2%80%9D-mobile-phones

Assembleia Legislativa do Estado de Sao Paulo: Lei N° 16.269, de 05 de julho de 2016. Consultado en: http://www.al.sp.gov.br/repositorio/legislacao/lei/2016/lei-16269-05.07.2016.html

Brasil (2007). Resolução nº 477, de 7 de agosto de 2007 – ANATEL- Aprova o Regulamento do Serviço Móvel Pessoal – SMP. Consultado en: http://www.procon.go.gov.br/legislacao/ resolucoes/resolucao-no-477-de-7-de-agosto-de-2007-anatel-aprova-o-regulamento-do- servico-movel-pessoal-smp.html

Carneiro, Flávio (2013). Celulares piratas serão bloqueados pelas operadoras; aprenda a identificar esses aparelhos. UOL Noticias. Consultado en: https://tecnologia.uol.com.br/ noticias/redacao/2013/04/17/detalhes-desmascaram-copias-piratas-de-smartphones-veja- dicas-para-evitar-compra.htm

Chebusiri, W. (2012), Kenya's battle to switch off fake phones, BBC. Consultado en: http://www. bbc.com/news/world-africa-19819965

Chile (2014). Cámara de Diputados. Boletín Nº 9767-15. pp. 1-2. http://www.senado.cl/

appsenado/templates/tramitacion/index.php?boletin_ini=9597-07

Chile (2014). Senado. Boletín N° 9.597-07.En línea, disponible en: http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=9597-07 [Fecha de consulta: 18 de abril de 2016], p.1.

Chile, Subsecretaría de Telecomunicaciones (2016), A partir de marzo se implementará normativa que reducirá el robo de celulares. Consultado en: http://www.subtel.gob.cl/a-partir-de-marzo-se-implementara-normativa-que-reducira-el-robo-de-celulares/

Chile (2016), Ley de Etiquetado de Celulares: Resolución número 1.463 exenta, de 2016.- Fija norma técnica que regula las especificaciones técnicas mínimas que deberán cumplir los equipos terminales utilizados en las redes móviles. Consultado en: http://www.diariooficial.interior.gob.cl/media/2016/06/16/do-20160616.pdf

Chile (2017). Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Consultado en: https://www.camara.cl/pley/pley_detalle.aspx?prmID=11661&prmBoletin=11144-07

Costa, D.; Casemiro, L. y Pessoa, T. (2015): "Telefonia móvel vira corrida de obstáculos para estrangeiros". O Globo, 25 de octubre de 2015. Consultado en: https://oglobo.globo.com/economia/defesa-do-consumidor/telefonia-movel-vira-corrida-de-obstaculos-para-estrangeiros-17870170#ixzz4gxeVFhUShttps://necessaryandproportionate.org/es/country-reports/brazil

Donovan, K., & Martin, A. (2014), The rise of African SIM registration: The emerging dynamics of regulatory change. First Monday, 19(2). doi:http://dx.doi.org/10.5210/fm.v19i2.4351

Eagle News (2016, August 2), SIM card registration to counter prank calls on emergency hotlines. Eagle News. Consultado en http://www.eaglenews.ph/featured-news/sim-card-registration-to-counter-prank-calls-on-emergency-hotlines/

El Mercurio (2014), Supertel y Senae empiezan registro de aparatos celulares. Consultado en: http://www.elmercurio.com.ec/422020-supertel-y-senae-empiezan-registro-de-aparatos-celulares/http://www.eaglenews.ph/featured-news/sim-card-registration-to-counter-prank-calls-on-emergency-hotlines/

Ferrari, V., & Schnidrig, D. (2016). Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina. Consultado en https://necessaryandproportionate.org/es/country-reports/argentina

Flores, P.(2015), Senado de Paraguay rechaza definitivamente la ley #Pyrawebs. FayerWayer. Consultado en: https://www.fayerwayer.com/2015/06/senado-de-paraguay-rechaza-definitivamente-la-ley-pyrawebs/

Fundación Karisma (2016), ¿Es legítima la retención de datos en Colombia? Consultado en: https://karisma.org.co/descargar/es-legitima-la-retencion-de-datos-en-colombia-2/

García, L. F. (2016). Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México. Red en Defensa de los Derechos Digitales. Consultado en https://necessaryandproportionate.org/es/country-reports/mexico

Gow, G. A., & Parisi, J. (2008). Pursuing the Anonymous User: Privacy Rights and Mandatory Registration of Prepaid Mobile Phones. Bulletin of Science, Technology & Society, Vol. 28(1), 60–68.

GSMA. (2013, November). The Mandatory Registration of Prepaid SIM Card Users: A White Paper. Consultado en http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

GSMA (2016), Mandatory 'real name' registration by prepaid SIM card users: Considerations for policymakers. Consultado en: http://www.gsma.com/newsroom/blog/mandatory-real-name-registration-prepaid-sim-card-users-considerations-policymakers/

GSMA (2017), "Coloured lists. Managed services". Consultado en: http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/coloured-lists/

Guatemala (2013), Decreto Número 8-2013, Ley de Equipos Terminales Móviles. Consultado en: http://ww2.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2013/pdfs/decretos/D08-2013.pdf

Instituto de Tecnologia & Sociedade do Rio y Access Now (2015). Connectivity at Risk/Study on the impact of blocking uncertified mobile devices in Brazil. Consultado en: https://www.accessnow.org/cms/assets/uploads/archive/docs/ITS_Report_English_Final_1.pdfhttp://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

Jentzsch, N. (2012), Implications of Mandatory Registration of Mobile Phone Users in Africa (Discussion papers No. 1192). Berlin: Deutsches Institut für Wirtschaftsforschung.

Kapellmann, D., & Reyes, B. (2015). Retención y Privacidad de Datos: Algunas Lecciones Derivadas de las Diversas Prácticas Internacionales. The Social Intelligence Unit, the-siu.net. p. 9. Consultado en the-siu.net

Kaye, D. (2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. United Nations, Human Rights Council. Consultado en www.ohchr.org/EN/HRBodies/HRC/.../A.HRC.29.32_AEV.doc

Keane, B. (2015, March 18). Your guide to the data retention debate: what it is and why it's

bad. Crikey. Consultado en https://www.crikey.com.au/2015/03/18/your-guide-to-the-data-retention-debate-what-it-is-and-why-it%E2%80%99s-bad/

México, Instituto Federal de Telecomunicaciones (s/f), ¿Te robaron o perdiste tu celular? Consultado en: http://www.ift.org.mx/usuarios-telefonia-movil/te-robaron-o-perdiste-tu-celular

México (2009), Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones. Consultado en http://dof.gob.mx/nota_detalle.php?codigo=5079751&fecha=09/02/2009https://www.crikey.com.au/2015/03/18/your-guide-to-the-data-retention-debate-what-it-is-and-why-it%E2%80%99s-bad/

Morachimo, M. (2015): Nueva norma permite a la Policía saber dónde está cualquier persona sin orden judicial. Hiperderecho, 27 de julio de 2015. Consultado en: http://www.hiperderecho.org/2015/07/norma-policia-geolocalizacion-sin-orden-judicial-1182/

Morachimo, M. (2016). Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú. Consultado en https://necessaryandproportionate.org/es/country-reports/peru

OHCHR (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/23/40. Consultado en: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

OSIPTEL (2015): "Desde hoy las líneas móviles prepago se venderán con identificación dactilar de los usuarios". Consultado en: https://www.osiptel.gob.pe/noticia/desde-hoy-lineas-prepago-identificacion-dactilar

Perú (2015). Ley N° 28.774, que crea el Registro Nacional de Terminales de Telefonía Celular, establece prohibiciones y sanciones. Consultado en: http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_3622.pdf

Perú (2017), Decreto Legislativo 1338 que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana. Consultado en: http://busquedas.elperuano.com.pe/normaslegales/decreto-legislativo-que-crea-el-registro-nacional-de-equipos-decreto-legislativo-n-1338-1471014-4/https://necessaryandproportionate.org/es/country-reports/peru

Privacy International. (2004). Mistaken Identity; Exploring the Relationship Between National Identity Cards & the Prevention of Terrorism (Interim report). Privacy International. Consultado en https://web.archive.org/web/20061209185839/http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf

Privacy International, Access, & Electronic Frontier Foundation. (2014, May). Necesarios & Proporcionados. Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Consultado en https://necessaryandproportionate.org/es/necesarios-proporcionados

Privacy International (2017). State of Privacy: Colombia. Consultado en: https://www.privacyinternational.org/node/977

Rodríguez, K. (2014). La Retención de Datos de Tráfico en Paraguay Es Espionaje Masivo e Inconstitucional. Electronic Frontier Foundation. Consultado en: https://www.eff.org/es/deeplinks/2014/11/la-retencion-de-datos-de-trafico-en-paraguay-es-espionaje-masivo-e

Sáenz, P. (2016), Señores Ministerio TIC: ¿Ya intentaron homologar un celular? Yo sí y ¡no pude! Fundación Karisma. Consultado en: https://karisma.org.co/senores-ministerio-tic-ya-intentaron-homologar-un-celular-yo-si-y-no-pude/

Sametband, R. (2016), Habilitan el sitio Web nacional para verificar si un celular es robado. La Nación. Consultado en: www.lanacion.com.ar/1896940-habilitan-el-sitio-web-para-verificar-si-un-celular-es-robadohttps://necessaryandproportionate.org/es/necesarios-proporcionados

Torres Mercado, T., Castro Trenti, F., & González Alcocer, A (2011). Iniciativa con proyecto de decreto por el que se reforman, adicionan y derogan diversas disposiciones del Código Federal de Procedimientos Penales, del Código Penal Federal, de la Ley Federal de Telecomunicaciones y de la Ley que establece las normas mínimas sobre readaptación social de sentenciados, Pub. L. No. Gaceta LXI/2SPO-228/28925.

Tribunal de Justicia de la Unión Europea. (2014 8). Comunicado de prensa N. 54/14. Consultado en http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf

United Nations Human Rights Council. (2014), The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights. United Nations Human Rights Council. Consultado en http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

Viollier, P. (2017), El estado de la protección de datos personales en Chile. ONG Derechos Digitales. Consultado en: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

Viollier, P. (2017b), Protección de datos: una buena noticia a medias, en un Chile a medias. ONG Derechos Digitales. Consultado en: https://www.derechosdigitales.org/11003/proteccion-de-datos-una-buena-noticia-a-medias-en-un-chile-a-medias/http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

Wallace, K. A. (1999), Anonymity. Ethics and Information Technology, 1, 23–35.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina