DERECHOS DIGITALES
América Latina

2010-2020

Trends related to ***regulatory developments in privacy and the internet*** in Latin America:

VALENTINA HERNÁNDEZ B.

Texto por Valentina Hernández Bauzá
Portada y diagramación: Constanza Figueroa.
Edición: Vladimir Garay.

Diciembre de 2020

Contents

Executive Summary

This report offers an analysis of the evolution of regulatory and case law trends in Latin America over the course of a decade. It addresses five areas related to privacy, its protection, and its violation through technological media (personal data protection, surveillance and intelligence activities, crimes against intimacy, rules on data retention -particularly in telecommunications- and biometrics regulations) and the challenges that the region faces in order to best address them in the medium- and long-terms. A series of key databases in these areas were used along with searches of legislation and case law in each country's judiciary and legislative portals and open internet searches.

In the area of personal data, the relevant legislation passed during this decade is reviewed along with the response to ARCO rights, the increase in constitutional recognition of the right to the protection of personal information, cross-border transfer and case law on the right to be forgotten. In regard to activities and intelligence, communications interception measures, their recording and intervention in computer systems are reviewed, as scant changes have been made given that it is frequently assumed that preexisting investigation rules apply to the internet. The author then turns to protection against surveillance measures such as requests for these measures and the recognition of encryption techniques.

In the section on crimes against intimacy, the amount of legislation enacted in each country over the course of this decade is listed, along with rules regarding the crime of disseminating or revealing intimate images and material, the dissemination of intimate material without consent and unauthorized access to data. The trends reflect legislative progress resulting from the updating of personal information rules and the criminal regulations created to adjust them to cybercrime and crimes committed online. In regard to telephone data and identity records, the author reviews changes to prepaid and SIM card services registration and telephone and/or digital communications records, identifying a limited trend to install new registration regimes.

There is a modern trend -which has already been manifested in Argentina and Mexico- to criminalize dissemination of intimate material without consent in the area of identity-related crimes. There are also multiple intelligence and criminal investigation laws that include hypotheses that allow for intervening computer communications and systems, as well as data retention. The article closes with a discussion of the legislation passed on biometrics and fingerprint and DNA regulation over the course of the decade in question. We believe that there will be important new developments in this area over the next ten years.

Introduction

The United Nations General Assembly (2016) has observed that the swift pace of technological development allows for an increase in the capacity of governments, companies, and individuals to conduct data surveillance, interception and collection activities that may violate or transgress human rights. In particular, they may violate the right to privacy established in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. As such, this is a matter of increasing concern:

> "...violations and abuses regarding the right to privacy in the digital age that may affect all individuals, including where there are particular effects for women, as well as children and those vulnerable and marginalized."[1]

Edward Snowden's revelations in 2013 demonstrated the risk to privacy that the use of communication tools poses in regard to personal privacy. This is not only due to the possibility of criminal intrusions, but also involves states' political interest in communications records. This may include the (voluntary or involuntary) cooperation of the private companies that broker those communications. In 2015, CCCBLab offered a summary on surveillance in Latin America, determining that various governments in the region conduct their own surveillance.[2] States and companies also engage in other forms of recording information, such as the growing accumulation of biometric information and the use of surveillance technologies in public spaces.

These points will be studied below as axes in which both state and private intervention allow entities to generate highly precise profiles of each subject. Unfortunately, legal protection does not always keep up with technological progress. This brief review explores how much of it is based on existing rules formulated prior to the digital revolution and how much of that is motivated by, or based on, changes to legislation over the past decade. We will thus highlight regional trends and future challenges related to providing individuals with more protection in the face of technological development.

---

1 United Nations General Assembly. 2016. The right to privacy in the digital age. Available at: https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1&referer=/english/&Lang=S

2 CCCBLab. 2015. Vigilancia Masiva en América Latina. 2015. Available at: http://lab.cccb.org/es/vigilancia-masiva-en-america-latina/.

Topics of study

Protection of personal data

Legislation

Several countries in the region modified their personal data regimes through the introduction of laws on the topic or by replacing earlier laws.

Just before the start of the decade, Mexico's Federal Constitution was modified and Article 16 on autonomous protection of personal data was introduced. In 2010, express dispositions for the handling of personal data in the private sector were introduced through the Federal Law on Protection of Personal Data Held by Private Entities (2010), which was followed by the General Law on the Protection of Personal Data Held by Regulated Entities (2017).

In Costa Rica, Law No. 8.968 on the protection of individuals against the handling of their personal data (2011) is the main regulatory body on this topic. It is complemented by the Regulation on the Law Protecting Individuals Against the handling of Their Personal Data, Executive Decree No. 37554-JP (2013).

El Salvador does not have a general law on personal data protection, but the Law Regulating Information Services on Personal Credit History (2011) was passed early on during the decade. A process to study a bill for a personal data protection and habeas data law has begun. This study addresses topics such as the regulation of applications that require facial recognition as well as those that have access to mobile phone information.[3]

Colombia has a general law that dates back to the beginning of the decade: Statutory Law No. 1581 of 2012 established general provisions for personal data protection. This law followed previous rules such as Statutory Law 1266 of 2008, which regulated habeas data and the use of information in the financial and credit sphere.

Peru has passed Law No. 29.773 (2011) on personal data and its regulation, Supreme Decree No.003-2013-JUS (2013).

Nicaragua also created regulations in the early part of the decade through Law No. 787 on Personal Data Protection (2012) and its regulations, Decree 36/2012, which addresses types

3 Legislative Assembly of the Republic of El Salvador, June 5, 2019, see: https://www.asamblea.gob.sv/node/9644

of consent and expressly includes the rights to access, rectification, cancellation, and opposition. Interestingly, Nicaraguan law defines "the right to be digitally forgotten" in the following terms: "The owner of the data has the right to ask social media platforms, browsers and servers to remove and cancel the personal data in their archives." (Our translation.)

More recently, Brazil's General Law on Personal Data Protection (2018) went into effect. It is one of the most modern laws on the subject and orders the creation of an independent public authority. Soon after, Panama passed its first general law on the subject, Law No. 8 on Personal Data Protection (2019).

Other countries updated their personal data regulations through constitutional changes. Chile's Political Constitution was modified to include personal data protection in its catalogue of fundamental rights through Law 21.096 of 2018.

The Dominican Republic's 2015 Constitution recognizes the right of all people to make decisions about the use of data about them and their assets within the article on the right to personal privacy and honor and included habeas data action in the chapter on constitutional guarantees. The country already had a law on personal data protection, Law No. 172-13 (2013).

While Cuba does not have a law on personal data protection, Article 97 of the 2019 Cuban Constitution recognizes the right of all people to access their personal data in records, archives or other databases and public information and to request that it not be released and obtain its due correction, rectification, modification, updating or cancellation. It also establishes that the use and handling of this data is conducted in accordance with the terms established under law.

Other countries do not yet have general laws on personal data, but there has been legislative progress in this area. Ecuador's Constitution recognizes protection of personal data as a fundamental right and regulates habeas data, and an organic personal data protection bill was published in 2019.[4]

Paraguay does not have a general personal data protection law either, but Law No. 1682 of 2001, which regulates private information, contains various rules and principles related to the topic. Over the past decade, the law underwent numerous changes, mainly in areas such as updating property data, the right of all people to collect, store and handle data, and cases in which an individual's property and financial data may be disseminated. There is also a personal data protection bill, which was submitted in 2019.[5]

In summary, Latin America has followed the global trend, establishing personal data pro-

4 Ecuador. 2019. National Assembly. Memorandum PAN-CLC-2019.- Personal data protection law bill. See: https://www.nmslaw.com.ec/wp-content/uploads/2019/09/Proyecto-de-Ley-Org%C3%A1nica-de-Protecci%C3%B3n-de-Datos-Personales.pdf

5 Paraguay. 2019. Personal data protection law bill. See: https://observatoriolegislativocele.com/paraguay-proyecto-de-ley-de-proteccion-de-datos-personales-2019/

tection legislation. The regional trend is to have general laws that address this area even in countries in which there were already special rules for the financial and credit areas.

As such, only six Latin American countries lacked personal data laws by the end of the decade. These are Bolivia, Cuba, Venezuela, Honduras, Ecuador, and Guatemala, though all of them have some sort of constitutional recognition of personal data protection. Ecuador already has a bill and Guatemala is holding a series of discussions and meetings aimed at reaching the same goal. Paraguay and El Salvador have special laws that contain provisions on personal data; they will be considered special personal data laws for these purposes.

Thirteen of the 19 countries have regulatory bodies (two with non-exclusive bodies), and two of the remaining six are in the process of creating them. It is also important to highlight the cases of Chile and Argentina. In the first, a personal data protection bill is being discussed that would replace the existing legislation, which is over 20 years old. Argentina has a 2018 bill designed to modernize current legislation.

It is important to mention that while the trend has been to legislate, not all of these countries have a global personal data law, but instead one that refers to one particular segment. Of the 13 laws on personal data protection, 11 are general laws. The rest apply to one area of personal data protection. El Salvador has the "Law to regulate information services on individuals' credit history" and Paraguay has "Law No. 1682 of 2015 regulating private information." The trend in the region is to have a global personal data protection law.

The decade between 2010 and 2020 was also productive in the area of new personal data laws, though a few laws were updated prior to this period. The laws that date back to before the period of study of this article are those of Chile (1999), Argentina (2000) and Uruguay (2008), with bills to update them pending (Chile, 2017 and Argentina, 2018).

In regard to content, a superficial reading shows that Spanish law has influenced personal data protection legislation in the region and the bills currently being discussed. In particular, we will consider the incorporation of ARCO (access, rectification, cancellation, and opposition) rights formulated in this way within each country's data laws for this point. In the northern part of the region, special laws expressly address them in 62% of cases, in Mexico, Nicaragua, Panama and the Dominican Republic, and further south in Peru. The Ecuadorean, Argentinean and Chilean bills also explicitly incorporate them. As such, of the eight laws issued or changed between 2010 and 2020, five fully address ARCO laws and two do so partially. Three bills have been introduced in countries that do not currently have such laws.

Over the past decade, Latin American countries have sought to become centers of technological development. In view of this, regulatory updates have had to address handling of personal data that goes beyond national borders, including the pressure to meet international personal data protection standards, particularly European ones, in order to develop business activities and persuade large companies to confidently open offices. The Dominican Repub-

lic, Colombia, Peru, Panama, Nicaragua, Mexico, and Brazil regulated or modified current legislation on international data transfer between 2010 and 2020, while Argentina, Paraguay, Ecuador and Chile include them in their bills.

Case law

Some cases are exemplary in the area of data protection, particularly in regard to the deindexing of contents and efforts to eliminate news articles that include personal information including names.

While this matter is intimately linked to freedom of expression, in the paragraphs that follow, we will describe some exemplary decisions that reveal the various discussions around different concepts of "the right to be forgotten."

In Chile, the July 2019 Supreme Court Ruling, No. 1279-2019 established that information from the media is of public interest and cannot be eliminated, even in the case of personal information. The Court ruled, however, that it must be updated to represent the current status of a person who has completed their sentence. While the petitioning party presented arguments based on the right to be forgotten, both the Court of Appeal and Supreme Court did not rule on that basis. Rather, the highest court decided that digital versions of the newspapers involved must correct the information rather than removing it from the internet. While the surgeon who sought the remedy of protection presented arguments based on the right to be forgotten, it was not recognized by the Chilean government.

In Mexico, in the case of Anonymous v. Google Mexico, the Federal Institute for Access to Information and Data Protection ordered the company to de-index certain URLs from its search engine and erase a person's information from its databases based on the request of an individual who stated that a Google search of their name revealed information about their deceased father and brothers as well as information about their business activities. It was determined that this was personal data management because it was public information about a person. Google Mexico was found responsible even though Google US handled the data.

The courts in Argentina ruled in 2014 on the case of Rodríguez v Google, Inc., which involved the Yahoo! And Google search engines. In this case, the complainant alleged that she was associated with pages with pornographic content. The highest court in that country ruled that search companies do not have objective responsibility, but rather a subjective responsibility regime. As such, "it is configured if they have effective knowledge of the legality of the content that is challenged and, in spite of this, do not act diligently to remove the corre-

sponding link." (Our translation.)[6] In referring to the content itself, the Supreme Court later ruled that the monitoring and filtering of content could involve prior censorship.

Colombia also has relevant case law. The Constitutional Court heard the case Martínez v. Google in 2013. It involved a request to eliminate the complainant's name from information that connected them to a cartel. They requested that the name be eliminated by both the newspaper that published the piece and the Google search engine. The Constitutional Court ruled that the newspaper must correct the information but released Google of all responsibility due to its role as a mere intermediary.

The case heard by the General Personal Data Protection Directorate in Peru, No. 045-2015-JUS/DGPDP, is worthy of note. Here, the Directorate determined that the Peruvian affiliate of Google, Inc. is subject to the country's personal data protection law in a case in which a subject who was found not to be criminally responsible asked to be removed from the search engine. This is due to the fact that Google searches for information that contains the personal information of Peruvian citizens in order to facilitate access to information for its users, and because its geolocalization function offers users the option of only receiving information from Peruvian sites.

In the 2018 case DPN v. Google Brasil Internet Ltda, DPN asked Google, Microsoft and Yahoo! To remove links with information referring to a case of fraud from the search results. The Superior Court ruled in favor of DPN, ordering the companies to remove information connecting DPN to the case of fraud from their search engines, referring to the "right to be forgotten."

Search engines were parties to cases in Colombia, Peru, Brazil, and Argentina. In Peru, a court ruled that its regulations applied to Google (both its affiliate and the North American parent company) given that the engine handles Peruvian citizens' data and its geolocalization function causes citizens of that country to preferentially access information originating in Peru. De-indexing was ordered in Brazil, and the right to be forgotten was expressly recognized. In Colombia, in contrast to Peru, Google was freed of responsibility given that it acts as an intermediary. In Argentina, it was established that search engines do not have an objective responsibility for their content, and the suit was dismissed in that it may involve prior censorship.

---

6 Llorente and Cuenca. 2015. El fallo "Rodríguez vs. Google" de la Corte Suprema de Argentina: ¿hacia una vía latinoamericana para el Derecho al Olvido? See: https://ideas.llorenteycuenca.com/wp-content/uploads/sites/5/2015/01/150129_informe_especial_reputacion_internet_ESP.pdf

Surveillance and intelligence activities

There are several legal updates in the area of surveillance, including both criminal investigation efforts and intelligence activities. In general, they seek to create regulatory frameworks to obtain information that can be useful for governments based on modern forms of communication.

In regard to communications interception, El Salvador has a Special Law for Telecommunications Intervention (2010), while Honduras passed Decree 243-2011, the Special Law on Private Communications Interventions (2012). In Colombia, the relevant regulations are set out in the Criminal Procedure Code, specifically in a change made in 2011.

Nicaragua has the Law on the Prevention, Investigation and Prosecution of Organized Crime and on the administration of seized, confiscated, and abandoned assets (2010). It is also important to mention the 2014 Criminal Procedure Code.

Mexico passed a national security law in 2005 that mentions communications interventions. However, we will focus on the regulations from the period under study: the federal law against organized crime (2016) and the Criminal Procedure Code (2014).

Full procedural regulations also were issued during the decade in question. Argentina's Criminal Procedure Code (2019), Ecuador's Comprehensive Organic Criminal Code (2014) and Venezuela's 2012 Criminal Procedure Code are worthy of note. Brazil reformed its Criminal Procedure Code in regard to guarantee judges in 2019 (Legal Decree No. 3.189 Criminal Procedure Code).

There were also updates in the area of intelligence. Paraguay issued Law 5241 in 2014 to create the national intelligence system. For its part, Uruguay passed Law 29.696 "Approval and regulation of the national State intelligence system" in 2018.

Various trends can be identified in these changes. Most countries in the region have regulations on phone taps, recording of communications and intervention in computer systems, and the majority of them were developed during the period under study. In regard to the regulatory body that governs these issues, some countries use intelligence law, some general criminal procedure codes, and other laws on organized crime or special rules on intercepting communications. The countries that have regulations on these matters that were created between 2010 and 2020 are Mexico, El Salvador, Honduras, Nicaragua, Colombia, Ecuador, Paraguay, Uruguay, Venezuela, Argentina, and Brazil.

Communications interception is the measure with the greatest presence in the regulations of the countries studied. While it is addressed in the special laws on intelligence and organized

crime, as a means of investigating crimes or conducts included in said regulations, it is also covered in criminal procedure laws and regulations focused entirely on the measure itself. In other words, various approaches are used to regulate them based on the crimes investigated and investigative methods used. This is the longest standing investigative measure, and it is linked to recording communications in procedure codes, as communications are not only tapped but also recorded to be listened to by those who ask judicial officials for access to the content. However, there are intelligence laws in which recording is considered a special procedure separate from surveillance.

One of the characteristics of the laws studied is the variability of the timeframes of the rules on the interception of different forms of communication. While these are usually considered to be included in telephonic communications and written correspondence, there are variations in regard to whether the various types of electronic communications are covered. A series of examples demonstrates this.

Article 143 of Argentina's 2019 Criminal Procedure Code refers to surveillance. It states that the judge may order the interception and capture of postal correspondence, telephone calls, electronic interactions, or any other form of communication or with another effect sent by the defendant or their recipient. That is exceptional in nature. Article 146 covers this provision and states that surveillance will be recorded using tapes or other means.

Article 476 of Ecuador's 2014 Comprehensive Organic Criminal Code addresses interception of communications or computer data. The judge may order this measure once the prosecutor has submitted a substantiated request. The same article refers to the recording of said content.

The fourth section of Venezuela's Organic Criminal Procedure Code, "On the use and interception of correspondence and communications," contains Article 205, which is entitled "Interception or recording of private communications." Under the law, the interception or recording of private communications may be ordered, and the contexts will be transcribed and added to the records.

In a 2011 change made to Colombia's Criminal Procedure Code, Article 235 on the interception of telephonic and similar communications states that the prosecutor may order, with the sole purpose of seeking evidentiary materials and physical evidence, the tape or similar recording of telephonic, radio and similar communications that use the electromagnetic spectrum if the information is of interest for the purposes of the proceedings.

The Special Law on Interventions in Private Communications of Honduras (2012) defines the intervention in communications in Article 3. It states that it is a special investigation technique that consists of authorities listening to, capturing, recording, saving, or observing a communication made by any means of transmission, emission or reception of signs, symbols, written signals, images, sounds, emails or information of any nature or by any means or type of transmission.

El Salvador also has a special law on phone tapping (2010). Article 13 on the execution of the intervention states that the entirety of the communication will be recorded and saved unedited through the mechanisms that the technician identifies and in accordance with judicial authorization.

The special law on organized crime passed in Nicaragua (2010) states in Chapter VIII "On the interception of communications" that judges may grant requests to impede, interrupt, intercept or record communications, electronic correspondence, other radioelectric and computer means of fixed, mobile, wireless, and digital communications or communications of any other nature solely for the purposes of criminal investigation. Article 213 of its Criminal Procedure Code (2014) addresses phone tapping.

In regard to Mexico's updated legislation, Chapter 6, "On intervention in private communications," of the 2016 federal law against crime states that intervention in these communications covers the entire communications system or programs that are the product of technological evolution that allow for the exchange of data, information, audio, video, messages, and electronic files that record, preserve the content of the conversations or record data that identify the communication. Article 18 determines which private communications may be the object of intervention. Article 294 of the Criminal Procedure Code (2014) also refers to this point.

Brazil's Criminal Procedure Code underwent a 2019 reform that included telephone tapping, the flow of communications in computer and telematic systems or other forms of communication in the preliminary definitions when referring to guarantee judges and their role in the authorization of intrusive measures.

Another important issue involves information gathering, including interception, for intelligence purposes. Chile's 2004 law on intelligence (Law No. 19.974) outlines special procedures for obtaining information that include intervening in communications, computer systems and networks, listening and electronic recordings and intervention in technological systems meant to process communications or information. In Paraguay, the law that created the National Intelligence System (2014) follows the same line as Chile, establishing a list of procedures for obtaining special information, which are exceptional and require judicial authorization. The four procedures outlined in this law are the same as those listed in the two aforementioned laws. In Uruguay, Law No. 19.696 of 2018 of the National State Intelligence System includes the same measures as the Chilean law and are similar in content.

In accordance with international human rights standards, the measures outlined above must follow the principles of legality, legitimate objective, necessity and proportionality and the existence of a competent legal authority, among others.

Under the revised Mexican federal law against organized crime, intervention in private communications is regulated by law and authorization from a judicial authority must be requested and granted. The activity must be conducted in accordance with the terms approved by

the judge. The request must be duly substantiated, and a deadline is set for the interception. The activity is also limited, in the sense that the authorization must identify the person or persons to be subjected to the measure; the place or places where it will be conducted, if possible; the type of communications; duration; process to be conducted and the lines, numbers or devices to be tapped; and, where applicable, the name of the telecommunications company through which the communication subject to the intervention is to be conducted. (Our translation.) It also states that, when the Public Prosecutor's Office deems such action necessary, a request identify the object and need may be submitted. The Criminal Procedure Code states that prior judicial authorization is required because the activity affects rights enshrined in the Constitution. This Code contains rules similar to those regarding intervention set out in the aforementioned special law, and it reiterates the requirements of necessity and delimitation of the object of the measure.

In El Salvador, the principles of the special law for wiretapping are set out in Article 2. It addresses jurisdiction ("Wiretapping may only be conducted once written and duly justified judicial authorization is given under the terms of this law"); proportionality, reserve and confidentiality; temporariness and subjective limitation ("The intervention should solely depend on the telecommunication and means of support of the individuals presumably implicated in the crime, whether the owners or regular or temporary users directly or indirectly including telecommunications by interconnection. Intervention may also involve telecommunications devices and other means of input available to the public.") (Our translation.) The application of the measure is bounded by a list of crimes contained in the law, which establishes conditions and outlines their execution. It also refers to judicial oversight of the intervention, stating that the authorizing judge must ensure that the intervention is conducted in accordance with the terms set out in the law and under the conditions set in the ruling.

In the case of Honduras, the legislation starts by recognizing the fundamental rights of the person who will be subjected to the measure. As such, the introductory statements of the decree that contains the communications intervention law address the right to intimacy, its international and national recognition and state that rights may only be restricted by judicial order and in accordance with the law. Furthermore, the preamble refers to fighting (or decreasing) crime, which suggests that this is recognized as the motivation for the regulation of intervention.

This law sets out a series of principles such as proportionality, necessity and adequacy, confidentiality, and jurisdictional reserve (the intervention may only be authorized by the competent jurisdictional body in writing and it must be substantiated and follow the terms of this law). Authorization, applications, and contents are regulated, among other elements.

The Nicaraguan regulation is shorter. It states that communications interception will be conducted at the express and substantiated request of the National Prosecutor General or General Director of the National Police and shall be authorized by criminal district judges.

It establishes a timeframe for the authorization and content of this practice that outlines its application.

Colombian law states that communications intervention must be substantiated in writing and conducted solely to seek evidentiary materials and physical evidence. Notably, it is regulated as part of "Actions that do not require prior judicial authorization." (Our translation.) That does not mean that judicial officials do not participate in the process, but that their participation is part of a subsequent hearing to ensure the legality of the measures taken in which the guarantee judge reviews the actions taken.

Ecuadorean laws also establish requirements for communications intervention such as prior judicial authorization, a reasoned request, the existence of indicators that are important for the purposes of the investigation (which are set out in the Code), the timeframe for the interception and confidentiality. In addition, it states that "the interception, recording and transcription of communications that violate the rights of children and adolescents, especially in cases that revictimize in acts of violence against women or nuclear family members and sexual, physical and psychological and other forms of violence are prohibited." (Our translation.)

The Paraguayan intelligence law, which covers the three intrusive measures analyzed, includes the following principles: respect for the legal order, respect for the democratic regime, respect for constitutional rights, prior judicial authorization, proportionality, reserve, and the exclusive use of information. It includes a section on the protection of rights and guarantees to reinforce this. Another noteworthy point is that it identifies the exceptional nature of these investigative procedures and states that they may only be used in cases in which the National Intelligence System agencies and institutions cannot obtain this information from open sources. Furthermore, it must be necessary to meet a series of objectives set out in the law.

Uruguay's intelligence law sets out its principles in the second article, stating that State National Intelligence System agencies shall develop their activities in strict compliance with the Constitution and the principles of the government's democratic republican regime with full respect for human rights. Later on, it expressly refers to the principle of legality and deliberation. Article 6 sets out rights, duties and guarantees and reiterates that the work of the State Intelligence System and activities of its members must strictly comply with the provisions set out in Section II of the Constitution and international laws and agreements adopted by the State in the area of protecting inhabitants' human rights and guarantees. It states that judicial authorization must be secured in order to use special information procurement procedures.

Article 205 of Venezuela's Organic Criminal Procedure Code states that the means of interception may be established in accordance with the law. Furthermore, the prosecuting entity will provide a substantiated request to the judge, specifying elements such as the crime being investigated and the duration of the surveillance.

The 2019 Code in Argentina opens by stipulating the general principles and guarantees that establish the protection of intimacy and privacy, the restriction of fundamental rights (which must be exercised in accordance with the principles of suitability, reasonableness, proportionality, and necessity) and the reason for judicial rulings, among others. In regard to the means of interception, it regulates the authorization of the measure, which must be requested in writing or orally by the Prosecutor's Office, specifying elements such as its purpose.

In Brazil, the 2019 procedural modification on guarantee judges establishes that these will be responsible for ensuring the legality of the criminal investigation and safeguarding of individual rights. It also mentions prior judicial authorization of certain measures including interception.

In short, all of the regulations issued during the period under study address, to a greater or lesser extent, requirements for the execution of intervention measures, which means protection of the rights of the individuals to whom they apply. However, the substantiated/reasoned request, judicial authorization and legal consecration are the minimum elements of each of them. It is also common for them to express the principles that govern these measures, which include proportionality and the protection of fundamental rights, to name a few.

Encryption

Individuals may opt to use encrypted systems to protect their privacy from public or private external omissions. Generally speaking, this is not subject to legal authorization or prohibition. On the contrary, it is commonly accepted as a necessary security practice for both communications (that is, information in transit) and data stored on personal devices or those of public and private institutions (that is, stored information). This has become especially important for human rights defenders, activists, journalists, and others who may be subject to surveillance and prosecution based on their work. The countries that have expressly referred to encryption during the decade under study are: Colombia (2013), Cuba (2011, repealed in 2019), Honduras (2012) and El Salvador (2010).

In Colombia, Article 44 of Statutory Law 1621 states that telecommunications service operators must offer agencies that conduct intelligence and counterintelligence activities a channel that allows for encrypted voice calls at a reasonable cost and utility, and for a specific number of users in conditions that do not degrade the operator's network or the quality of the service that it provides. In this case, the right to access to encryption by intelligence systems is granted exclusively. By contrast, "communications equipment that uses the electromagnetic spectrum," such as cell phones, are in principle prohibited from sending "encrypted messages or messages in an unintelligible language" (Law 418 of 1997, extended until 2022, our translation).

Article 21 of El Salvador's Communications Interception Law states that in a process of intervention that depends on protected material (due to encryption, password protection or a similar reason), it may be preserved until it is translated or interpreted. It also defines it, noting its purpose of making a communication inaccessible or unintelligible to those who are not authorized to access it. Similarly, the 2012 Special Law on Telephone Interventions passed in Honduras defines encryption as a technical capacity.

Finally, Cuba established the duty to secure official approval to use any type of application or service through a private network that involves encrypting the information transmitted in a 2011 regulation. The measure was repealed in 2019.

Crimes against intimacy

Three general aspects are key in regard to the criminal punishment of crimes against privacy or intimacy. On the one hand, there are rules in place regarding crimes against intimacy that may or may not apply to crimes in the digital environment, as is the case of procuring or disseminating private images or information. Second, there are approaches that refer to the form of commission instead of addressing legal assets tied to intimacy, as is the case of the regulation of cybercrimes with targets that may consist of private information. Finally, there are various legislative efforts to update all of these rules.

Non-consensual dissemination of intimate images (frequently referred to in the media as "revenge porn") has been widely reported during this decade. Activism has played a key role in making the issue visible and producing legal changes. Of the 19 countries under study, several categorize crimes of disseminating images with sexual content or images taken in private spaces. This categorization is very varied in terms of both content and scope given that not all of the applicable rules are from the decade under study. Furthermore, that variation is conditioned by the age of the criminal rules or limited political recognition of these cases, failing to consider all of the material that may be disseminated or to refer to sexual content (they generally refer to violating intimacy at the generic level), which is part of the nature of gender violence that is common to these actions. In some cases, a specific place of the production of the material disseminated (private places) is considered a requirement for the criminal categorization and no reference is made to electronic media.

However, there are countries in which the criminal rules can be used to configure hypotheses, though limited, regarding dissemination of sexual content or intimate images without consent.

In Peru, Article 154-B of the Criminal Code expressly outlaws the dissemination of audiovisual images and material with sexual content. In El Salvador, the categorization of the crime of improper dissemination of data or personal information includes images, video, audio, and other content (which may include intimate content). Ecuador recognizes the crime of violating intimacy and identifies the dissemination and publication of voice, audio, and video as an element of this crime. Several states in Mexico approved the Olimpia's Law bill. The Dominican Republic's Criminal Code punishes transmission of a person's image when they are in a private space, which may include intimate images, without consent.

The recognition of dissemination of intimate content without consent has been a trend during the decade, and various bills seek to categorize it as a special crime. The common element is the lack of consent from one of the participants in the intimate act. In Chile, the bill expressly refers to the internet, and Mexico expressly recognizes cyberstalking. Colombia incorporates an aggravating factor if the victim is a woman.

As of December 2019, various Mexican states passed Olimpia's Law, which was named for ac-

tivist Olimpia Coral Melo.[7] Its purpose is to recognize the dissemination of intimate content without consent as a crime against intimacy and to recognize cyberstalking as a crime that generates sexual violence on the internet. Mexico City adopted the law, as have the following states: Aguascalientes, Baja California Sur, Chiapas, Coahuila, Guanajuato, Guerrero, Estado de México, Nuevo León, Oaxaca, Puebla, Querétaro, Veracruz, Yucatán and Zacatecas. Mexico City-based organizations expressed their concern regarding the approval of criminal rules understood as deficient for preventing revictimization and protecting fundamental rights.[8]

In 2019, Argentina opened the first case on dissemination of intimate content.[9] This was included in the Criminal Code reform that was conducted that same year, and it was defined as "dissemination of images or audio recordings of a sexual nature produced in an intimate setting without consent." (Our translation.)[10]

In 2018, a bill was proposed in Chile about dissemination of intimate images without consent. It is still under discussion and some changes have been made to the text. In principle, it sought to punish anyone who "disseminates or publishes online or via any other electronic channel images with sexual content or connotation that have been obtained as part of the private life of a couple without the consent of one of the partners. Internet site managers who fail to take the images down will be subject to the same sanction." (Our translation.)

A bill against dissemination of intimate images without consent was submitted in Colombia in 2019 that would sanction anyone who "shares intimate material: videos, photographs, documents without the consent of the affected person" (Our translation) with an aggravated sentence if the victim is a woman,[11] thus recognizing the gender component behind this conduct. Ecuador's Comprehensive Criminal Code (2014, modified in 2017) contains provisions relevant to this section.[12]

It is necessary to analyze two related crimes separately: the crime of unauthorized access to data and the dissemination of personal information. They are not the same, but illegally procuring information may lead to dissemination either publicly or to interested third parties.

7 El Sol de México. ¿De qué se trata la Ley Olimpia? December 03, 2019. See: https://www.elsoldemexico.com.mx/mexico/justicia/de-que-se-trata-la-ley-olimpia-violencia-digitial-porno-venganza-ciberacoso-mujeres-coral-melo-4539259.html

8 Notoriox. "Preocupa a R3D y ARTICLE 19 aprobación de Ley Olimpia", December 7, 2019. See: https://notoriox.com/preocupa-a-r3d-y-articulo-19-aprobacion-de-ley-olimpia/

9 Infobae, "Pornovenganza y Sextorsión: Arranca hoy el primer juicio en el pais por difundir material sexual íntimo", November 21, 2011. See: https://www.infobae.com/sociedad/policiales/2019/11/21/pornovenganza-y-sextorsion-arranca-hoy-el-primer-juicio-en-el-pais-por-difundir-material-sexual-intimo/

10 https://www.argentina.gob.ar/noticias/pornovenganza-nuevo-delito-incluido-en-la-reforma-del-codigo-penal

11 https://nmas1.org/news/2019/08/29/colombia-carce-pornovenganza

12 Ecuador. 2014. Criminal Procedure Code. Available at Redlatam.

Criminalization of unauthorized access to information is not necessarily a trend during this decade, but there has been a series of data leaks during this period in the region that have made this crime the subject of public discussion. To name just a few cases, in 2016, data on guests who stayed at Hyatt hotels in Argentina, Chile, Brazil, Panama and Mexico was stolen.[13] The F-Secure blog made a map of cyberattacks in Latin America in 2019, and the countries that stand out include Peru, Chile and Mexico.[14]

The countries that included a rule punishing unauthorized access to data during this period are Peru (2013) and El Salvador (2016). Peru expressly includes computer crimes within this law and not as part of a more general crime. Nicaragua regulates it within the Criminal Code ("unauthorized access and use of data," our translation).

The dissemination of personal information is categorized as a crime in some Latin American regulatory bodies, including those of the Dominican Republic, Peru, El Salvador, and Ecuador. Peru also criminalized illegal trafficking of personal information. El Salvador has the "Special Law on Computer and Related Crimes," which was passed in 2016 and focuses on these topics. Article 337 of the Dominican 2014 Criminal Code punishes attacks on the intimacy of private life.

Peru passed legislation on the topic during this decade through its computer crime law (2013, modified in 2014) and Criminal Code, which added Article 154A on illegal trafficking of personal information in 2014. This reveals an increasing regulatory concern regarding protection through criminal sanctions on private information from various angles.

13 We live security. 2016. https://www.welivesecurity.com/la-es/2016/01/15/roban-datos-huespedes-hyatt-paises-latinoamerica/

14 F-Secure. 2019. https://blog.f-secure.com/es/mapa-de-los-ataques-ciberneticos-en-latinoamerica-2018/

Telephone identity record mandates

Over the past few decades, various countries in the region have maintained or tried to introduce general identity record mandates related to the use of prepaid mobile devices. The argument is usually that this measure is taken to combat crimes such as cell phone theft. However, the use of unregistered phones has been linked to the commission of various crimes such as scams, fraud, communications among criminal groups and drug trafficking. Based on this, several countries have chosen to keep a record of all adult telephony users with a view to address these issues, as this allows them to trace who is communicating with the device. There have been critiques of the quality of these records and difficult situation that users could face in the case of device theft.

Certain countries in the region have decided to introduce mandatory SIM card registration for telephone service users. SIM cards are very important given that they hold a series of user data such as their phone number, carrier, contacts, photos, and bank account information.[15] SIM card registration thus goes beyond linking the phone to a user, given that even if the person switches phones,[16] the card usually survives, following the person who has the device.

The following countries in the region have (or had) prepaid number registries: Mexico, Costa Rica, Guatemala, El Salvador, Cuba, Argentina, Peru (2004), Colombia and Uruguay. It is worth noting that Mexico abandoned this measure, but there have been discussions about reintroducing it.[17] Bills on this topic have been submitted in Chile, but they have not been passed. Similarly, there is no relevant information in Costa Rica on this topic, but there is a "Register Your Prepaid Phone"[18] platform managed by the Superintendency of Telecommunications (SUTEL).

Guatemala has a law on mobile terminal equipment (2013) and prepaid devices must be registered.[19] Argentina's regulation on the quality of telecommunications services (2013) addresses this, and it launched "Your Line Is Your Own," an initiative promoted by the Ministry of Security, National Telecommunications Entity (ENACOM) and the Ministry of Commu-

15 Augusto Peña. ¿Qué información guarda tu tarjeta SIM? El internacional, March 11, 2019. Available at: https://www.eluniversal.com.mx/techbit/que-informacion-guarda-tu-tarjeta-sim

16 Estimates generated in Argentina suggest that people do so every 18 months. See La Nación, ¿Con qué frecuencia reemplazan los argentinos sus celulares? November 21, 2016 Available at: https://www.lanacion.com.ar/tecnologia/cada-cuanto-tiempo-cambian-los-argentinos-sus-celulares-nid1958175

17 https://digitalpolicylaw.com/mexico-alista-otra-iniciativa-para-registrar-las-tarjetas-sim-prepago-tras-intento-fallido-de-2009/

18 https://digitalpolicylaw.com/apenasuna-sexta-partedelaslineas-prepagoesta-registrada-en-sutel/

19 https://www.guatemala.com/noticias/sociedad/como-y-quienes-deben-registrar-su-celular-en-guatemala-para-que-no-lo-suspendan.html

nications in October 2018 addresses mandatory registration of prepaid devices.[20] Uruguay introduced Decree 274/14 dated October 1, 2014, which regulates registration of prepaid devices.

In Guatemala, Article 14 of the law on mobile terminal equipment from 2013, states: "Users who acquire a SIM card must show the salesperson their personal identity document to verify that they are an adult. In the case of foreign nationals, a current passport must be provided. The user or buyer who acquires a SIM card must provide the salesperson a physical or electronic copy of their legal personal identity document. The copy that the salesperson keeps must list the SIM number -that is, the phone number that the user is acquiring-, or the aforementioned information must be written on the respective form, which may be electronic. The salesperson must store those files or documentation for a period of three (3) years." (Our translation.)

In Nicaragua, Article 45 of the regulations of the Law on the Prevention, Investigation and Prosecution of Organized Crime (2010), referring to the official registration and identification of users, establishes that this includes companies or individuals that sell mobile phones and SIM cards through any channels. As such, the sellers of these cards are registered. Police and prosecution service officials will then have access to this record in the exercise of their roles and powers.

20 https://www.argentina.gob.ar/registra-tu-linea

Rules on the retention of communication data

In addition to registering users linked to a phone number or service and rules on communications interception, it is necessary to review the cases in which conservation measures or the provision of data on communications are established. This involves data related to telephonic communications, such as the duration of the interaction or numbers of the participants, as well as data associated with internet browsing and communication.

Decree No. 360 on the Security of Information and Communication Technologies and National Cyberspace Defense of Cuba (2019) orders the creation of mechanisms and procedures that ensure the identification of the origin of connections, including switched connections. It also states that this information can be recorded and saved for at least one year (Article 87). The decree also states that there is an obligation to provide the competent authorities the records on these connections and to cooperate with efforts to investigate violations of the rules and security incidents.

Article 39 of the Special Law on Telephonic Interventions of Honduras (2012) requires companies that provide phone services to store data on all connections for each user for five years. This covers both landlines and mobile phone lines.

Article 65 of Nicaragua's law on organized crime (2010) states that public and private companies that offer phone, computer, or other electronic services and those that use the electromagnetic and radio spectrum must maintain an official record of the users or clients that use them. We note that this includes both phone and internet communications.

In Venezuela, Article 10 of Administrative Ordinance 171 of 2017 refers to data service records and requires mobile and fixed telephony companies to store and make available a record of subscribers that contains elements such as sender and recipient IP addresses, the date and time of the connection and geographic coordinates. The operators must provide this information when requested.

Peru issued Legislative Decree 1182 on this topic in 2015. The final complementary provisions included in this document establish that data derived from telecommunications must be stored. Public telecommunications service concessionaires and public entities related to these services must store these data for 12 months in computer systems that can be consulted and provide the information online and in real time.

In Colombia, Article 44 of Law No 1621 on collaboration with telecommunications operators (2013) states that telecommunications service operators will be required to provide intelligence and counterintelligence agencies with the communications logs of associated telephone subscribers, technical data that can be used to identify said subscribers and localization of cells in these terminals, among other things.

Finally, Article 15 of Brazil's Civil Internet Framework (2014) states that internet applications

providers constituted as legal entities that exercise that activity in a professional organized manner and for profit must maintain internet application access records in a controlled environment for six months.

Paraguay does not have any regulations in place in this area. The 2015 bill that sought to requires internet service providers to store communications data failed in 2015 (Díaz, 2017).

In short, of the 19 countries included in the study, seven have regulations on telephonic or digital communications records issued during the decade under study.

Rules on biometrics

Although there was a strong tendency to incorporate and regulate aspects related to biometrics throughout Latin America during this decade, its scope was limited to the regulation of uses within investigation processes. While we know that there is a growing use of biometric technologies for identification and identity verification purposes, particularly with public surveillance purposes and control of the provision of state services,[21] including the creation of biometric databases by States, an important part of this growing usage is not accompanied by special legal modifications. The changes that have been made have not focused on the aspects that are most closely linked to the digitalization of information or the datafication of individuals in their interaction with various institutions.

It is important to mention some important changes in any case. In El Salvador, the 2009 Criminal Procedure Code (modified in 2016) addresses fingerprints in regard to the identification of defendants (Article 83), which this method can be used to achieve. Article 187 addresses DNA tests. Honduras' Criminal Procedure Code (1999) includes a rule (Article 107) on physically examining and taking samples from defendants. This article was incorporated in 2013. No examples of these tests and samples are provided. Article 238 of Nicaragua's Criminal Procedure Code (2014) includes a mention of body searches that includes tests of bodily fluids and other physical interventions.

Argentina's 2019 Federal Criminal Procedure Code refers to both fingerprints and DNA. In regard to the former, Article 66 on identification and domicile states that personal data, unique characteristics, and fingerprints can be used to identify individuals. It also mentions other means, which opens the article up to more biometric data. Article 175 states that the court may issue an order to obtain DNA from a defendant or other individual in order to identify someone. In Colombia, the 2004 Criminal Procedure Code mentions biometric data. The change incorporating this occurred during the decade under study. Article 245, which was added in 2018, refers to DNA tests of the defendant or suspect. It states that these and other data that allow individuals to be identified, such as fingerprints, require an express order from the prosecutor. Article 251 on identification methods is more specific, mentioning genetic profiles or morphological characteristics such as fingerprints.

Ecuador's 2014 Comprehensive Organic Criminal Code refers to genetic data as part of sampling as follows: "The procurement of samples of bodily fluids and organic and genetic-molecular components." (Our translation.)

---

21 Díaz, M. (2018). El cuerpo como dato. See: https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf

In regard to identity verification, Article 55.2 of Uruguay's 2015 Criminal Procedure Code establishes that if the person does not have the documents necessary to identify them, they may authorize officials in writing to fingerprint them. Those fingerprints may only be used to identify them. Article 195 of the 2012 Organic Criminal Procedure Code in Venezuela mentions physical and mental examination of the defendant in general terms but does not provide examples or specific cases.

The first regional trend that emerges is that there are no bodies of rules focused specifically on regulating the collection and use of biometric data. As such, the articles that address this point are contained in other types of laws. Where changes have been made, the use of technologies is addressed as an ancillary aspect that is subject to other forms of oversight. The daily use of biometrics by surveillance agencies is excluded.

The biometric data that were identified in the largest number of codes were fingerprints. During the decade under study, fingerprints were included in regulations in Uruguay, El Salvador, Argentina, and Colombia. As we have seen, the cases involve identity checks and identification. This aligns with the definition of biometric data provided in the introduction, which establishes that they can be used to identify individuals. Each person's fingerprints are unique, which means that they can be used to accurately identify the subject under investigation with 100% certainty. It is important to note Uruguay's rule, which establishes that these biometric data can only be used for identification purposes.

In closing, in this study we did not find any body of regulations or rule on automated facial recognition technologies. Despite the growing trend to use surveillance systems with those capacities in public spaces and the unique risk that facial recognition poses in that sense,[22] only constitutional rules and legal rules on personal data and the powers of public officials could be used to regulate or control such applications.

22 See, for example, https://www.reconocimientofacial.info.

Summary of findings

If there is one thing that stands out in this study, it is the updating of certain regulatory bodies. The dates of issue of the Criminal Procedure Codes and personal data protection laws are noteworthy, as most fall within the decade under study. Legislation updates are also present in other types of special laws (such as those addressing telecommunications or organized crime), but to a lesser extent. The two types of laws that tend to be updated are of utmost importance in that they directly affect the personal data, surveillance and, to a lesser extent, communications sections. Unfortunately, there are fewer regulations on biometric data.

In regard to personal data, what stands out the most is that the majority of the countries in the region have special laws on the topic and approximately one third of those that do not regulate this area specifically are in the process of doing so. Seventy-seven percent of the Latin American countries that currently have data protection laws passed them during the decade under study. Finally, there are incipient trends to consider personal data protection as an autonomous right separate from privacy or intimacy. At the judicial level, there is a tendency to hear cases related to the right to be forgotten.

In regard to surveillance and intelligence activities and the laws passed between 2010 and 2020, 58% of Latin American countries have a law on communications interception that dates back to this decade, 47% have laws on their recording and two countries contemplate intervention in computer systems, both of which were issued in the same period. The majority of these measures are regulated in each country's criminal procedure legislation. A minority of them are special laws/regulations on communications surveillance, intelligence laws and organized crime. Of the 17 countries with rules on these matters, 12 have updated their legislation during the decade under study. On average, around 50% of the countries of the region regulated the first two measures between 2010 and 2020, while computer system intervention is an incipient trend in the intelligence laws from this decade.

In regard to crimes against intimacy, while laws or bills that punish acts that constitute the crime of dissemination of intimate material without consent are an incipient trend from the second half of the decade, various Criminal Codes have penalized the dissemination or release of sexual content or images as a broader category of crimes that could contain it. Another important crime is unauthorized access to data, which is subject to law in half of Latin America in both Criminal Codes and computer crime laws.

In regard to rules on retention of personal data or rules requiring telephone identity records, the trend from 2010 to 2020 in Latin America on the imposition of prepaid telephone service registration is seen in 42% of the 19 countries analyzed. Similarly, 16% of these countries

register SIM cards. Both measures are mainly justified by efforts to fight crime. On the other hand, 37% of the countries of the region have rules on telephone or digital communication records measures. Of these nine countries, five expressly mention online communications.

Finally, we study rules on biometrics. First, it is worth noting that the majority of the laws that cover this area were updated between 2010 and 2020. As such, 59% of the Criminal Procedure Codes contain dispositions on the topic that went into effect or were changed during that period. As a general point, 19 countries were analyzed, and it was found that 16 include rules on biometric data in their legislation. Specifically, the most regulated type of biometric data is the fingerprint (21%). A minority of countries regulate DNA tests (16%).

Identifying challenges

Personal data protection:

Given that only five of the 19 countries in the study recognize personal data protection as an autonomous right, the first challenge consists of the countries consecrating it, ideally at the constitutional level, in order to elevate it to the apex of each country's legal systems.

While judicial action is key for the effective protection of this right, an institutional structure meant to protect personal data must be installed. While it goes beyond the scope of this study, having an oversight authority with the power to impose penalties would strengthen enforceability and compliance with regulatory provisions given that they are not very effective if they only exist on paper.

As we have seen, several countries fully or partially recognize ARCO rights. We suggest that all of these rights be adopted, and that each country's inhabitants have easy-to-use channels for exercising them, such as an online form on the website of the corresponding state agency.

Considering the interconnectedness of these countries and the region's growing ability to attract large corporations, cross-border transfer of data must be regulated given that in many industries (such as pharmaceuticals, finances, and technology) manage a large volume of personal information. The strengthening of standards and regulations related to this flow are of economic and social interest, and an effort must always be made to require equal or greater guarantees in the handling of them that exist in each country.

Surveillance and intelligence:

It is important to consider that 29% of regional regulations were enacted prior to 2010. As such, the first necessary step involves updating legislation. As we have seen, one challenge is the drafting and updating of laws other than the Criminal Procedure Code. Criminal prosecution of organized crime and crimes covered under intelligence laws involve strong criminal investigation. Some countries' intelligence laws establish a series of special highly intrusive evidentiary procedures, but they are also subject to strict conditions. In view of this, each country must have provisions regarding this type of measure in special criminal prosecution laws that could interfere with individuals' right to privacy, establishing detailed requirements and guarantees in cases in which they must be used.

One regional trend is the consecration of communications intervention in general terms, but not the establishment of a rule or special law focused on this specific investigative mea-

sure. We believe that each country faces the challenge of developing a separate rule that complements the measure mainly set out in Criminal Procedure Codes, again, establishing more requirements and conditions of security and protection of the rights of the individual investigated.

Crimes against intimacy

During the second half of the decade, there was a positive trend to criminalize dissemination of intimate material without consent either through laws (such as those enacted in Mexico) or through legislation (as seen in Chile). Given that the discussion was launched by female activists impacted by this conduct in countries like Colombia and Mexico, one can observe a regional trend favoring the fight against this form of violence. However, it is possible to think that there is silence around these situations in other countries in the region, so one future challenge involves passing laws to categorize these actions as a crime and punish those who commit them. It is interesting to consider the case of Colombia, where being a female victim of this crime was established as an aggravating factor.

Some countries criminalize unauthorized access to databases, and this practice should be extended throughout the region. It is also necessary to establish strict security measures that support the defense of each individual's data.

Retention of personal data and identity records in telephony:

There are arguments in favor of considering prepaid service and SIM card registration. However, if that is done, robust security measures must be established to protect these data along with channels for updating them and an efficient way to report and block these devices. The registration measure itself can create incentives for creating a black market of stolen equipment or for stealing them to commit crimes. As such, it is a challenge to bring together all of these elements in cases in which the countries find registration measures necessary. When they are created, positive and negative factors must be analyzed considering efforts to fight crime and the disadvantages that these measures may generate.

In regard to recording communications, each country's laws must be updated to incorporate digital communications. Few countries regulate it. They must also establish high security standards for gathering and storing this information.

Biometrics:

The countries included in this study must provide more detailed regulations in this area beyond the gathering of biological samples, which is broadly covered in Latin American criminal procedure legislation. As we have seen, the specific regulated biometric data that

we identified as a trend are fingerprints and DNA tests. These are increasingly being used in ways that go beyond the specific regulations and this seems to be covered by general rules on protection of sensitive personal data. Not all countries regulate these uses, so a first step should involve expanding their regulation throughout the region under study. There are also other types of biometric data that are captured and used such as face or eye scans. These are broadly used to unlock doors, for example. Latin American countries must regulate this situation promptly in a manner that is respectful of people's rights.


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina