DERECHOS DIGITALES
América Latina

TECHNOLOGY FOR PRIVACY AND FREEDOM OF EXPRESSION: REGULATION OF ANONYMITY AND ENCRYPTION:

CHILE IN THE LATIN AMERICAN CONTEXT

VALENTINA HERNÁNDEZ BAUZÁ

Cover page: Violeta Cereceda and Constanza Figueroa.

Layout: Violeta Cereceda.

Translation: Macarena Alliende.

December 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.

1. Executive Summary

Anonymity and encryption are related but different concepts in the digital environment. Anonymity consists of hiding the identity of the issuer of a message (both name and other qualities), without necessarily hiding the content of the message. The encryption of the message hides its content, but not necessarily the data of the communication itself that allows the identification of those who communicate. To ensure the right to privacy in the digital era, both methods must act together.

The questioning of anonymity and encryption has been a fundamental part of the global agenda against organized crime and terrorism, arguing that these techniques are used by highly trained criminals with computer skills to coordinate their actions.

The discussion between the supporters of anonymous and encrypted communications and those who seek to establish technological measures to break the encryption lock is not recent, but the debate has gained relevance with the increase in the use of these measures. The current scenario is one of opposite positions: on the one hand, the position of state investigation and criminal prosecution agencies and on the other, the one of technology companies that resist introducing vulnerabilities to their equipment to avoid compromising traffic safety online, in addition to gaining the trust of its users. In both cases, these actors consist of developed countries or powerful companies, with an important control over the global financial and information flows.

Organizations such as the Human Rights Council of the United Nations or the Inter-American Commission on Human Rights, through their Special Rapporteurs for Freedom of Expression, have emphasized that the use of anonymity and encryption tools are key elements to adequately protect the right to privacy and thereby guarantee other rights such as freedom of expression.

Sectors that see a threat in the use of encryption technologies have adopted measures such as the insertion of vulnerabilities in the systems, the request of copies of the keys that allow deciphering the hidden content and the provision of technical capabilities and authorizations to break the encryption, through brute force. All of them present different risks, not only to the rights and fundamental freedoms of users, but to the secure traffic of the network, which would be exposed not only to the entrance of authorized public officials, but also to hackers and others individuals with malicious intentions.

There are at least three interests that should be considered in the regulation of these matters: public safety, the right to privacy and security in the exchanges of information online. Therefore, the solutions must keep a balance among them.

It is proposed to allow access to content or fragments of communication in specific cases, given a prior judicial order, thus protecting all interests at stake. The training of officials responsible for investigation, prevention and criminal prosecution is also proposed, so they can be in better conditions to face the digital criminal activity, being able to foresee and combat the latter in a more effective way, avoiding the most burdensome actions regarding privacy and other rights, turning to access measures as a last resort. Most notably, the introduction of vulnerabilities is rejected, as well as the hacking done by the state aimed at obtaining information about both; the identity of the individuals and the content of their communications.

Chile is in a Latin American context where, in line with the regional trend, there is a tendency to reduce the areas of digital anonymity, even though, as a general rule, it is not prohibited. Although in the process of Chile's National Cybersecurity Policy the value of encryption is recognized, government actions aimed at diminishing the ability to sustain communications anonymously have remained strong.

2. Introduction: Anonymity and Encryption

It is not new that the internet is an extremely important form of communication to inform, communicate and express personal opinions. The same reality is part of Latin America. In 2010, it was already said that it is the largest source of information in the world.[1] As a matter of fact, the network is the main source of telecommunications, which has only increased since the mass use of smartphones. The threats that this presents include the current technical capacity available to governments and private entities to monitor the population, intercept communications and collect information about people.[2]

This surveillance capacity implies a high risk on fundamental rights: those who know our name, what we do, where we are, with whom we speak and what we say, have control over ourselves. The use of tools that allow online anonymity and the encryption of communications have been identified as effective techniques to recover some control over our information, minimize the risks of a connected life and guarantee the respect and exercise of rights such as freedom of expression and privacy.

It is for this reason that civil society has been insisting on the importance of respecting anonymity and the use of online encryption as forms of protection against violations and the effective exercise of the right to freedom of expression.

This report attempts to shed light on the rules governing anonymity and encryption from a normative perspective, with an emphasis on Chile, in contrast to the general Latin-American context. We will point out how the concepts of anonymity and encryption can be understood in the light of the available technology in today's society, to later deal with the Latin American regulations on anonymity and encryption, ending with the detail of the Chilean regulations, determining whether the provisions, both regional and national, allow the use of anonymity and encryption, or if they prohibit or hinder it.

Primarily, our efforts are focused on encryption, both from a technical and legal standpoint, highlighting its importance for safeguarding the exercise of fundamental rights. We refer to the normative restrains of online anonymity through the efforts of regulating or limiting encryption, neglecting the characteristics of the internet and focusing only on its uses associated with criminal activity, without properly pondering both the potential violations that this can cause in relation to the fundamental rights enunciated, as well as the safe traffic in the network.

---

1 Deccan Herald. Online, available at:http://www.deccanherald.com/content/117379/internet-now-single-biggest-source.html [date of access: 09 February, 2016]

2 UNITED NATIONS. 2014. The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights Online, available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf [date of access: 09 February, 2016], p. 3.

3. The growth of mobile internet

A study carried out in 2014 by the GSMA estimated that, by the year 2020, Latin America will be the second region with the largest number of mobile Internet connections in the world, due to the increase in smartphone users, as well as the improvement and migration to mobile internet services of greater speed like 3G, 4G,[3] and the standards succeeding them.

Chile has also presented signs of internet migration, in addition to the tendency of the preference for mobile internet services. A statistical report prepared by the undersecretariat of Telecommunications (Subtel) on the state of telecommunications in the country in 2015, gives an account of the above, noting that 79.2% of internet access in Chile is performed through mobile services. It also indicates a 14.1% growth in that year of subscriptions to mobile internet telecommunications services, in contrast to the fall in mobile minutes usage figures, indicating that in 2015 the total traffic of fixed mobile voice services fell by 2%, which is mainly attributed to the use of communications via data.[4]

Considering such a base of users sharing ideas, the internet represents an essential environment for the exercise of fundamental rights. This exercise of rights is protected by the various legal systems at the same level as rights outside the network: the same rights that assist an offline person are fully applicable online.[5]

---

3 GSMA. 2014. The Mobile Economy Latin America 2014. Available at : http://www.gsmamobileeconomylatinamerica.com/GSMA_Mobile_Economy_LatinAmerica_2014.pdf [date of access: 09 February, 2016], pp. 1-19.

4 CHILE. 2016. SUBTEL. Sector de Telecomunicaciones Cierre 2015. Available at: http://www.subtel.gob.cl/wp-content/uploads/2015/04/PPT_Series_DICIEMBRE_2015_V5.pdf [Date of access: 09 February, 2016: 19 April, 2016], pp. 2-3.

5 UNITED NATIONS. 2012. General Assembly, Human Rights Council. Twentieth Session. Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development. Available at:: ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc [Date of access: 25 April, 2015], p. 2.

4. Anonymity[6]

We understand anonymity as a way of communicating in which people do not know the name of the person that produces the expressive act, hiding the information of the author (Meo, 2010).

The concept of anonymity is not recent. The word has its origin in the Greek voice anonymia, which means "without a name".[7] As Solove, Rotenberg and Schwartz (2006) point out, the very idea of going undercover to communicate is inherent to the human being: the concept of "person" means "mask". For the authors, this mask is made in order to present ourselves to the rest of society.

Throughout history, the confidentiality or the secret about the identity of a person (or a group of people) has been fundamental to the exercise of rights and freedoms, especially of the rights to privacy and freedom of expression. An example of this is the case McIntyre v Ohio Elections Commissions of the Supreme Court of Justice of the United States of America, of 1995. This ruling defined anonymity as a protective shield against the tyranny of the majority, this being recognized and considered as part of the essential content of the First Amendment of the US Constitution (which is understood to consecrate freedom of expression), serving as a safeguard against reprisals that can be taken by those who do not agree with the way of thinking of those who express themselves (Grabow, 1997).

Considering technological advances, data processing capabilities and the nature of the network, it is not enough to hide the name to be anonymous. Therefore, Gary T. Marx (2001) defined the elements that make up the identity of an individual, understanding a contrario sensu, that these are the elements that must be hidden to ensure real anonymity. These are:

The name of the person, both complete and partial. This answers the question "who".

- Identification data such as to locate and find the subject. This answers the question of "where". Here we can find, for example, phone numbers or email addresses.
- Symbols or sequences of characters that can be linked to a person -who- or to a place or an address -where-. For example, bank card numbers, biometric data or date of birth, associated to specific people.
- Nicknames, pseudonyms or symbols linked to a specific person, which at first sight, cannot be traced. This may be because the same law or policies of use of the service grant a number to access it or receive a result without at any time providing the name of the individual (for example, a number generated by a health service to access to the results of an HIV test) or also those cases in which the subject is using a false identity online.
- Patterns of behavior or identifying features related to the physical appearance of the person. Largely as a result of the use of technological tools, these data are widely available. It must be highlighted that although the name of someone is unknown, it does not imply they cannot be recognized.
- The social categories in which a subject can be classified: sex, socioeconomic stratum, state of health, affiliations of any kind, among other examples. The mere fact of being friends with someone or meeting a certain group of people in a place and time can

6 This section is based on what was discussed by Hernández (2016).

7 VOCABULARY.COM., "Anonymity". Vocabulary.com. En línea, disponible en: http://www.vocabulary.com/dictionary/anonymity [Fecha de consulta: 05 de mayo de 2016].

be key to deciphering the identity of the individual, or to attribute characteristics that they do not possess or to frame them in a group, without actually being a member .

- Finally, those certifications that prove knowledge or a particular preference, which can range from a password, any visible sign that gives information of a person (a uniform or a tattoo, for example), the possession or purchase of an object (a ticket for a concert) or an ability either physical or intellectual (such as speaking a foreign language or knowing how to drive).

Although there is a historical recognition of anonymity in public discourse, technological tools limit this non-identification. But in this context of huge amounts of data, anonymity has also been recognized as necessary at the inter-American human rights system level. This has been especially true since the publication of the Special Rapporteurship for Freedom of Expression of the Inter-American Commission on Human Rights in 2013, entitled "Internet and Freedom of Expression." In this report, the Rapporteurship highlights the close relationship that exists between the rights to privacy and freedom of expression, indicating that States should avoid implementing measures that arbitrarily or abusively restrict such rights.[8]

The Rapporteurship identifies specific policies to protect privacy and freedom of expression, in line with anonymity and the protection of personal data. On anonymity, it expressly states that political participation without revealing the identity of the issuer is a usual practice in modern democracies and that it favors the expression of ideas, while protecting the subject of reprisals only because of their way of thinking.[9]

However, the same Inter-American Commission recognizes that anonymity does not protect all types of discourse, thus, it does not give the protection to anonymous speech to those messages that exceed the content of the right to freedom of expression (apology to hatred or criminal activity).[10]

The Inter-American Court of Human Rights in the Escher v. Judgment. Brazil (2009), while not specifically referring to anonymity, recognizes protection not only to the content of a private communication, but also to "any other element of the communication process itself, for example, the destination of calls or the origin of those received, the identity of the speakers, the frequency, time and duration of the calls, aspects that can be verified without the need to register the contents of the call by recording the conversations".[11] The latter is harmonious with the postulates of Gary Marx on the elements that compose the identity of a person, beyond their name. The metadata, when analyzed together with other data, can give enough signs of the subject that navigates through the network. Therefore, encryption techniques, in conjunction with anonymity, are necessary to protect an accumulation of fundamental rights that are subject to the threats that have arisen from technological development.

---

8 COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, Relatoría Especial Para la Libertad de Expresión. "Libertad de Expresión e Internet". 2013, p. 63.

9 Ibíd., pp. 63-64.

10 Ibíd., p. 65.

11 INTER-AMERICAN COURT OF HUMAN RIGHTS, Case of Escher and Others v Brazil (Judgment of July 06, 2009). Online, available at http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf [Date of consultation: October 19, 2015], paragraph 114, p.34.

5. Encryption of communications

In the Spanish language it has been discussed whether the correct term is encoding or encryption, considering that the latter would be a term apparently adopted from the translation of the English verb to encrypt.[12] Thus, it has been said that "encrypt", used in the field of technology and communications, means preparing a file or message which can only be interpreted if a password is available.[13] On the other hand, "encode" has been understood as a verb used in cryptography, which is used as a synonym for encryption. The general language has differentiated them, granting them to encrypt a broader meaning, which does not always have the objective of hiding information, but converting a message into such a code that will allow its later deciphering.[14]

From now on, we will use the term "Encrypt", understood as a reversible cryptographic operation, which transforms data that is initially unprotected, known as plain text, into illegible data, known as encrypted text, using a key called an encryption key (Ewow, 2014). More simply, it can be understood as the process of converting messages or information to an illegible form for all those who are not the addressee.[15]

Encrypting, like anonymity, is not an invention of our time. Its origins can be traced back to ancient times, mainly in Africa, Asia and Europe, normally associated with the exchange of information associated with merchandise trade and military campaigns. Even ancient Egypt there are signs of its use to hide the content of communications.[16] Further development is also associated with the increase in forms and technologies of distance communication.

Thus, the computer-based encryption techniques used most widely today have their origin in the United States in the 1970s, when IBM developed the standard to be used by the NSA for digital security.[17]

Although during the 20th century encryption techniques had a predominantly military use, with the release of the first version of PGP (Pretty Good Privacy) in 1991, by Phil Zimmermann, these became available to the common population. Although there were already paid services to protect users' private communications, PGP is especially notable for two reasons: it is freeware and became a current standard for online security.[18] [19]

---

12 DOMINICAN ACADEMY OF THE LANGUAGE. "Encrypt". Dominican Academy of the Language. Online, available at http://academia.org.do/encriptar/ [Date of Consultation: December 03, 2015]

13 FUNDÉU BBVA. "Encrypt is Hide a Message with a Password". Fundéu BBVA. Online, available at http://www.fundeu.es/recomendacion/encriptar-es-un-termino-valido/ [Date of consultation: December 03, 2015]

14 Ibíd., loc. cit.

15 See, for more detail: SANS INSTITUTE. 2001. "History of Encryption". Online, available at https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730 [Date of consultation: December 3, 2015], pp. 1-3.

16 Ibid., pp. 1-3.

17 Ibid., p. 5

18 Ibíd., p. 6.

19 Currently, PGP is a payment software, with the PGP Corporation as its owner. Among the current free software options available is GPG (Gnu Privacy Guard). GPG is a rewrite and update of PGP, which uses an encryption algorithm different from GPG to ensure its gratuity. Currently, PGP allows the download of its software for free only for personal use (the commercial is paid for), on the other hand, GPG allows its download without cost for both personal and commercial use. Excerpted from DIFFERENCEBETWEEN.NET. Difference Between PGP and GPG. Differencebetween.net. Online, available at http://www.differencebetween.net/technology/software-technology/difference-between-pgp-and-gpg/ [Date of consultation: May 31, 2016]

Zimmermann (1999) points out that in the era of digital information, the privacy of users' communications is more vulnerable than before and it is easier for governments to intercept them. By virtue of that, it recognizes two fundamental reasons that led to the publication of PGP for free: a bill presented by the US Senate in 1991 (Senate Bill 266), which sought to compel both companies that provided digital communications services and the manufacturers of technological equipment that would allow secure communications to install exit doors to such equipment (backdoors), thus allowing the government to have access to the contents of these communications, prior judicial authorization. For Zimmermann, the massification and popularization of encrypting technologies will make it more difficult for the government in turn to make its use illegal (Zimmermann, 1999).

The second reason is that it considers encrypting as the only way to avoid the threats of the right to privacy created in the era of digital information.

It should be noted that Zimmermann sees the utility of encrypting software in relation to attempts to criminalize the use of encrypting techniques.

4.1. How do the current encrypting techniques work?[20]

In a similar way to anonymity, encrypting has adapted over time: from the use of ideograms, drawings or messengers that, in person, carried an encrypted message in a physical format to the recipient, to public and private key systems digital devices that allow encrypting the message sent by the sender and be decoded only by its individualized receiver at the beginning of said communications.

The use of encrypting in private communications between people has become widespread, as we have seen since the 1990s, and is present in a large part of digital communications. Previously, it was mainly used in relation to the protection of access to information or focused on transactions carried out through the network, between servers or between individuals and companies, but it has been extended to private communications between people. Our analysis will concentrate on these.

An encrypting system currently used in various communication channels is the public-private key system, known as point-to-point or end-to-end encryption. In simple terms, each person has a pair of keys, a public one (that everyone knows) and a private one (that only the owner knows). The operation of this cryptosystem is based on the safeguard of the private key of each one and the distribution of the public key to the others. In this way, when sending an encrypted message, we have two people: the sender and the receiver. The sender, must know their public key to establish encrypted communication with the receiver, which can be sent by them or can extract it from a public directory of keys. Thus, by sending an encrypted message to the recipient, the public key transforms the message into an apparently illegible one.

So, how can the receiver read what the sender sends? Here the so-called private key comes into operation, which is a file where the parameters necessary to decipher the encrypted message based on the public key of the same receiver are found. Given the nature of the mathematical problems used in encryption, breaking it by brute force is practically impossible, since it requires computation operations to guess the encryption parameters which would take a very long time. As explained, it is finally the receiver (or rather, the owner of the private key) the only one with the ability to decipher the content of the encrypted message.

---

20 The collaboration of Martin Gubri and Israel Leiva in the writing of this section is gratefully acknowledged.

Within this scheme, there may eventually be a third participant, an adversary that seeks to intercept communications between the sender and receiver, usually during its "rout". In case this third party can capture the message, it will not be able to understand it, given that it will be composed of numbers, symbols, letters, among others (without an obvious pattern).

On the other hand, there is encrypting of communications with web site servers, identified with HTTPS (Hypertext Transfer Protocol Secure). This encryption protocol creates a secure communication between the user and the server in which the site is hosted, by means of an SSL (Secure Sockets Layer) or TLS (Transport Layer Security, a later version of SSL) certificate associated with a domain name or a server to an organization and its location. In this way, when using an HTTPS connection, whoever enters the site makes sure that the content seen on the screen is the real site, which has not undergone any modification between the transport of information between the equipment and the server, thus protecting sensitive information, such as passwords or bank accounts. It is the server who deciphers the message communicated, not the parties that hold the file that allows access to the content.[21]

4.2. The current debate on the use of encrypting techniques

Currently, it is possible to find freeware that supports encrypted communications: applications for phones such as WhatsApp, Signal or Telegram; chat services such as Cryptocat or obfuscation of chats with OTR mode (off-the-record); GPG Tools to facilitate the use of PGP to send encrypted emails or protect access to storage devices or files, among others. In this group, as an expression of the current trend, the adoption of point-to-point encryption by WhatsApp (owned by Facebook)[22], the messaging application with the largest user base in the world, with respect to its competitors stands out.[23]

The operating systems of desktop computers and laptops (macOS, Windows[24] and free and open source operating systems), as well as the most popular smart mobile phones on the market (Android and iOS, in the case of the latter by default) deliver also the option to encrypt the information contained in your storage systems (such as hard disks and solid state disks). In this case, the encryption is maintained over static information; however, in the face of any attempted seizure by a third party that does not have a decryption key, the content will be virtually inaccessible.

---

21 If the private key encrypting system responds to how the message is encoded, point-to-point encrypting responds to where it is decrypted. Thus, a simple definition is in Wired.com which indicates that "(...) the messages are encoded in such a way that only the receiver can decipher it and not another person in between. In other words, only the computer at the end of the chain contains the key that allows deciphering it and the company acts as an illiterate messenger, which transports the message without being able to decipher it or read it for itself ". Definition extracted from GREENBERG, A. 2014. "Hacker Lexicon: What is End-to-End Encryption?". Wired.com. Online, available at: http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ [Date of consultation: January 18, 2016] (translation is ours). Thus, for example, Facebook does not use point-to-point encryption because it is the server which decrypts the sent message so that the receiver can read it, which is in practice how https mechanisms work. On the other hand, if we send an encrypted email with a tool like PGP Tools, it is not our mail server that decrypts the content for the receiver, but the private key that consists of a device that contains it, for example, the laptop of the receiver.

22 EL PAIS. 2016. WhatsApp Activates the Encryption of Messages for All Users. Elpaís.com. Online, available at: http://tecnologia.elpais.com/tecnologia/2016/04/05/actualidad/1459875233_301649.html [Date of consultation: April 25, 2016]

23 EL COMERCIO. 2015. WhatsApp is the Most Popular Messaging App of 2015. Elcomercio.pe. Online, available at: http://elcomercio.pe/tecnologia/actualidad/whatsapp-app-mensajeria-mas-popular-2015-noticia-1862521 [Date of consultation: 25 de abril de 2016]

24 On storage encrypting in Windows, see Lee (2015).

The use of encryption techniques, both in the protection of information and in private communications, is intended to reduce the risks of interception of content during communication, risks that include access to sensitive data associated with the execution of actions such as purchasing by Internet, receiving medical data, accessing social network accounts, bank account and, in general, any type of online activity that involves access to information that if extracted illegitimately can reveal extremely precise details of privacy and as a consequence, generate damages.

Despite this panorama, not all uses of encryption techniques are equally accepted. The use of protected communications software has been the concern of various governments for years, as we recall, the launch of PGP in 1991 was a response to a bill in the United States that sought to introduce vulnerabilities in communications services and in the equipment necessary to carry them out. The fight against organized crime, electronic scams, child pornography, trafficking of illicit substances and terrorist activity has led, mainly since the last decade, to incorporate changes in the regulation of telecommunications services, assuming high-intensity intromissions to the right to privacy of users.

In a similar way to what has happened with anonymity, the use of encryption is not something that has left the authorities indifferent.

When creating PGP in 1991, Zimmermann wanted to raise awareness about the existence of suspicions on the part of governments, especially by the national security sectors, in relation to the use of encryption techniques by citizens. There, Zimmermann pointed out that in the use of encryption tools there is a power game of which the government is aware of (Zimmermann, 1999).

In this decade the discussion was revitalized, especially since the end of 2015, after a series of serious terrorist attacks that occurred in France, California and Belgium. The fight against highly dangerous crime has influenced in the legislative agenda at a global level, where the use of anonymity and encryption techniques is usually associated with the commission of highly complex crimes. In this sense, the debate on the legality and legitimacy of the use of encrypted communications has escalated in relation to public security.

In his recent work, Phillip Rogaway (2015) of the University of California Davis, advocates for a development of communication technologies with the awareness of the damage that can be caused to the public with the advances of science. He suggests that the same technology that has laid the foundations for the current structure of state surveillance can help to reverse this reality for the users of the network, with the use of encryption. He also expresses his apprehension for the lack of ethics and concern of the scientific community when investigating, who, for the sake of the computer advance, have forgotten and seem not to be interested in the repercussions that their work will have on the lives of each one of us. In this sense, the author states that scientific work has political consequences, even when scientists are not always fully aware of them.

For both Zimmermann and Rogaway, it is this power game between the government and the civilian population where the current true discussion on encryption lies.

The desire to incorporate vulnerabilities in the software and hardware of communications was denounced in the United States of America in the early 1990s with a series of bills, which are the first antecedents that exist of attempts to weaken the use of encryption by the state intelligence community. At the time, the arguments used by those who fought against government access to all communication, as well as by those who supported access to protected communications by the government, at the cost of introducing vulnerabilities to the systems, were quite vehement.

In 1994, in relation to the famous Clipper Chip case[25], Dorothy Denning of Georgetown University stated that if a vulnerability was not implemented, "all communications transmitted through the information highway would be immune from legal interception. In a world threatened by internationally organized crime, terrorism and corrupt governments, this decision would be foolish" (Levy, 1994).[26] On the other hand, when consulting Phil Zimmermann about the illegitimate uses of encryption with his idea of creating a PGP protected telephone, he replied: "I am worried about what could happen if communications are managed with unlimited security, but I also believe that in it there are tremendous benefits. Some bad things could happen, but the trade-off would be worth it. You have to look at the global picture" (Levy, 1994).[27]

With the revelations of Edward Snowden in mid-2013 about the surveillance of the NSA, the discussion on encryption regained renewed strength, with the reaffirmation of the arguments on national security. Likewise, it is striking that the desire to incorporate vulnerabilities into private communication systems (in order to make it possible to deliver them to the government if requested) also does not enjoy a special novelty (McCullough, 2014). Although the initiative was rejected in the 90s, it has now been reconsidered by the security services, as they claim that encryption has made their work more complex (Temple-Raston, 2015).

Although the controversy over the use of encryption was already present, the terrorist attacks that took place in Paris in November 2015 placed encryption techniques at the center of political attention.[28] To coordinate such suicide attacks, they would allegedly have used encrypted messaging services such as WhatsApp and Telegram[29], even though this was eventually denied, since it was revealed that the attackers used unencrypted text messaging (SMS).[30]

However, in July 2015 the then director of the FBI James Comey had pointed out that the use of encryption, especially in smartphones, has been a hindrance in the exercise of their organization. He argued that even they do not have the necessary tools to be able to intervene a strong encryption.[31] The same former official, in different speeches, highlighted the value of security as a public good (as opposed to privacy that is individual).

---

25 The case of the Clipper chip occurred in the United States in 1993. The administration of former President Bill Clinton sought to incorporate a back door into the communications equipment by means of a chip that would be installed in them in such a way that the police forces could have access to the private communications carried out by means of these, using a copy of the key that the Government would have stored for such purposes (key escrow). That measurement finally did not prosper, when resistance prevailed. Excerpt collected from Higgins (2015).

26 "'If something like Clipper is not implemented', writes Dorothy E. Denning, a Georgetown University computer scientist, 'All communications on the information highway would be immune from lawful interception. In a world threatened by international organized crime, terrorism and rogue governments, this would be folly'".

27 "'I am worried about what might happen if unlimited security communications come about,' he admits. 'But I also think there are tremendous benefits. Some bad things would happen, but the trade-off would be worth it. You have to look at the big picture'".

28 A summary of the discussion can be found in Henn, S. and Selyukh, A., "After Paris Attacks, Encrypted Communication Is Back In Spotlight". NPR.org, November 16, 2015. Online, available at http://www.npr.org/sections/alltechconsidered/2015/11/16/456219061/after-paris-attacks-encrypted-communication-is-back-in-spotlight [Date of consultation: January 5, 2016]

29 PEREZ, E and PROKUPECZ, S. 2015. "First on CNN: Paris Attackers Likely Used Encrypted Apps, Officials Say". CNN Online, available at http://edition.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/ [Date of consultation: January 5, 2015]

30 Farivar, C., "Paris Police Find Phone With Unencrypted SMS Saying 'Let's Go, We're Starting'". Ars Technica. Online, available at: http://arstechnica.com/tech-policy/2015/11/paris-police-find-phone-with-unencrypted-sms-saying-lets-go-were-starting/ [Date of consultation : April 25, 2016]

31 TEMPLE-RASTON, D. 2015. op. cit.

He also pointed out that the rapid technological advance has created a gap in current legislation and has given space for the undetectable commission of highly dangerous crimes. A central point to the argument, is that the requests to a court in the framework of a criminal investigation would have no value, since the use of encryption does not allow to find out the critical data necessary for the persecuting entity, since it can only be traced to a certain point and then it disappears (going dark) (Rogaway, 2015). Thus, they plead for the incorporation of access mechanisms to the data contained in telecommunications devices.

The successor of Comey in the FBI, Christopher Wray, maintained the same opinion. Recently, in October 2017, he said in a public speech that encryption is a big problem that impacts all kinds of investigations: narcotics, human trafficking, counterintelligence, gangs, organized crime and child exploitation. On the occasion, he also revealed that the FBI had failed to access the content of more than 6,900 mobile phones because of encryption.[32]

On the other hand, the defenders of encryption tools (mainly members of civil society and technology companies) have pointed out different arguments against the imposition of premeditated vulnerabilities. We present the most common mechanisms of vulnerabilities used to circumvent the strong encryption techniques, the arguments against the implementation of these and now, in general, the reluctant position to the widespread use of encryption by the population can be summarized in the following:

- It does not necessarily help the fight against organized crime: As it is often said in discussions regarding the illegitimate use of technologies, encryption, as a tool, is neither good nor bad in itself: technology is neutral, and users are the ones who use it either for good or for illegal purposes (Botero, 2015). Likewise, what happens on the network is just a manifestation of what happens outside of it; therefore, if illicit acts are committed in the digital environment, they have always existed and will continue to be carried out, even with or without encryption techniques, on the other hand, the same measures that criminals use in the network to avoid being discovered are similar to those used by those in charge of maintaining citizen security as well as by the members of vulnerable groups of society to protect themselves from harassment that may mean that they express their opinion online.[33]

- At the same time, attention has been drawn to the fact that there is no conclusive evidence to show that the use by high-risk criminals of encryption technologies is an insurmountable barrier to criminal prosecution[34], since even when the content of the sent file or of the communications is protected, there is a lot of information associated to the sent encrypted message that allows to find out the necessary data that prove a connection between individuals, belonging to certain groups, time, date, place and support used to communicate, frequency of sustained contacts , among other types of information.

- Much of the encrypted information can be known anyway without having to be deciphered: As stated by Moxie Marlinspike (founder of Open-Whisper Systems, creators of the free software encryption tool that uses WhatsApp to protect their communications) to NPR.com in 2015, most of the services commonly used by consumers, encrypt the content of messages sent by those, but not the metadata,

---

32 Farivar, C., "FBI director: Unbreakable encryption is a 'huge, huge problem'", Ars Technica, October 23, 2017, available at https://arstechnica.com/tech-policy/2017/10/fbi- director-unbreakable-encryption-is-a-huge-huge-problem [Date of consultation: October 24, 2017]

33 UNITED NATIONS, Human Rights Council. 2015. op.cit., p.6

34 Ibíd, op. cit., p. 15.

therefore, if a terrorist network contacts through a certain platform, intelligence services are able to detect it.

- In fact, metadata analysis allows predicting behaviors with a high degree of certainty, revealing patterns of behavior, points of view, interactions with others and affiliations, considering that it exposes more to the subject than the content itself of communications, which enjoys a greater legal protection.[35] The encryption does not necessarily protect all the data of the communication, even though it may not be possible to know the message sent, the IP address of the involved computers is not always hidden, therefore, with this single data, third parties can collect an amount of meaningful information.[36] It is also necessary to remember that in some countries of the world (Chile included) there are regulations that require the retention of communication data, through which users of equipment connected to the network can be reached (Díaz, 2017).

- Deliberately creating a vulnerability can affect more services than those necessary for criminal prosecution. By introducing some kind of weakness in a computer system, this vulnerability not only acts in favor of the government interested in maintaining the security of the population, it can be exploited by anyone with the technical skills.[37] The representatives of the largest technology companies hold this position.

  For Tim Cook (CEO of Apple), a consciously introduced weakness can be used by those who have legitimate access as well as for frauds. At the same time, he recognizes that Apple devices contain a lot of data about their user, who have an expectation that their privacy will be respected when choosing the company. This is why he believes that it is good for the consumer to be able to control the flow of such data.[38]

  Encryption not only protects files and messages, it also protect the commercial traffic of individuals and large companies, as well as industrial and intellectual property secrets (Greene, 2015). Additionally, the governmental apparatus can be subject to existing vulnerabilities in a system leading to the subsequent exposure of the information contained therein, an exemplary case is what happened in December 2015 in the United States with the security flaws existing within the firewall of Juniper Networks.[39] Therefore, if a given government requires technology companies (whether they are equipment manufacturers, telecommunications companies or software companies) to introduce vulnerabilities intentionally, it not free of risks.

  In this sense, the sensitive information of the population needs to be stored to provide certain services, such as those associated with health, online processing before public services or economic transactions, to name a few examples. The introduction of a vulnerability can open the window for illegitimate access to such sensitive data, which should be protected by the highest standards of online security.

---

35 PRIVACY INTERNATIONAL. What is Metadata ?. Privacyinternanal.org. Online, available at: https://www.privacyinternational.org/node/53 [Date of consultation: January 11, 2016]

36 UNITED NATIONS, Human Rights Council. 2015. op.cit., pp. 4-5.

37 Ibíd, p. 4.

38 NPR, "Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right'. NPR.org, October 1, 2015, available at: http://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right [Date of consultation: January 11, 2016]

39 ZETTER, K., "Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors". Wired.com, December 18, 2015, available at: http://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ [Date of consultation: October 23, 2017]

- The installation of backdoors transgresses the fundamental rights of the affected party. In the report prepared by David Kaye (2015), Special Rapporteur for Freedom of Expression of the Human Rights Council of the United Nations, the role of anonymity and encryption is highlighted, since it allows individuals to exercise their rights to privacy and freedom of opinion and expression in the digital era.

  Specifically regarding encryption, Kaye points out that, while it is not enough on its own, the traces it leaves in its network traffic diminish. Encryption works by creating a security zone that safeguards the right to freedom of expression, thus encouraging navigation, opinion and development of ideas in the face of external threats. He emphasizes on the role of the private sector in the protection of the right to freedom of expression, promotion and protection of encryption tools. Thus, he indicates that telecommunications companies, internet service providers, information storage services, search engine managers, among others, can act or compromise the use of encryption techniques, as these companies handle large volumes of data from their users, and the public authorities request such information to them.[40]

  The special place that private entities have in the respect of human rights has been often noted, in 2011, John Ruggie produced a report for the United Nations in which he referred to their role in the protection, respect and remedy for violations of human rights. In this document, Ruggie established as a fundamental principles of a framework that considers the three edges just mentioned "the obligation of companies to respect human rights, which means acting with due diligence so as not to violate the rights of third parties , and repair the negative consequences of their activities. "[41]

- Kaye (2015) insists that any restriction on encryption should be done in specific cases, such interference with the requirements of legality, necessity, suitability and proportionality of the measure, being approved by a judge. He also advocates that the discussion on the limitations to this type of tools should consider the positive uses, as it usually focuses on the negative aspects. Finally, he suggests that States should promote the use of strong encryption techniques, so that individuals feel protected in their privacy.[42]

4.3. Mechanisms of forced decryption and circumvention of encryption

As we have mentioned, there are various encryption circumvention mechanisms or vulnerabilities of encryption systems. They consist of mechanisms that integrate both technical and institutional components, in which the law plays an important role as a facilitator of the forced decryption of communications or stored information. These mechanisms can normally be divided into the following:

- Backdoors: They are defined as a method to circumvent the authentication or other type of security control necessary to access a computer system or the data contained in it. They can exist both at the operating system level, in an encryption algorithm or within an application (Wysopal et al, 2008). These doors allow access to the system or

40 Ibíd, p.10.

41 UNITED NATIONS, Human Rights Council. 2011. "Report of the Special Representative of the Secretary General for the Question of Human Rights and Transnational Corporations and Other Companies, John Ruggie." Online, available at: http://www.ohchr.org/Documents/Issues/Business/A.HRC.14.27_sp.pdf [Date of consultation: January 13, 2016], p. Four.

42 UNITED NATIONS, Human Rights Council. 2015. op.cit., p. 19-20.

information contained therein locally or remotely.[43] It has been said that in the United States and in the United Kingdom these mechanisms are currently being sought to decipher encrypted communications (Leonard, 2015).

This particular method has been the object of criticism, since introducing a vulnerability of this type does not discriminate between legitimate and illegitimate access, nor between access by the government or by third parties. The weakness created can be exploited by anyone, since it does not recognizing the purpose of the intrusion into the system.

- Copy of the private key: Unlike a back door, in which a computer system is surreptitiously accessed, there are other methods in which the entry is direct and frontal. Within this form of intervening communications and encrypted files, the two most common forms are the legal obligation of delivery of the private key in case of being requested (key disclosure) and key deposit (key escrow).

  The first of these methods (key disclosure) consists of the obligation contained in a law that requires an individual to reveal his private key to the entities in charge of criminal prosecution in the event that those request it, complying with the procedure legally established for that purpose; generally, after judicial authorization (Lin, 2010).

  Many countries have legislated on the subject, which has been criticized, especially concerning the intensity of the intrusion to the rights of the subject to whom the delivery of this code is required. Intrusive measures are usually delimited by the contours that the judge establishes in the authorization, where (ideally) it must be indicated with precision on which specific pieces the measure falls, thus minimizing the violation in the rights of this individual, by reason of a test of proportionality. Thus, requesting a private key is not the same as requiring the delivery of a document since, by its nature, this implies giving access to all archives and protected communications, overcoming any margin of proportionality (Clemens, 2004).

  The second mechanism, key escrow, has been defined as a process in which something (such as a document or a private key) is delivered to a third party, who can only authorize access to the file delivered prior compliance with the conditions imposed for that. Normally, this mechanism implies the delivery of a copy of the private key to the public security agencies or that the telecommunications companies maintain one, only revealing it in case of a criminal investigation against the subject. A good example is the "Chip Clipper" in the 90s, to which we have already referred.

  The discourse of the US NSA was aimed at obtaining this type of entry to the encrypted communications, noting that you do not want a backdoor, but a frontal one, that contains multiple locks (see Gellman and Nakashima, 2015). On the other hand, it has been said that these types of solutions are too complex to execute and can be contradictory, in addition to highlighting that complexity is the enemy of security: as the system is more complex, it will contain more imperfections that can be exploited by third parties seeking illegitimate access (Abelson, 2015).

  For David Kaye (2015), the key escrow mechanisms also presents a series of problems to be taken into account, mainly linked to trust in the repository of the key (which can be the government or a reliable third party). This system depends on the integrity of the person who stores the key, the security of the key file, which can be the object of

43 PC MAGAZINE ENCYCLOPEDIA. "Definition of Back Door". PC Magazine.com. Online, available at http://www.pcmag.com/encyclopedia/term/38339/back-door [Date of consultation: January 5, 2016]

external attacks trying to access this file illegitimately. Regarding key disclosure solutions, Kaye states that a mechanism less harmful to the principle of proportionality would be that the authorities (prior judicial authorization) request the subject to decipher the particular message or messages whose content they need to know, instead of requesting the key that allows full access

- Brute force: It is the most rudimentary method, which consists of trying all possible combinations until finding the one that allows access to the system, usually through mechanisms that automate each attempt varying the combinations. This is easier when the passwords used are weak (very short or easy to derive, they are much easier to guess than "strong" passwords).[44]

  Regarding the private key, the situation is similar, since like a password, it is a sequence of characters. Originally, as we saw, the sequences used to be smaller, so to be able to ensure the protection of this key, it has been chosen to increase its extension and the randomness of its composition in a sustained manner. However, as much as the structure has become more complex, it does not make them invulnerable. In effect, the encryption in its essence is still a mathematical operation and computers are increasingly powerful, increasing their ability to decipher a private key.[45]

  Specifically, within the encryption systems of public-private keys, there is an algorithm to create new keys, therefore, if the previous one is discovered, the process of deciphering the private key is simplified in this way (Blumenthal, 2007).

- Malware:[46] Contraction of malicious software; it is a generic concept that encompasses a series of programs designed to alter or deny the operations of the system, collect user information or allow the exploitation of other services, obtain unauthorized access to system resources and other types of abusive behavior. Malware interferes with the normal functions of a computer system or sends user data to unauthorized third parties over the network. The concept of malware includes a series of harmful software such as viruses, Trojans, worms, spyware, browser hijacking, among others.

  Under this definition it is possible to understand how the file containing the private key can be obtained in a computer system and, in fact, any private communication or file that is protected by a strong encryption can be accessed. For example, if you need to enter a password to access an account or to view a protected file or you want to see the content of the communications supported by an encrypted text messaging service, the installation of a keylogging software is sufficient. Then, having unlocked the file can be copied and sent to other devices.

---

44 A simple example of how to create strong passwords can be found in González (2014).

45 See, for example: "Brute-Force Attacks Explained: How All Encryption is Vulnerable." How-to-Geek.com. Online, available at: http://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable/ [Date of consultation: January 7, 2016]

46 Definition extracted from USLEGAL. "Malware Law & Legal Definition". USlegal.com. Online, available at: http://definitions.uslegal.com/m/malware/ [Date of consultation: January 7, 2016]

5. The Relationship between Anonymity and Encryption

5.1. The technical relationship between anonymity and encryption [47]

By default, an encrypted message is not anonymous. Encryption allows to maintain secure communications without an external third party being able to understand the transmitted message. And, in case the message is intercepted, it cannot be decoded. However, although the message will be illegible, a third party can still know the metadata associated with the contact between the parties.

In effect, the above is due to the very nature of computer networks which, basically, are a set of several connected computers that send each other small pieces of information or "packages", transporting those from one place to another. The network requires knowing where the message is going and where it comes from so that it can be sent. Those who use software and common communication and messaging applications such as GnuPG, off-the-record chat, Signal or other, only see the content of the communication protected by point-to-point encryption, but such services do not offer anonymous protection.

As a result, if a third party is monitoring the network, even when it cannot decipher or access the content of the message sent, it will be able to find out a series of data related to such communication: those who communicate, the number of sent messages, the time and date of issue (including the approximate weight of each of those) and, usually, you can also find out the software by which the contact between the parties was maintained.

As in the case of the use of an end-to-end method, encryption via the HTTPS protocol does not guarantee anonymity, but only protects highly sensitive data from third parties. First, the server is able to identify the person who accesses it to send messages, since it knows the metadata listed above, all the information that the person seeking to use the service must submit in order to create an account, and another accumulation of information that can be collected in case of using the mobile versions (geolocation, registration of telephone numbers, files stored in the device, among others).

On the other hand, the server itself may contain online tracking methods (website visitor trackers), which can be defined as external content to a website, but are incorporated into it, which identify the browser used by the user, in addition to the pages visited. Normally, they are used to know who visits a particular site for the purpose of social networks advertisement or to identify the favorite content of those who visit a site, in order to plan the preparation of contents according to the preferences of the navigators. Not even the secure communications that can be sustained in these sites can protect the user of all these trackers.

Finally, there is the notion of fingerprint. This allows that every time we visit a site, our browser and its extensions can filter information so our combination of operating system, browser, extensions, programs and habits account for our identity (Gilbertson, 2010).

However, there are ways to navigate and communicate in an encrypted and anonymous way, being the Tor network (The Onion Relay network) the best example. Tor encrypts the information to be sent in several layers, and then sends it through a network of servers around the world (the Tor network), where each server deciphers one layer and passes the information to the next, only by knowing who sent the information and to whom it should be sent, but not the entire journey. The final server (or output) decrypts the last layer and identifies the final destination of the communication. Thus, no server in the path recognizes the origin and destination at the same time.

---

47 The collaboration in the elaboration of this section to Martin Gubri and Israel Leiva is gratefully acknowledged.

It should be noted that Tor only encrypts the communication while it occurs within the Tor network, not before or after. A weakness of this is that if the traffic is not encrypted from the beginning (as in the websites with HTTPS), the server can analyze the content and try to de-anonymize the user. On the other hand, using Tor allows to hide the place of origin of the communication, but that is not enough to be completely anonymous. For this, additional safeguards should be taken, such as using secure protocols, not repeating browsing patterns and avoiding technologies prone to being exploitable by hackers (such as Adobe Flash), among other measures. Notwithstanding the foregoing, Tor is not flawless, as by its design, it is possible to identify the user of the network at both: the exit and entry nodes (Koebler, 2014).

5.2. The Relationship between Anonymity, Encryption and Fundamental Rights

David Kaye (2015) identifies anonymity and encryption as the ideal means for online security, since they provide the individual with methods to protect their privacy, empowering them to navigate, read, develop and share their opinions and information without interference, as well as to allow journalists, civil society organizations, members of ethnic or religious groups, those who are persecuted for their sexual orientation or gender identity, activists, researchers, artists and society as a whole to exercise their right to freedom of expression and opinion.

The Special Rapporteurs for Freedom of Expression of the United Nations and the Inter-American Commission on Human Rights have previously referred to mass surveillance and its repercussions on the rights of technology users.

In the joint declaration of 2013, on surveillance programs and their impact on freedom of expression, the then special rapporteurs expressed their concern about the harmful effect that online monitoring can have on these two rights, given their highly invasive nature, emphasizing the great technical capacity currently available within States to monitor private communications, the important role played by the Internet in the current exercise of human rights and how this traffic has entailed a large accumulation of persona data, that can systematize and reveal[48] as much or even more that what people want to communicate. This is the last reason why the protection of online anonymity is relevant.

As explained previously, anonymity and encryption not only go hand in hand from a technical point of view, but also from the rights protection perspective. The Special Rapporteurship for Freedom of Expression of the IACHR identifies as appropriate policies to protect the rights to privacy and freedom of expression on the Internet, both the protection of personal data and anonymous speech[49], but anonymity is not enough in modern democratic participation -in the terms of the Rapporteurship-, but, as Kaye envisions, it is also necessary that communications are safeguarded.

Although there are no references to encryption in the 2013 publication and in the joint declaration, the 2014 Annual Report of the IACHR's Rapporteurship contains indirect references to encryption, especially with regards to surveillance programs and reserve of journalistic source.

In this annual report, the Rapporteurship expressed its concern on the existence of such programs in countries of the region and the serious detriment that they generate to human rights, recommending that States establish limits to the power to monitor private communications and that, when measures that involve vigilance are taken, the principles of necessity and proportio-

---

48 UNITED NATIONS, ORGANIZATION OF AMERICAN STATES. 2013. Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression. Online, available at: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927 [Date of consultation: January 29, 2016]

49 INTER-AMERICAN COMMISSION ON HUMAN RIGHTS. 2013. op. cit, p. 63

nality are respected. In addition, it is recommended that they provide public access to information about surveillance programs, to ensure that they are not used arbitrarily. Finally, it suggests that journalists, members of the media or members of civil society who publicly disclose the information they obtain about this type of program are not sanctioned.[50]

The foregoing shows that anonymity does not protect by itself the rights to privacy and freedom of expression in the face of mass surveillance. Therefore, encryption is necessary to protect messages sent between senders and receivers, especially if they belong to especially vulnerable groups, listed at the beginning. This was the view taken by Bruce Schneier[51], indicating that encryption is the most important tool that exists today to protect the privacy of people and that it should be used by the entire population. The widespread use of encryption makes less conspicuous to those who use it to protect its integrity.

In case it is not the message, but the sender or receiver who needs to protect themselves, anonymity takes a second dimension that must be protected, which is addressed to the individual as long as they want to hide their identity.

In this sense, anonymity has been raised throughout history as a method for expressing unpopular opinions, such as expressing oneself about a minority life option and learning about it (Shaik, 2014), issuing a controversial political opinion (Simpson, 2015), to denounce irregularities (Véliz, 2013), to express artistically without fear that the attention of the critic will be directed to the author but to the work, and the development of journalism (García, 2004).

However, the communications sustained between members belonging to these groups, the journalist and the sources, the whistleblower and the entity that receives the reports, the messages sent between the real person of the artist and editor, must be protected by a strong encryption, since the identity of the complainant can be deciphered as a result of an analysis of online activity and information crossings which will mean that the usefulness of anonymity will be lost, since anonymity as a concept, described by Marx (2001), includes many data apart from the name.

This is how encryption and anonymity, altogether, are the most suitable tools that we currently have in order to exercise and protect our rights to privacy and freedom of expression in the era of digital communications.

---

50 ORGANIZATION OF AMERICAN STATES. Inter-American Commission on Human Rights. 2015. Annual Report of the Inter-American Commission on Human Rights 2014. Annual Report of the Office of the Special Rapporteur for Freedom of Expression. Online, available at: http://www.oas.org/es/cidh/expresion/docs/informes/anuales/Informe%20Anual%202014.pdf [Date of consultation: January 28, 2016], p. 435

51 PRIVACY INTERNATIONAL. 2015. Securing Safe Spaces Online: Encryption, Online Anonymity and Human Rights. Online, available at: https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf [Date of consultation: January 29, 2016], p. 3-4.

6. Legal Regulation of Anonymity and Encryption.

6.1. Human rights and regulation of digital communications

The aforementioned report of the Office of the Special Rapporteur for Freedom of Expression of the IACHR, referring to the year 2014 and launched in 2015, gives an opinion on the matter, expressing concern about the attempts of several Latin American States to regulate one or more aspects related to access and use of the internet, while some of these attempts violate fundamental rights. It also draws attention to the attempts to regulate this form of telecommunication considering the strategies used for others means, such as telephony, ignoring its unique characteristics.[52]

Thus, the report suggests to the Latin American States to take into account the following points when elaborating normative initiatives related to the internet:

- Refrain from applying regulatory approaches developed for other means of communication other than the Internet, and design an alternative and specific regulatory framework for this medium, according to its particularities, in accordance with international standards in this regard.
- Encourage self-regulation as an effective tool when dealing with offensive expressions that may be issued through the Internet.
- Protect Internet intermediaries and those who provide technical services regarding any responsibility for the contents generated by third parties and that are disseminated through the services they provide.
- Promote universal access to the Internet to guarantee the widespread and effective enjoyment of the right to freedom of expression through this means.
- Ensure that the processing of data and Internet traffic is not subject to any type of discrimination based on factors such as devices used, content, author, origin or destination of the material, service or application, in accordance with the principle of net neutrality.

The Human Rights Council of the United Nations, through the report of Ruggie (2015), has highlighted that the private sector, like the public sector, fulfills a role in this protection, therefore it should adapt its practices to the respect of human rights and ensure that respect. Therefore, telecommunications companies must not only comply and respect fundamental rights and freedoms by virtue of the mandates destined for this purpose in the sectoral regulation prepared by the competent public bodies, but also should have initiative in this operation.[53]

In this line, it has been argued that self-regulation in the Internet is the most viable option to regulate the network.[54] Under a self-regulatory model, telecommunications companies develop the practices they deem appropriate to protect the rights of their users, which may excel the legally required standard and avoid inefficiencies inherent in over-regulation (Castro, 2011). Howe-

---

52 INTER-AMERICAN COMMISSION ON HUMAN RIGHTS, Office of the Special Rapporteur for Freedom of Expression. 2015. op. cit., p. 434.

53 UNITED NATIONS, Human Rights Council. 2011. op. cit., pp. 3-6.

54 See, for example, THE GUARDIAN. 2008. Harmful Content on the Internet: Self-Regulation is the Best Way Forward. The Guardian. Online, available at: http://www.theguardian.com/media/organgrinder/2008/aug/01/post88 [Date of consultation: February 1, 2016]

ver, in relation to the right to privacy, the adoption of a co-regulatory model has been proposed, since self-regulation has not yielded positive results, since technology companies increasingly collect more data from their users.[55]

Whatever the option taken by governments to regulate the network (self-regulation, state regulation or intermediate models), there are two basic ideas that must be respected and taken into account. The first one, as indicated by various reports of special rapporteurships, is that the Internet differs from other classic methods of communication such as radio or telephony and that these special characteristics must be respected and taken care of in case of passing laws and developing administrative regulations. Moya (2003) states such characteristics:

- Global: You can access it from anywhere in the world.
- Decentralized: It has no owner, legal representative or manager, since the key idea to its design is that it is decentralized, without any restrictions or ties. Likewise, Moya points out that, within this feature, it is included that the internet free of hierarchical surveillance and control structures.
- Open: Anyone with access to the internet can generate content, with few access barriers.
- Large: Given its high storage capacity.
- Interactive: The design of the network itself - bidirectional - aims to ensure that all users can be transmitters and receivers of the information there, modifying the traditional communication schemes.
- Controlled by the user: The user is free to choose the contents that can be accessed and shared.
- Independent of the infrastructure: It is not linked to any infrastructure other than the physical network composed of cables, antennas and satellites, thus being far from effective government control.

On the other hand, the States have the duty to protect the human rights of those who use digital technologies, taking this into account when legislating, which becomes urgent considering the global tendency to elaborate regulations that transgress such rights in order to protect others, such as public security. Thus, when regulating the internet, it must be ensured that the principles stated above are not transgressed, encouraging individuals to generate content and allowing them to express themselves, in addition to respecting the nature of the Internet as an independent, open and decentralized network.

6.2. Regional overview of the regulation of anonymity and encryption

At the regional level, there are several rules that contain provisions referring to encryption and anonymity, which are generally concentrated in legal bodies such as: the Constitution and laws of protection of personal data, telecommunications, mobile registration and traffic on the internet, those that regulate the media in the criminal procedure legislation and in those that create some registry for the use of public institutions, such as transport cards. Hereinafter, a series of schemes will be presented, that set out the rules applicable to the two topics that are the subject of this report.

55 See as an example HIRSCH (2011).

Identity reservation

The reservation of sources is enshrined in principle No. 8 of the Declaration of Principles of Freedom of Expression of the Inter-American Commission on Human Rights in the following terms: "Every social communicator has the right to reserve their sources of information, notes and personal and professional files." The content of the source reservation is given by reserving the following facts: the existence of information, its content, the origin or source of it, or the manner in which it was obtained.[56]

Constitutional safeguard: In the Latin American Constitutions there is no broad protection of anonymity in all circumstances. However, the Constitutions of Argentina, Brazil and Paraguay grant protection to informative sources, this being the only manifestation of it.

In Argentina, Article 43 of the Constitution, in relation to the regulation of the protective action, provides that although this action may be interposed to know the personal data contained in public or private records, in no case may it affect the reserve of journalistic sources.

Despite prohibiting anonymity, the Brazilian Federal Constitution accepts it only and exceptionally in the case of the reserve of journalistic sources. Thus, Title II, Chapter I, Article 5 XIV establishes that access to information is guaranteed to all and the confidentiality of the source will be safeguarded, whenever the foregoing is necessary for the performance of professional work.

Paraguay constitutionally protects the reserve of sources in article 29, which establishes that the exercise of journalism, in any of its forms, is free and not subject to prior authorization. He goes on to point out that journalists of mass media in fulfillment of their functions, will not be forced to act against the dictates of their conscience or to reveal their sources of information.

The Ecuadorian Constitution, in its Article 20, provides that the State will guarantee the conscience clause to every person, and the professional secrecy and the reserve of the source to those who inform, to emit their opinions through means or other forms of communication, or work in any communication activity. The modification to the regulation of administrative infractions of the organic communication law of 2015, establishes in its fifth article that the public and private bodies that must deliver information to the Superintendence of Information and Communication in the investigations are obliged to make such delivery in the denunciations, even the information that is subject to reservation, introducing an enormous exception to the constitutional guarantee to the reserve of sources.

Protection of anonymity in press laws: Although not all countries in the region grant constitutional protection to anonymity, many do so at a legal level. Chile, Panama, Uruguay and Venezuela are part of this model. The Chilean case will be dealt with in the following section.

Law No. 22 of 2005 of Paraguay provides in article 4 that the person responsible for the information or the news disseminated by the mass media will not be obliged to reveal the identity of its source, without prejudice to the responsibilities incurred by their statements.

The Law No. 16,099 of the year 2000 of Uruguay, which establishes regulations regarding freedom of expression, opinion and dissemination, in the final part of its first article contemplates the reservation of anonymous information sources in the following terms: "Journalists shall have the right to rely on professional secrecy regarding the information sources of the news disseminated in the media."

---

56 COLOMBIA. Constitutional court. 2009. Sentence T-298/09 Constitutional Duties of the Media. corteconstitucional.gov.co. Online, available at: http://www.corteconstitucional.gov.co/relatoria/2009/T-298-09.htm [Date of consultation: May 2, 2016]. The highlight is ours.

Regarding whistleblowers, Peru grants specific protection, but at an administrative level and only with respect to complaints in the public sector, in a similar way as the Transparency Law in Chile. The rest of the countries contemplate a degree of indirect protection, which can be found in criminal procedural legislation.

Protection of anonymity in personal data protection legislation: The laws of protection of personal data of some countries in the region establish and obligation of carrying out processes of anonymization of the personal data collected.

Generally, these provisions are found in the most up-to-date regulations issued within the last ten years. It is not so much an identity concealment, but the dissociation of information from the people concerned.

As an example, article 28 of Law No. 25.326 on Protection of Personal Data of Argentina, stipulates that the protective law is not applicable as if the information cannot be attributed to a determined or determinable person, therefor, opinion surveys, measurements and statistics, market prospecting, scientific or medical research and other analogous activities are excluded of this protection. Now, in those cases in which anonymity is not possible in the information gathering process, the dissociation technique must be applied, so that no person can be identified.

Similarly, the Peruvian personal data law incorporates the obligation to anonymize personal data if used for a purpose other than the originally stated.

Regulation that prohibits anonymity.

In this section we will delve into the laws of countries of the region that prohibit anonymity. Within the different legal systems we can find the following obstacles to anonymity:

Express prohibition of anonymity:

The Brazilian Federal Constitution in its article 5, regarding freedom of expression, states that "the manifestation of thought is free, anonymity being prohibited".

Article 57 of the Constitution of the Bolivarian Republic of Venezuela states that: "Everyone has the right to freely express their thoughts, ideas or opinions orally, through writing or any other form of expression, and to make use of any means of communication and dissemination, being censorship prohibited. Whoever makes use of this right assumes full responsibility for everything expressed. Anonymity, war propaganda, discriminatory messages, and the promotion of religious intolerance are not allowed."

The Venezuelan law on social responsibility in radio, television and electronic media of 2004 provides in its article 29 the conducts prohibited by law as well as the specific sanctions. The dissemination of anonymous messages is considered among the infractions.

Ecuador, in article 20 of the Organic Law of Communications of 2013, stipulates that the comments formulated at the foot of the electronic publications of the means of communication on the Internet must have records of the personal data of those who issue their opinions in order to identify them; thus, data such as name, email, identity card or citizenship must be supplied, as well as mechanisms to report and eliminate comments that harm the rights guaranteed in the constitution and the law. In case of non-compliance with the above, the media will incur in civil, criminal and administrative responsibility for the comments.[57]

---

57 ECUADOR, National Assembly. "Organic Law of Communication". June 25, 2013. Online, available at http://www.cncine.gob.ec/imagesFTP/63228.5_LEY_ORGANICA_COMMUNICACION.pdf [Date of consultation: November 2, 2015]

Restriction of anonymity

There are rules on registration or identification, including the obligation to keep online activity records, which do not necessarily prohibit or sanction anonymity, but still create data bases that compromise the ability to communicate or express anonymously. Within such rules, we find the following:

- Pre-paid mobile phone registration: In several Latin American countries state this requirement by law, in others its implementation is discussed, as detailed by Díaz (2017). Brazil began to demand registration in 2003, through Law No. 10.703 that provides for the registration of users of prepaid cell phones.

  In Colombia, the registration of SIM cards of all mobile phones is mandatory, justifying such public policy to generate a list of both registered devices and a blacklist with stolen equipment.

  Ecuador began to apply the registration obligation as of 2014, with respect to prepaid mobile phones as well as those paid monthly, with similar reasons to those of the Colombian case.

  Guatemala approved a cellphone registration law in 2013, which sought to combat the rise in thefts of these devices, in addition to establishing harsh penalties for such crimes.

  In Peru, the process of identification of prepaid equipment began in 2010 with the Supreme Decree 024-2010 MTC that approves the procedure for the rectification of the information recorded in the prepaid subscriber registry, and was justified in the criminal use that anonymous lines can have.

  Chile has no law on compulsory registration of SIM cards and prepaid telephone equipment, nonetheless two bills that seek to implement it are currently being discussed in the National Congress.

  Mexico is a counterpoint to the reality of all the Latin American countries previously discussed, where in 2009 the compulsory registration of SIM cards began to apply. In August 2011, this measure was terminated for several reasons, among others: it did not help to reduce the type of crimes that were sought to be fought, on the contrary, these increased; there were many practical problems when implementing the registry: telecommunication companies where often unable to verify whether the information given by customers was real, and there were few incentives for companies to seek the quality and accuracy of such data.58

  Registration of identification cards, transport and biometric data: There is a tendency in Latin America to collect a series of data from the population in the most diverse areas and services. The Mexican59 and Peruvian60 governments have enacted laws on geolocation, allowing both to locate phones that are involved in criminal activity,

---

58 GSMA 2013. "The Mandatory Registration of Prepaid SIM Card Users". Online, available at http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf [Date of consultation: November 4 of 2015]. p. eleven.

59 FORBES STAFF. "What is the Geolocation Law?" January 16, 2014. Forbes Mexico. Online, available at http://www.forbes.com.mx/de-que-va-la-ley-de-geolocalizacion/ [Date of consultation: November 04, 2015]

60 PERÚ, Presidencia de la República. "Decreto Legislativo Nº 1182". 27 de julio de 2015. En línea, disponible en http://www.elperuano.com.pe/NormasElperuano/2015/07/27/1268121-1.html [Fecha de consulta: 04 de noviembre de 2015].

without requiring a prior court order. At the same time, many states have arranged or authorized the use of biometric technologies to verify the identity of people, in an increasing trend (Ferreyra and Ucciferri, 2017).

Although all these mechanisms do not in themselves constitute restrictions on anonymity, they reduce its effectiveness: there is more and more information that, when directly linked to a name, or through the relationship between one and the other, can help identify a person.

Encryption

Regarding the encryption of communications, there are few mentions in the Latin American regulations. So we can only mention the Colombian case, the Brazilian case and the Cuban experience, the only legal systems that have regulated its use.

Brazil contemplates a constitutional prohibition on anonymity, understood as a limit to the right to freedom of expression. Although this provision does not mention the use of encryption, in 2014 there were two cases that were analyzed based on such a prohibition, but they fell on the request to remove from circulation and proscribe the use of encrypted communications software: Cryptic and Secret.

Regarding the Secret case[61], the Brazilian courts requested both Apple and Google to withdraw the application from their download platforms. Secret basically consists of a social network that allows you to chat anonymously and encrypts the data of the participants, in order to prevent them from being recognized. Cryptic[62], on the other hand, is the Secret version for Windows Phone. Although the contents of the messages can be seen by all, the encryption was used to protect the identity of the users of the same, who poured content on their Facebook contacts. The Brazilian justice not only requested the definitive removal of these applications from the digital stores of these three companies, but also requested that, in some way, these where deleted from the telephones that already had them.[63]

The civil judge Paulo Cesar de Carvalho, who knew about the case, stated that: "Freedom of expression does not constitute an absolute right, with numerous hypotheses in which its exercise conflicts with other fundamental rights or collective legal rights protected constitutionally, which will be resolved through a balance of interests at stake, in order to guarantee the right to honor, privacy, equality and human dignity and, likewise, protect childhood and adolescence (...),"[64] thus highlighting that anonymous discourse is not protected by the right to freedom of expression within the legal system of that country, as well as indicating that the balance was tipped in favor of the protection of the rights of children and adolescents (considering this applications were originally questioned because their use was linked to cases of school bullying), emphasizing the illegitimate uses of anonymity and encryption.

---

61 BRITO, E. 2014. "Use or Secret App to Discover All Segredos de Seus Amigos". Techtudo. Online, available at: http://www.techtudo.com.br/tudo-sobre/secret.html [Date of consultation: February 3, 2016]

62 JESUS, A. 2014. "Com Cryptic, Compartilhe Seus Segredos Anonymously not Windows Phone". Techtudo. Online, available at: http://www.techtudo.com.br/tudo-sobre/cryptic-app.html [Date of consultation: February 3, 2016]

63 SALA, M. 2014. A Brazilian Judge Dictates that Google Eliminate Secret of its Play Store and the Smartphones of its Users. Hipertextual.com. Online, available at: http://hipertextual.com/2014/08/eliminacion-secret-brasil [Date of consultation: February 4, 2016]

64 G1 "Justiça do ES Determines Remoção do Secret de Lojas de Aplicativos no Brasil". August 20, 2014. Globo.com. Online, available at http://g1.globo.com/tecnologia/noticia/2014/08/justica-do-es-determina-remocao-do-secret-de-lojas-de-aplicativos-no-brasil.html [Date of consultation: November 2, 2015]

Separately, the Brazilian justice has, on several occasions, ordered the blockade of the operation of the WhatsApp service throughout the country, in response to the failure to deliver copies of private conversations between persons under investigation. The company refused to deliver it, not out of stubbornness, but because of the impossibility of compliance: WhatsApp conversations, even those on their servers, are encrypted, and are only deciphered at their ends. Despite this impossibility, the judicial attack on the encryption was repeated on more than one occasion.[65]

Colombia has a paradoxical and doubtful situation. Law No. 1621 of 2013, on intelligence and counterintelligence, establishes in article 44, paragraph 2, that telecommunications service operators must offer encrypted voice calls to high-level government and intelligence personnel. However, for the rest of the population that uses communication equipment that use the "radio spectrum", it is forbidden to send messages "encrypted or in an unintelligible language", according to article 102 of Law 418 of 1997. This prohibition has been constantly renewed by multiple laws, and is in force in its current form at least until 2018. It is doubtful, but likely, that the ban will reach mobile telephony (Castañeda, 2015), including the 3G telephony protocol to modern encrypted point-to-point applications.

Cuba contemplates a specific normative mention on the use of encryption in Resolution 179/2008 on Public Internet Providers, which was modified by Resolution 102/2011 in the year 2011. In this last version of the document, in article 19 the obligations of said suppliers are listed, establishing in letter e of said provision that "for the use of any type of application that entails the encryption of the information to be transmitted, it is a requirement to process the approval, in accordance with the current provisions that regulate it". Thus, it is the Ministry of Interior that will evaluate whether or not such authorization is granted.

This norm has been criticized because it disproportionately restricts freedom of expression, depriving users of the right to carve out a private space for opinion and expression without an illegal purposes.[66] On the other hand, the mere fact of requesting authorization to use encryption turns on the Government's alerts, especially in the case of vulnerable groups who request such permission.

6.3. Anonymity and Encryption in Chilean Law

Anonymity and identity reservation.

Press law.

In Chile, following the Latin American trend, there is no constitutional mention of anonymity, but rather its first manifestation of protection can be found in the law, in relation to the different forms of professional secrecy.

Concerning the media, the regulation of journalistic sources is relevant. Law No. 19.733 on freedom of opinion and information and the exercise of journalism has brief mentions in this regard. Article 7 of this law, although it does not define the right to reserve a journalistic source, it indicates to whom it is extended (and may enforce it). The directors, publishers of social me-

---

65 Sobre la cuarta vez, Correio, "Justiça do Rio de Janeiro manda bloquear WhatsApp", 19 de julio de 2016, disponible en: http://www.correio24horas.com.br/noticia/nid/justica-do-rio-de-janeiro-manda-bloquear-whatsapp/ [fecha de consulta: 12 de febrero de 2017)

66 CARTAYA, R. 2015. Critica Relator de ONU Control a Cifrado de Datos Personales en Cuba. Martínoticias.com. En línea, disponible en: http://www.martinoticias.com/content/cuba-internet-derechos-encriptacion/97366.html [Date of consultation: February 4, 2015]

dia, journalists, students of journalism schools and foreign correspondents who work in Chile, will have the right to keep reserve about their informative source, which will be extended to the elements that work in their power and that they allow to identify it and they will not be able to be forced to reveal this even judicially.

The reserve of sources has limits. Article 1 of the Chilean press law states that the freedom to issue an opinion and the right to inform, without prior censorship, are fundamental rights of people. This entails not being persecuted or discriminated against because of one's opinions, seeking and receiving information, and disseminating it by any means, without prejudice to respond to the crimes and abuses committed, in accordance with the law. This is a repetition of what is already stated in the Constitution.

Pursuant to the above, the commission of a crime could involve the request, prior judicial order, from the persecuting entity to know the data associated with the secret source. The Criminal Judge will analyze the proportionality of the measure in terms of the injury it may cause to the right to freedom of expression in comparison to the magnitude of the crime being investigated, as well as the suitability of the intrusive measure.

Personal data protection. The Law No. 19.628 on Protection of Personal Data contains the principles and rights relating to the processing of personal data. Although it does not expressly indicate the possibility of applying anonymization mechanisms, authorization is provided for private legal persons to process the data of people without their consent. This is an exceptional situation and is allowed for the exclusive use of the private legal person, its associates and the entities to which it is affiliated, for statistical purposes, for fixing tariffs or others means of general benefit.

Another extensive authorization for the use of personal data exists in relation to "sources of public access", being this a source of data that allows its treatment in a lawful manner and without the consent of the holders, as is the case with public access databases. In this way, given the margins of vulnerability, data collection and processing in Chile allow for sufficient crossings to draw up profiles of people, facilitating their identification based on dissociated identity factors.

On the other hand, Law No. 19.628 defines statistical data as the data that, in its origin, or as a consequence of its treatment, cannot be associated with an identified or identifiable owner (Article 2, literal e). Therefore, although it is not an express mention, Chilean law would allow processing data without the consent of the owner or beyond the end of the time-lapse for which it was collected, as long as it is done in such a way that it cannot be linked to the owner (Art. 4th final paragraph). There are no provisions associated with the prevention or sanction of de-anonymization.

Criminal investigation and data retention. Another angle of the national legislation that comes into conflict with the exercise of anonymity online is in the legal framework on criminal investigation and prosecution, as well as the expressions of the same contemplated in the regulation of telecommunications.

The Criminal Procedure Code, in article 222 and following, regulates the intrusive measure of interception of communications, including electronic communications. This last point creates an obligation that is detrimental to anonymity: the retention of telecommunications metadata. The execution of this measure is regulated in more detail in Decree 142 of the Ministry of Transport and Telecommunications (Undersecretary of Telecommunications of September 2005) also known as "Regulation on interception and recording of telephone communications and other forms of communications." Retention extends to the IP numbers from which computers connect to the Internet, and the range of IP numbers maintained by each connection provider. With this it is possible, in theory, to approach whoever commits a criminal offence, by linking an

address to an IP range of a communications company, which in turn will have the information of the clients with the use of those IP numbers.[67]

On a much more rudimentary attempt to register those who use the internet, the Constitutional Court ruled in 2011 when considering a draft law that sought to force cybercafé users to register. At that time, said court stated in ground 20:

"That, of course, anyone understands - even without being a lawyer - that it is in their legitimate discretion to circulate anonymously and indistinguishably from others, without checks or records, unless in the opinion of a competent authority there are probable causes that incite to think that concrete and credible criminal acts are being perpetrated.

So that considered, this intimacy would be usurped in case of systematic, constant and focused follow-ups or monitoring to snoop to what places someone attends, for belonging to a suspected a priori category of citizens; to where they travel; what is the number of the sites they visit and the addresses contacted, precisely; with whom, or with how much duration and frequency the connections made are produced.

> **"Even more so when, from these data, today it is feasible to infer histories or individual profiles, which include habits and patterns of human behavior, until the political preferences, commercial options and social inclinations of people are revealed;".**[68]

The Court of Justice of the European Union in April 2014 declared the Data Retention Directive invalid, which initiated a similar discussion as that started by the Chilean Constitutional Court three years earlier regarding cybercafés. The ECJ expressed that such measure violates the essential content of the fundamental right to privacy and the protection of personal data and that although there is a legitimate purpose for which such an affectation occurs (public safety), the injury to such rights lacks proportionality. It remains doubtful if there will be any similar pronouncement in Chile regarding the persistent obligation to retain communication data. The contrast is greater when we consider that in Europe the conservation of data for at least six months was considered disproportionate, while in Chile the minimum is at least one year, without a maximum. It should also be considered that European Union law has a model of personal data protection for the rest of the world, while the Chilean law offers no protection and lacks adaptation to reality. Moreover, Chile is one of the few countries in the region that does not have constitutional protection of personal data (Remolina, 2012).

In this way, the measure of interception and conservation of private communications, and its special form of implementation with respect to communications made over the Internet (with IP registries) is in conflict with the idea of allowing online anonymity, as it provides sufficient information to allow accurate profiles of the users of telecommunications services, a subject that within both, Chile and Europe, has drawn attention for causing a disproportionate impact on fundamental rights.

Registration of mobile devices. In support of the fight against highly dangerous crime, a couple of bills that seek to introduce the obligation of SIM card registration on mobile equipment subscribed to the prepaid regime are currently being processed both in the Chamber of Deputies and in the Senate. Although both initiatives are in the legislative process, they include provisions that eliminate anonymity online, making the person behind the telephone fully identifiable. In addition, considering that at present the use of mobile internet surpasses the use of fixed-line Internet, it would allow accumulations of information beyond the personal data and telephone number of the user.

---

67 For more details see Diaz (2017).

68 CHILE, Constitutional Court. 2011. Ruling N ° 1894-2011-CPR (preventive control of constitutionality), ground 20.

This is even more critical in the project presented by the lower house (Bulletin 9767-15 of December 9, 2014)[69], which designated the SUBTEL (undersecretariat of telecommunications) as the body in charge of receiving the registration information made in the points of sale of SIM cards, considering that according to the regulations of criminal and administrative procedural reviewed, said undersecretariat already has the IP address registry and the sites visited by each user, giving away greater volumes of information that make the anonymity in the network an illusion.

Anonymity in the public space:

In ground 23 of the already cited judgment from the Chilean Constitutional Court (ruling STC 1984-2011) on the bill that sought to impose the registration of cybercafés users, the importance of the private physical space of the individual in relation to the exercise of fundamental rights and freedoms is highlighted. In this regard, the Constitutional Court stated:

> **"TWENTY-THIRD: That intimacy cannot only occur in the most recondite places, but it also extends, in some circumstances, to certain public spaces where specific acts are executed with the unequivocal will to subtract them from the observation of others (...).**
>
> **Thus, despite the fact that cybercafés premises are generally accessible to the public, as long as no customer or user can be inadmissible. Unlike other places of mass influx, they are usually organized internally in individual and reserved chambers or booths, precisely in consideration of the interconnection services facilitated and considering that within them a certain area of privacy has been sheltered. Correspondingly, the internet, although it is a global computer network that can be considered an open space, as well as emails and instant messaging produced there, are confidential; ".**[70]

The ruling cited not only recognizes that online privacy manifests itself in the digital environment, but also materially in a physical space. It is not enough to grant a reserve on the activity of the subject in the network and the accounts of communication services through the internet that this person can use, but also regarding the physical identity of the subject, as G. Marx posits. In effect, the Constitutional Court understands that those who use the network have an expectation of privacy that extends not only to what they do on the internet but also to the fact that they are not looked upon on what they are doing in the digital environment by other people. The people should not only be protected from identification mechanisms but also from those aspects that allow anyone to interfere in the private sphere, as it is (in this case) that others observe their computer screen.

Further in its expression, but without impact on its scope, was the ruling of the Court of Appeals of Santiago of August 21, 2017, in Case No. 34,360-2017, resolving the constitutional protective action against the use of drones of video surveillance in the municipality of Las Condes, in the Metropolitan Region of Santiago. Although it recognizes the possibility of circulating anonymously through public spaces, it limits that expectation when unlawful acts are committed.

27th In effect, it is reasonable that when accessing a public space each person aspires, among other aspects, that their conversations are not of public access, as well as that their displacement is not subject to personal registration or monitoring, that is, that they can wander freely while maintaining anonymity in front of those around them, unless that person engages in illegal

---

69 CHILE, Chamber of Deputies. 2014. Bulletin N 9767-15 Requires Mobile Telephony Operators to Register the Personal Data of Customers Acquiring a Line in the Prepaid Modality. Online, available at: https://www.camara.cl/pley/pley_detalle.aspx?prmid=10187&prmboletin=9767-15 [date of consultation: February 9, 2016]

70 CHILE, Constitutional Court. 2011. Ruling N ° 1894-2011-CPR (preventive control of constitutionality), considering twenty-third.

conducts or is involved in emergency situations, because in such cases, it is normal for such expectations of privacy to vanish [...] [Recording by the drones] are also panoramic views of these [public] places, which safeguard the anonymity of passersby, unless, of course, in the case of criminal or emergency situations in which anonymity may decrease in favor of other legitimate purposes of security.

The ruling culminates authorizing the use of drones for video surveillance. It does not explain the link between an expectation of concealment of identity as a factual situation and the normative expectation of keeping the identity in reserve in front of an investigation of a state agent. But beyond that, it arguments absurdly that audiovisual record is not an act that affects anonymity, even though it records the body of those who are watched.

- Legislation on encryption in Chile

  Regarding the encryption of communications, there is no applicable regulation or law in Chile. So far, there have been no relevant cases in which it has been judicially stated that there is a right to use encryption freely by the population, nor prohibitions.

  This is particularly important regarding the possibilities provided by the Chilean law to seize computer equipment, which's information may be encrypted, or to intercept encrypted private communications between its ends. There are no express legal authorizations in Chile for the adoption of measures that allow knowing the content of those devices or of those communications when they are encrypted, or to demand decryption keys.

Without making explicit reference to the encryption tools, the Code of Criminal Procedure provides the possibility of carrying out unnamed intrusive investigative measures, as provided by articles 226 and article 9, which requires that, prior to the completion of an investigative measure that "deprives the accused or even third party of the exercise of the rights that the Constitution secures, or it restrict or disturbs this rights", the Public Ministry requests and obtains a judicial authorization.

In this way, theoretically, the criminal judge could be asked to hack a hard drive or the encryption of a private key, although in practice it is highly difficult or expensive to execute, considering that this is a recent global practice.

In fact, the controversy between Apple and the FBI in relation to the iPhone of Syad Farook, one of those responsible for the attack carried out in December 2015 at the Inland Regional Center in San Bernardino, has shown how strong encryption is and that it cannot be hacked, even by the same company that implemented it on the device. The problem revolved, mainly, around the fact that Farook configured his phone so that after ten failed attempts to enter the code, all the information contained in the cellphone would be erased. In this way, the use of a brute force method was limited.[71]

In order to break the encryption, the FBI asked Apple to create a software that would allow the numeric code of the iPhone to pass through. The company refused. Finally, the FBI was able to enter the device, hiring an external anonymous third party who performed the procedure.[72]

---

71 DOMONOSKE, C and SELYUHK, A. 2016. Apple, The FBI And iPhone Encryption: A Look At What's At Stake. Npr.com Online, available at http://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at -stake [Date of consultation: April 24, 2016]

72 Ibíd.

Latin America hardly has the technical capabilities to access an encrypted system. Therefore, the option adjusted to the law is to request to the owner of device to access to their mail or the specific document requested, following the rules of the criminal procedure legislation referred to intrusive investigative measures. We are not sure that such a case has happened.

Two recent events show the position adopted by the Chilean State on encryption.

In the first place, the value of cryptography is revealed in the National Cybersecurity Policy, officially launched in April 2017. According to it, in order to increase security and confidence in cyberspace,

> Measures based on this policy should promote the adoption of point-to-point encryption for users, in line with international standards; and in no case will the intentional use of unsafe technologies be promoted, nor the obligation to any person or organization that provides digital services, to implement "backdoor" mechanisms that compromise or elevate the risks associated with the security technologies used.[73]

Additionally, the local development of standards and the use of cryptography stands out as an example of the potential development of a local cybersecurity industry.

Second, during the month of October 2017, eight members of Mapuche[74] communities in southern Chile were arrested and accused of terrorist illicit association for various attacks against private property, in an area of constant conflict over the demands of indigenous peoples on ancestral territories, today mostly under the ownership and exploitation of forestry companies. The Public Prosecutor's Office managed to obtain the arrest and the declaration of preventive detention for all of them, presenting a report from the Directorate of Intelligence, Drugs and Criminal Investigation of the police force of Chile, which revealed conversations between the detainees carried out by WhatsApp.[75]

None of the precedents allowed us to suppose that the police had access to the mobile equipment, nor that it had infiltrated the communications, the technical method of obtaining the information was outside the background presented by the Public Ministry. The judicial authorization of intervention was made within the parameters of Law 19,974 on intelligence of the State, and instead of detailing the mechanism of intervention, a very broad authorization of interception of communications was given.

The Supreme Court revoked the measure of preventive detention, because the order of such a measure lacked sufficient justification, by not expressing its grounds or weighing the defense's arguments. The questioning had already spread, because there was not enough connection between the nicknames supposedly used in the conversations, the facts could doubtfully be termed as terrorists, and because in her testimony, of the wife of one of the detainees, said that he did not use WhatsApp. If the police actually has mechanisms to bypass encryption, or if it was a case of staging is something that remains uncertain.

---

73 National Cybersecurity Policy, p. 19

74 The Mapuche are a group of indigenous inhabitants of south-central Chile.

75 El Mercurio, "Mensajes entre mapuches detenidos dan cuenta de envío de armas desde Argentina", 26 de septiembre de 2017, page C2.

7. Conclusions and recommendations

Anonymity and encryption are not new techniques. Nowadays they can be achieved through the use of computer tools, given that a fundamental part of the threats and injuries to the rights to freedom of expression and protection of privacy are made through the network. Thus, they are useful for the exercise and full respect of fundamental rights, considering that the Internet is today, the preferred channel for opinion and information.

Both the United Nations and the inter-American human rights system, especially in the last three years, have focused their attention on the relationship between the Internet and its effect on the human rights of the population. They have been able to identify its relevance in the exercise, protection and promotion of such rights, but it also has a series of risks. While some are not a novelty in the history of humanity, its intrusive capacity, high scope, intensity of involvement and, above all, the low cost for governments and private companies to engage in such practices with impunity is a new phenomenon. Therefore, for the individual to be protected against these risks, online anonymity and the use of encryption techniques have been identified as the most appropriate way to protect their privacy and other rights.

That is why some organizations, especially the United Nations, have emphasized that governments should not prohibit the use of such mechanisms, especially in the case of groups identified as especially vulnerable, including ethnic and social minorities, political opponents of the current government, members of civil society, human rights defenders and researchers and academics.

However, the different governments of the world have sought to regulate aspects of the Internet in order to protect other legal rights, especially public security, often to the detriment of the rights of the population. For the foregoing, measures are established that, while complying with the requirements of legality and necessity, usually do not approve the proportionality test.

The current models on Internet regulation often forget two key points: the characteristics that differentiate the network from other telecommunications services and their importance with respect to the exercise of human rights.

In Latin America, although it is possible to find regulations and provisions that protect the use of anonymity and encryption, there are also legal bodies and even constitutional mentions that hinder their use, which adds up to practices within those States and the global trend to give prominence to criminal prosecution over the protection of the right holders.

Chile is in an intermediate situation in comparison to neighboring countries, since it presents an anchylosed legislation that has areas of vulnerability. In addition, there is a tendency to present bills that include threats to the population that exist in other countries, or validate or introduce measures that in other countries have been questioned or removed from the legal system.

Finally, there are still doubts about the responses of the normative system and the persecuting system when, in fact, there are reasons that justify circumventing the mechanisms of obfuscation of identity or communications.

Therefore, the public policy proposals are the following:

- To refrain from establishing generalized prohibitions or require compliance with requirements that in practice function as a prohibition or restriction on the use of online encryption and anonymity by the population. Among others, abstain from promulgating laws that require identification for acts of expression or communication, or that have the effect of prohibiting anonymity or encryption.

- Abstain from persecuting individuals and organizations that use encryption software or the veil of anonymity on the internet to legitimately manifest their right to freedom of expression or seek to protect their privacy online.

- Refrain from developing legal norms or regulations that imply restrictions on the circulation or distribution of communications encryption technologies.

- Promote the widespread use of strong encryption and anonymity online, especially in the case of groups that can be monitored, such as human rights defenders, activists, researchers, political opponents and minorities. In this way, those who use such elements are prevented from being especially distinguishable and, also, monitored. The PNCS is a significant step forward in that regard.

- Not only to abstain from requiring, but to prohibit the intentional incorporation of vulnerabilities to hardware and software in order to access the content of communications and encrypted files, since this compromises the security of the entire network.

- Refrain from demanding, legally or judicially, the handing over of a private encryption keys, and refrain from establishing key file measures. Also refrain from requesting it in the framework of a criminal investigation in order to overcome the encryption that protects communications or files.

- Insist, in the exercise of the powers of criminal prosecution and prosecution of crimes, that investigative measures and collection of information is done in the least intrusive manner possible.

- Strengthen trust and the sense of security, promoting initiatives such as prohibiting the use of intentionally introduced computer vulnerabilities. This will not only improve citizens' perception of their online privacy and security, but will also benefit the people (those who do not compromise their online activities and services for these vulnerabilities in the system) and the State itself before the rest of the society.[76]

- Establish clear rules for the use of highly intrusive technologies in case their use is justified, in such a way that the legal description of the same delimits its application.

- Comply with global cybersecurity standards, giving prompt course to the measures of the PNCS.

---

76 CASTRO, D y MCQUINN, A. 2016. Unlocking Encryption: Information Security and the Rule of Law. Information Technology & Innovation Foundation. En línea, disponible en: http://www2.itif.org/2016-unlocking-encryption.pdf [Consultation date: 31 May,2016], pp. 33-34

Bibliography

ABELSON, H et al. 2015. Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications". Computer Science and Artificial Intelligence Laboratory Technical Report.

ACADEMIA DOMINICANA DE LA LENGUA. "*Encriptar". Academia Dominicana de la Lengua. En línea, disponible en http://academia.org.do/encriptar/ [Fecha de Consulta: 03 de diciembre de 2015]

ARTHUR, C. 2013. How Internet Encryption Works. The Guardian. En línea, disponible en: http://www.theguardian.com/technology/2013/sep/05/how-internet-encryption-works [Fecha de consulta: 10 de diciembre de 2015]

BLUMENTHAL, M. 2007. "Encryption: Strengths and Weaknesses of Public-Key Cryptography". En línea, disponible en:

http://www.csc.villanova.edu/~tway/courses/csc3990/f2007/csrs2007/01-pp1-7-MattBlumenthal.pdf [Fecha de consulta: 07 de enero de 2016]

BLUEPRINT FOR FREEDOM OF SPEECH. Peru – Whistleblowing Protection. blueprintforfreespeech.net. En línea, disponible en: https://blueprintforfreespeech.net/document/peru [Fecha de consulta: 29 de abril de 2016]

BOTERO, C. 2015. "En Defensa del Cifrado". ElEspectador.com. En línea, disponible en: http://www.elespectador.com/opinion/defensa-del-cifrado [Fecha de consulta: 13 de enero de 2016]

BRITO, E. 2014. "Use o App Secret Para Descobrir Todos os Segredos de Seus Amigos". Techtudo. En línea, disponible en: http://www.techtudo.com.br/tudo-sobre/secret.html [Fecha de consulta: 03 de febrero de 2016]

CARTAYA, R. 2015. Critica Relator de ONU Control a Cifrado de Datos Personales en Cuba. Martínoticias.com. En línea, disponible en: http://www.martinoticias.com/content/cuba-internet-derechos-encriptacion/97366.html [Fecha de consulta: 04 de febrero de 2015]

CASTAÑEDA, D. 2015. "La peligrosa ambigüedad de las normas sobre cifrado de comunicaciones en Colombia". Digital Rights LAC, disponible en: https://www.digitalrightslac.net/es/la-peligrosa-ambiguedad-de-las-normas-sobre-cifrado-de-comunicaciones-en-colombia/ [fecha de consulta: 27 de abril de 2016]

CASTRO, D. 2011. Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising. The Information Technology & Innovation Foundation. En línea, disponible en: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/dae-library/benefits_and_limitations_of_industry_self-regulation_for_online_behavioral_advertising.pdf [Fecha de consulta: 27 abril de 2016]

CASTRO, D y MCQUINN, A. 2016. Unlocking Encryption: Information Security and the Rule of Law. Information Technology & Innovation Foundation. En línea, disponible en: http://www2.itif.org/2016-unlocking-encryption.pdf [Fecha de consulta: 31 de mayo de 2016]

CLEMENS, A. 2004. "No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key" en UCLA Journal of Law and Technology 8(2). En línea, disponible en http://www.lawtechjournal.com/articles/2004/02_040413_clemens.pdf [Fecha de consulta: 06 de enero de 2016]

COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, Relatoría Especial Para la Libertad de Expresión. "Libertad de Expresión e Internet". 2013. COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, Relatoría Especial Para la Libertad de Expresión. "Libertad de Expresión e Internet".

CRYPTO MUSEUM. 2015. "Clipper Chip". Crypto Museum. En línea, disponible en http://www.cryptomuseum.com/crypto/usa/clipper.htm [Fecha de consulta: 04 de enero de 2016]

DECCAN HERALD. 2010. Internet Now Single Biggest Source of Global Information. Deccan Herald. En línea, disponible en: http://www.deccanherald.com/content/117379/internet-now-single-biggest-source.html [fecha de consulta: 09 de febrero de 2016]

DIARIO HOY. "El Nuevo DNI de Randazzo en la Mira: Privacidad en Peligro". 30 de junio de 2014. Diario Hoy. En línea, disponible en http://diariohoy.net/politica/el-nuevo-dni-de-randazzo-en-la-mira-privacidad-en-peligro-30932 [Fecha de consulta: 04 de noviembre de 2015]

DÍAZ, Marianne. 2017. "Retención de datos y registro de teléfonos móviles: Chile en el contexto latinoamericano". En línea, disponible en https://www.derechosdigitales.org/wp-content/uploads/informe-marianne-retencion-de-datos.pdf [Fecha de consulta: 23 de octubre de 2017]

DIFFERENCEBETWEEN.NET. Difference Between PGP and GPG. Differencebetween.net. En línea, disponible en http://www.differencebetween.net/technology/software-technology/difference-between-pgp-and-gpg/ [Fecha de consulta: 31 de mayo de 2016]

DOMONOSKE, C y SELYUHK, A. 2016. Apple, The FBI And iPhone Encryption: A Look At What's At Stake. Npr.com. En línea, disponible en http://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake [Fecha de consulta: 24 de abril de 2016]

EL COMERCIO. 2015. WhatsApp es la App de Mensajería Más Popular del 2015. Elcomercio.pe. En línea, disponible en: http://elcomercio.pe/tecnologia/actualidad/whatsapp-app-mensajeria-mas-popular-2015-noticia-1862521 [Fecha de consulta: 25 de abril de 2016]

EL PAÍS. 2016. WhatsApp Activa el Cifrado de los Mensajes Para Todos los Usuarios. Elpaís.com. En línea, disponible en: http://tecnologia.elpais.com/tecnologia/2016/04/05/actualidad/1459875233_301649.html [Fecha de consulta: 25 de abril de 2016]

EWOW. 2014. "Educación y Ciencia, Cifrado Asimétrico" citado en VILLALOBOS, J. 2014. "Consideraciones para el uso de Cifrado en las Bases de Datos". 31 de julio de 2014. .Seguridad. En línea, disponible en http://revista.seguridad.unam.mx/numero22/consideraciones-para-el-uso-de-cifrado-en-las-bases-de-datos [Fecha de consulta: 03 de diciembre de 2015]

FARIVAR, C. 2015. Paris Police Find Phone With Unencrypted SMS Saying "Let's go, We're Starting". Armstechnica.com. En línea, disponible en: http://arstechnica.com/tech-policy/2015/11/paris-police-find-phone-with-unencrypted-sms-saying-lets-go-were-starting/ [Fecha de consulta: 25 de abril de 2016]

FERREYRA, E. y UCCIFERRI, L. 2017. Cuantificando identidades en América Latina. https://adcdigital.org.ar/wp-content/uploads/2017/06/ADC-Cuantificando-identidades-en-LatAm.pdf [Fecha de consulta: 20 de octubre de 2017]

FORBES STAFF. "¿De qué va la Ley de Geolocalización?". 16 de enero de 2014. Forbes México. En línea, disponible en: http://www.forbes.com.mx/de-que-va-la-ley-de-geolocalizacion/ [Fecha de consulta: 04 de noviembre de 2015]

FUNDÉU BBVA. "Encriptar es Oculta un Mensaje con una Clave". Fundéu BBVA. En línea, disponible en http://www.fundeu.es/recomendacion/encriptar-es-un-termino-valido/ [Fecha de consulta: 03 de diciembre de 2015]

G1. "Justiça do ES Determina Remoção do Secret de Lojas de Aplicativos no Brasil". 20 de agosto de 2014. Globo.com. En línea, disponible en http://g1.globo.com/tecnologia/noticia/2014/08/justica-do-es-determina-remocao-do-secret-de-lojas-de-aplicativos-no-brasil.html [Fecha de consulta: 02 de noviembre de 2015]

GARCÍA, L. 2004. La Protección de la Identidad de las Fuentes Periodísticas a la Luz de los Instrumentos Internacionales de Derechos Humanos y de los Estándares de sus Órganos de Aplicación. Anuario de Derecho Constitucional. En línea, disponible en: http://www.juridicas.unam.mx/publica/librev/rev/dconstla/cont/2004.2/pr/pr10.pdf [Fecha de Consulta: 29 de Enero de 2016]

GELLMAN, B y NAKASHIMA, E. 2015. "As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security". The Washington Post. En línea, disponible en https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html [Fecha de consulta: 06 de enero de 2016]

GILBERTSON, S. 2010. "Why Your Digital Fingerprint Makes You Easy to Track". Wired.co.uk. En línea, disponible en: http://www.wired.co.uk/news/archive/2010-01/29/your-digital-fingerprint-makes-you-easy-to-track [Fecha de consulta: 19 de enero de 2016]

GONZÁLEZ, G. 2014. "Cómo Crear una Contraseña Súper Segura en Cinco Sencillos Pasos". Hipertextual.com. En línea, disponible en http://hipertextual.com/archivo/2014/06/crear-contrasena-segura/ [Fecha de consulta: 07 de enero de 2016]

GRABOW, R. 1997. McIntyre v. Ohio Elections Commission: Protecting the Freedom of Speech or Damaging the Electoral Process?. Catholic University Law Review 46(2). En línea, disponible en: http://scholarship.law.edu/cgi/viewcontent.cgi?article=1542&context=lawreview [Fecha de consulta: 05 de mayo de 2016]

GREENBERG, A. 2014. "Hacker Lexicon: What is End-to-End Encryption?". Wired.com. E**n línea**, disponible en: http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ [Fecha de consulta: 18 de enero de 2016]

GREENE, T. 2015. "Mandating Backdoors for Encrypted Communications is a Bad Idea". Networkworld. En línea, disponible en: http://www.networkworld.com/article/2945374/security0/mandating-backdoors-for-encrypted-communications-is-a-bad-idea.html [Fecha de consulta: 12 de enero de 2016]

GSMA. 2013. The Mandatory Registration of Prepaid SIM Card Users: A White Paper. En línea, disponible en: http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf [fecha de consulta: 09 de febrero de 2016]

GSMA. 2014. The Mobile Econonomy Latin America 2014. En línea, disponible en: http://www.gsmamobileeconomylatinamerica.com/GSMA_Mobile_Economy_LatinAmerica_2014.pdf [fecha de consulta: 09 de febrero de 2016]

HENN, S y SELYUKH, A. 2015. "After Paris Attacks, Encrypted Communication Is Back In Spotlight". NPR.org. En línea, disponible en http://www.npr.org/sections/alltechconsidered/2015/11/16/456219061/after-paris-attacks-encrypted-communication-is-back-in-spotlight [Fecha de consulta: 05 de enero de 2016]

HERNÁNDEZ, V. (2016). Libertad de Expresión y Anonimato. En: ASOCIACIÓN POR LOS DERECHOS CIVILES. Libertad de Expresión en el Ámbito Digital. El Estado de la Situación en Latinoamérica, pp. 7-45.

HIGGINS, P. 2015. On the Clipper Chip's Birthday, Looking Back on Decades of Key Escrow Failures. Eff.org. En línea, disponible en: https://www.eff.org/deeplinks/2015/04/clipper-chips-birthday-looking-back-22-years-key-escrow-failures [Fecha de consulta: 25 de abril de 2016]

HIRSCH, D. 2011. The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?. Seattle University Law Review 34. En línea, disponible en: http://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=2003&context=sulr [Fecha de consulta: 01 de febrero de 2016]

HOW-TO-GEEK. "Brute-Force Attacks Explained: How All Encryption is Vulnerable". How-to-Geek.com. En línea, disponible en: http://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable/ [Fecha de consulta: 07 de enero de 2016]

INGRAHAM, N. 2013. 'Harry Potter' Author J.K. Rowling Assumed Male Identity to Secretly Release a Detective Novel. The Verge. En línea, dsponible en: http://www.theverge.com/2013/7/14/4522398/harry-potter-author-j-k-rowling-secretly-releases-detective-novel [Fecha de consulta: 29 de enero de 2016]

JESUS, A. 2014. "Com Cryptic, Compartilhe Seus Segredos Anonimamente no Windows Phone". Techtudo. En línea, disponible en: http://www.techtudo.com.br/tudo-sobre/cryptic-app.html [Fecha de consulta: 03 de febrero de 2016]

JUST, M. 2011. Key Escrow Definition en JAJODIAL, S y VAN TILBORG, H (editores) 2011. "Encyclopedia of Cryptography and Security". Estados Unidos, Springer USA, segunda edición.

KOEBLER, J. 2014. "How the NSA (Or Anyone Else) Can Crack Tor's Anonymity". Motherboard. En línea, disponible en: http://motherboard.vice.com/read/how-the-nsa-or-anyone-else-can-crack-tors-anonymity [Fecha de consulta: 19 de enero de 2016]

LEE, M. 2015. Microsoft Gives Details About its Controversial Disk Encryption. The Intercept. En línea, disponible en https://theintercept.com/2015/06/04/microsoft-disk-encryption/ [Fecha de consulta: 11 de diciembre de 2015]

LEONARD, J. 2015. "US to Take Backdoor Approach to Introducing Backdoors to Counter Encryption". Computing.uk. En línea, disponible en http://www.computing.co.uk/ctg/news/2426334/us-to-take-backdoor-approach-to-introducing-backdoors-to-counter-encryption [Fecha de consulta: 05 de enero de 2016]

LEVY, S. 1994. "Battle of the Clipper Chip". The New York Times. En línea, disponible en http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?-module=Search&mabReward=relbias:r,{%221=%22:=%22RI:6=%22}=&src=pm&pagewanted=2&_r=0 [Fecha de consulta: 15 de diciembre de 2015]

LIN, F. 2010. "Cryptography's Past, Present, and Future Role in Society". En línea, disponible en https://engineering.wustl.edu/current-students/student-services/ecc/Documents/Lin.pdf [Fecha de consulta: 06 de enero de 2016]

MARX, G. 2001. "Identity and Anonymity: Some Conceptual Distinctions and Issues for Research" en Documenting Individual Identity: The Development of State Practices in the Modern World. Princeton University Press. En línea, disponible en http://web.mit.edu/gtmarx/www/identity.html [Fecha de consulta: 19 de octubre de 2015]

McCULLOUGH, B. 2014. "The NSA Tried this Before -What the 90s Debate Over the Clipper Chip can Teach Us About Digital Privacy". Internet History Podcast. En línea, disponible en http://www.internethistorypodcast.com/2014/08/the-nsa-tried-this-before-what-the-90s-debate-over-the-clipper-chip-can-teach-us-about-digital-privacy-debates/ [Fecha de consulta: 04 de enero de 2016]

MEO, A. 2010. Consentimiento Informado, Anonimato y Confidencialidad en Investigación Social. La Experiencia Internacional y el Caso de la Sociología en Argentina. Aposta. Revista de Ciencias Sociales. En línea, disponible en: http://apostadigital.com/revistav3/hemeroteca/aines.pdf [Fecha de consulta: 05 de mayo de 2016]

McDONALD, W. Søren Kierkegaard (1813—1855). Internet Encyclopedia of Philosophy. En línea, disponible en: http://www.iep.utm.edu/kierkega/ [Fecha de consulta: 29 de enero de 2016]

MINISTERIO DE SEGURIDAD, "La Presidenta Presentó el SIBIOS". 07 de noviembre de 2011. Ministerio de Seguridad. En línea, disponible en http://www.minseg.gob.ar/la-presidenta-present%C3%B3-el-sibios [Fecha de consulta: 04 de noviembre de 2015]

MINISTERIO DE TRANSPORTE Y TELECOMUNICACIONES, Subsecretaría de Telecomunicaciones. 2014. Sector Telecomunicaciones. En línea, disponible en: http://www.subtel.gob.cl/wp-content/uploads/2015/01/PPT-Series-Septiembre-2014-041214-v1.pdf [fecha de consulta: 09 de febrero de 2016]

MOYA, R. 2003. La Libertad de Expresión en la Red Internet. Revista Chilena de Derecho Informático 2.

NPR STAFF. 2015. Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right'. NPR.org. En línea, disponible en: http://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right [Fecha de consulta: 11 de enero de 2016]

PC MAGAZINE ENCYCLOPEDIA. "Definition of Back Door". PC Magazine.com. En línea, disponible en http://www.pcmag.com/encyclopedia/term/38339/back-door [Fecha de consulta: 05 de enero de 2016]

PEREZ, E y PROKUPECZ, S. 2015. "First on CNN: Paris Attackers Likely Used Encrypted Apps, Officials Say". CNN. En línea, disponible en http://edition.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption/ [Fecha de consulta: 05 de enero de 2015]

PRIVACY INTERNATIONAL. 2015. Securing Safe Spaces Online: Encryption, Online Anonymity and Human Rights. En línea, disponible en: https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf [Fecha de consulta: 29 de enero de 2016]

PRIVACY INTERNATIONAL. What is Metadata?. Privacyinternanal.org. En línea, disponible en: https://www.privacyinternational.org/node/53 [Fecha de consulta: 11 de enero de 2016]

REMOLINA, N. 2012. Aproximación Constitucional de la Protección de Datos Personales en Latinoamérica. Revista Internacional de Protección de Datos Personales 1.

ROGAWAY, P. 2015. The Moral Character of Cryptographic Work". En línea, disponible en: http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf [Fecha de consulta: 10 de diciembre de 2015]

SALA, M. 2014. Un Juez Brasileño Dicta que Google Elimine Secret de su Play Store y de los Smartphones de sus Usuarios. Hipertextual.com. En línea, disponible en: http://hipertextual.com/2014/08/eliminacion-secret-brasil [Fecha de consulta: 04 de febrero de 2016]

SANS INSTITUTE. 2001. "History of Encryption". En línea, diponible en https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730 [Fecha de consulta: 03 de diciembre de 2015]

SHAIK, R. 2014. How Crucial is Anonymity for Sexual Exploration and Promoting Sexual Rights Activism. Genderit.org. En línea, disponible en: http://www.genderit.org/es/node/4147 [Fecha de consulta: 29 de enero de 2016]

SIMPSON, D. 2015. Letter to the Editor: The Benefits of Anonymous Political Speech. The Washington Post. En línea, disponible en: https://www.washingtonpost.com/opinions/the-benefits-of-anonymous-political-speech/2015/01/25/092abefe-a326-11e4-91fc-7dff95a14458_story.html [Fecha de consulta: 29 de enero de 2016]

SOLOVE, D, ROTENBERG, M and SCHWARTZ, P. 2006. Privacy, Information and Technology. New York, ASPEN Publishers.

TEMPLE-RASTON, D. 2015. "FBI Director Says Agents Need Access To Encrypted Data To Preserve Public Safety". NPR.org. En línea, disponible en http://www.npr.org/sections/thetwo-way/2015/07/08/421251662/fbi-director-says-agents-need-access-to-encrypted-data-to-preserve-public-safety [Fecha de consulta: 05 de enero de 2016]

THE GUARDIAN. 2008. Harmful Content on the Internet: Self-Regulation is the Best Way Forward. The Guardian. En línea, disponible en: http://www.theguardian.com/media/organgrinder/2008/aug/01/post88 [Fecha de consulta: 01 de febrero de 2016]

USLegal. "Data Encryption Law & Legal Definition". uslegal.com. En línea, disponible en http://definitions.uslegal.com/d/data-encryption/ [Fecha de consulta: 03 de diciembre de 2015]

USLegal. "Malware Law & Legal Definition". uslegal.com. En línea, disponible en: http://definitions.uslegal.com/m/malware/ [Fecha de consulta: 07 de enero de 2016]

VÉLIZ, C. 2013. 'Whistleblowers': Los Canarios Morales en la Mina de la Democracia. The Huffington Post. En línea, disponible en: http://www.huffingtonpost.es/carissa-veliz/whistleblowers-los-canari_b_3560252.html [Fecha de Consulta: 29 de enero de 2016]

VOCABULARY.COM., "Anonymity". En línea, disponible en: http://www.vocabulary.com/dictionary/anonymity [Fecha de consulta: 15 de Octubre de 2015]

VOORHOOF, D. 2010. "Internet and the Right of Anonymity" en Proceedings of the Conference Regulating the Internet. Belgrado, 2010.

WYSOPAL, C. "Static Detection of Application Backdoors". En línea, disponible en http://www.veracode.com/sites/default/files/Resources/Whitepapers/static-detection-of-backdoors-1.0.pdf [Fecha de consulta: 06 de enero de 2016]

ZAMORANO, E. 2012. Chile: Servel Publicó Datos de 13 Millones de Ciudadanos. FayerWayer. En línea, disponible en: https://www.fayerwayer.com/2012/08/chile-servel-publico-datos-personales-de-13-millones-de-ciudadanos/ [Fecha de consulta: 04 de febrero de 2016]

ZETTER, K. 2015. "Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors". Wired.com. En línea, disponible en: http://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ [Fecha de consulta: 12 de enero de 2016]

ZIMMERMANN, P. 1999. Why I Wrote PGP: Part of the Original 1991 PGP's User Guide (updated in 1999). philzimmermann.com. En línea, disponible en https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html [Fecha de consulta: 09 de diciembre de 2015]

Legislation, jurisprudence and other legal documents:

ARGENTINA, Cámara de Diputados de la Nación. 2008. "Ley Nº 25.326 Sobre Protección de Datos Personales Y Normas Reglamentarias y Complementarias". En línea, disponible en http://www1.hcdn.gov.ar/dependencias/dip/textos%20actualizados/25326.010408.pdf [Fecha de consulta: 05 de noviembre de 2015]

BRASIL, Lei nº 10.703, de 18 de julho de 2003. En línea, disponible en http://www.anatel.gov.br/legislacao/leis/469-lei-10703 [Fecha de consulta: 04 de noviembre de 2015]

BRASIL, Cámara de Diputados. "Constitución Federal de la República de Brasil". 2010. En línea, disponible en http://english.tse.jus.br/arquivos/federal-constitution [Fecha de consulta: 04 de noviembre de 2015]

CHILE, Cámara de Diputados. 2014. Boletín N 9767-15 Exige a los Operadores de Telefonía Móvil Registrar los Datos Personales de los Clientes que Adquieran una Línea en la Modalidad de Prepago. En línea, disponible en: https://www.camara.cl/pley/pley_detalle.aspx?prmid=10187&prmboletin=9767-15 [fecha de consulta: 09 de febrero de 2016]

CHILE. 2000. Código Procesal Penal. En línea, disponible en: http://www.leychile.cl/Navegar?idNorma=176595 [fecha de consulta: 08 de febrero de 2016]

CHILE, Ministerio Secretaría General de Gobierno. 2001. "Ley Nº 19.733 Sobre Libertades de Opinión e Información y Ejercicio del Periodismo". En línea, disponible en http://www.leychile.cl/Navegar?idNorma=186049 [Fecha de consulta: 04 de febrero de 2016]

CHILE, Ministerio de Transporte y Telecomunicaciones, Subsecretaría de Telecomunicaciones. 2005. Decreto 142 del Ministerio de Transporte y Telecomunicaciones, Reglamento sobre interceptación y grabación de comunicaciones telefónicas y de otras formas de comunicaciones. En línea, disponible en: http://www.leychile.cl/Navegar?idNorma=242261 [fecha de consulta: 08 de febrero de 2016]

CHILE, Tribunal Constitucional. 2011. Sentencia Rol N° 1894-2011-CPR (control preventivo de constitucionalidad).

COLOMBIA. Corte Constitucional. 2009. Sentencia T-298/09 Deberes Constitucionales de los Medios de Comunicación. corteconstitucional.gov.co. En línea, disponible en: http://www.corteconstitucional.gov.co/relatoria/2009/T-298-09.htm [Fecha de consulta: 02 de mayo de 2016]

COLOMBIA, Ministerio de Defensa Nacional. 2009. "Resolución 912 de 2008". En línea, disponible en https://www.redjurista.com/documents/r_mdef_0912_2008.aspx [Fecha de consulta: 03 de noviembre de 2015]

CORTE INTERAMERICANA DE DERECHOS HUMANOS, Caso Escher y Otros v Brasil (Sentencia de 06 de julio de 2009). En línea, disponible en http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf [Fecha de consulta: 19 de octubre de 2015]

CUBA, Ministerio de la Informática y las Comunicaciones. 2011. "Resolución 102/2011". En línea, disponible en: http://www.di.sld.cu/documentos/resol/resol_102_2011.pdf [Fecha de consulta: 04 de febrero de 2015]

ECUADOR, Asamblea Nacional. "Ley Orgánica de Comunicación". 25 de junio de 2013. En línea, disponible en http://www.cncine.gob.ec/imagesFTP/63228.5_LEY_ORGANICA_COMUNICACION.pdf [Fecha de consulta: 02 de noviembre de 2015]

ECUADOR, Arcotel. 2013. "Codificación de la Norma que Regula el Procedimiento para el Empadronamiento de Abonados del Servicio Móvil Avanzado (SMA) y Registro de Terminales Perdidos, Robados o Hurtados". En línea, disponible en http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/codificacion_norma_empadronamiento.pdf [Fecha de consulta: 03 de noviembre de 2015]

ECUADOR. 2008. "Constitución de la República del Ecuador". En línea, disponible en: http://www.oas.org/juridico/PDFs/mesicic4_ecu_const.pdf [Fecha de consulta: 02 de febrero de 2016]

GUATEMALA, 2013. "Decreto Número 8-2013. Ley de Equipos Terminales Móviles". En línea, disponible en: http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2013/pdfs/decretos/D08-2013.pdf [Fecha de Consulta: 03 de noviembre de 2015]

KONRAD-ADENAUER-STITFUNG. "Cláusulas de Libertad de Expresión: Venezuela". En línea, disponible en http://www.kas.de/upload/auslandshomepages/mediosla-tinos/venezuela/clausulas_de_libertad_de_expresion_-_venezuela.pdf [Fecha de consulta: 02 de noviembre de 2015]

KONRAD-ADENAUER-STITFUNG. "Constitución de la Nación Argentina". En línea, disponible en http://www.kas.de/upload/auslandshomepages/medioslatinos/argentina/argentina_constitucion.pdf [Fecha de consulta: 04 de noviembre de 2015]

NACIONES UNIDAS, Consejo de Derechos Humanos. 2011. "Informe del Representante Especial del Secretario General para la Cuestión de los Derechos Humanos y las Empresas Transnacionales y Otras Empresas, John Ruggie". En línea, disponible en: http://www.ohchr.org/Documents/Issues/Business/A.HRC.14.27_sp.pdf [Fecha de consulta: 13 de enero de 2016]

NACIONES UNIDAS, ORGANIZACIÓN ESTADOS AMERICANOS. 2013. Declaración Conjunta Sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión. En línea, disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927 [Fecha de consulta: 29 de enero 2016]

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. Comisión Interamericana de Derechos Humanos. Declaración Sobre Principios Sobre Libertad de Expresión. En línea, disponible en: https://www.cidh.oas.org/basicos/basicos13.htm [Fecha de Consulta: 02 de mayo de 2016]

ORGANIZACIÓN DE ESTADOS AMERICANOS. Comisión Interamericana de Derechos Humanos. 2015. Informe Anual de la Comisión Interamericana de Derechos Humanos 2014. Informe Anual de la Relatoría Especial para la Libertad de Expresión. En línea, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/anuales/Informe%20Anual%202014.pdf [Fecha de consulta: 28 de enero de 2016]

PANAMÁ, Asamblea Nacional Legispam. 2005."Ley Número 22 de 2005 Que Prohíbe la Imposición de Sanciones por Desacato, Dicta Medidas en Relación al Derecho a Réplica, Rectificación o Respuesta y Adopta Otras Disposiciones". En línea, disponible en http://www.oas.org/juridico/spanish/mesicic2_pan_anexo_34_sp.pdf [Fecha de consulta: 05 de noviembre de 2015]

PARAGUAY, Convención Nacional Constituyente. "Constitución Nacional". 1992. En línea, disponible en http://www.oas.org/juridico/spanish/par_res3.htm [Fecha de consulta: 04 de noviembre de 2015]

PERÚ, Congreso de la República. 2013. "Ley Nº 29.733 de Protección de Datos Personales". En línea, disponible en http://www.claro.com.pe/portal/recursos/pe/pdf/Ley29733.pdf [Fecha de consulta: 05 de noviembre de 2015]

PERÚ, Presidencia de la República. 2015. "Decreto Legislativo Nº 1182". 27 de julio de 2015. En línea, disponible en http://www.elperuano.com.pe/NormasElperuano/2015/07/27/1268121-1.html [Fecha de consulta: 04 de noviembre de 2015]

PERÚ, Presidencia de la República. 2010. "Decreto Supremo Nº 024-2010-MTC que Aprueba el Procedimiento para la Subsanación de la Información Consignada en el Registro de Abonados Pre Pago". En línea, disponible en transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_1902.pdf [Fecha de consulta: 04 de noviembre de 2015]

REPÚBLICA BOLIVARIANA DE VENEZUELA, Asamblea Nacional. 2004. "Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos". En línea, disponible en http://www.nci.tv/archivos/Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electr%C3%B3nicos.pdf [Fecha de consulta: 03 de noviembre de 2015]

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. 2014. Comunicado de Prensa 54/14. En línea, disponible en: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf [Fecha de consulta: 08 de febrero de 2016]

UNITED NATIONS. 2012. General Assembly, Human Rights Council. Twentieth Session. Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development. En línea, disponible en: ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc [Fecha de consulta: 25 de abril de 2015]

UNITED NATIONS, Human Rights Council. 2015. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of opinion and Expression, David Kaye".

UNITED NATIONS. 2014. The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights. En línea, disponible en: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf [fecha de consulta: 09 de febrero de 2016]

URUGUAY, Comunicaciones e Informaciones. 2002. "Ley Nº 16.099 Díctanse Normas Referentes a Expresión, Opinión y Difusión, Consagradas por la Constitución de la República". En línea, disponible en http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=16099&Anchor= [Fecha de consulta: 05 de noviembre de 2015]


DERECHOS
DIGITALES
América Latina