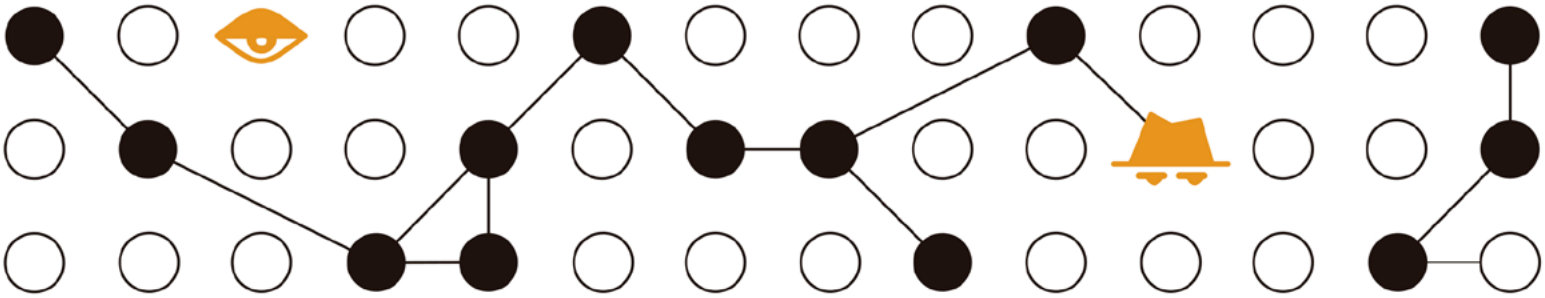

IS DATA RETENTION LEGITIMATE IN COLOMBIA?

COMPARATIVE ANALYSIS OF A MASS SURVEILLANCE TOOL THAT RESTRICTS HUMAN RIGHTS

KARISMA FOUNDATION

By Juan Diego Castañeda

Elaborate by:
Karisma Foundation
karisma.org.co

With the support of Privacy International

PRIVACY INTERNATIONAL

Fundación Karisma
www.karisma.org.co

January 2016

Karisma Foundation, in a continuing effort to make its documents more accesible -that it, in a format that allow the content to be read by as many people as possible, regardless of their disability or context of use— linked the bibliographical sources in the content itself, the bibliographical Sources utilized can be found in the references section.

Check this analysis on-line at

https://karisma.org.co/es-legitima-la-r…atos-en-colombia/

Index

Introduction

Concerns for national security and for the surge of criminal activity online have become a justification for law enforcement surveillance of information and communication technologies (ICTs). However, not every intelligence activity by States is legal or legitimate. It behooves us to analyze new surveillance techniques and to review the legal frameworks in each country to insure that they are aligned with human rights.

Communications surveillance by States aims to gather data for intelligence or criminal investigation. This process involves the collection, storage, processing and circulation of data, and employs a number of techniques. The most common techniques are communications interception, data retention, and the use of hacking tools (e.g. penetration testing and exploiting security vulnerabilities). However, without a democratic process in shaping surveillance capacity building and in the establishment of review and transparency measures, these techniques can be used illegally, and can cause serious human rights violations, compromising the very basis of democracy[1].

This document analyzes Colombian regulations regarding data retention, and compares them with those in Peru, Mexico and Brazil from the perspective of compliance with international standards for establishing measures that restrict fundamental rights, especially freedom of expression and privacy. Given the specifics of the Argentinean case, an overall comparison will be omitted, but specific comparisons will be used when appropriate.

The main purpose of this document is to review the scope of human rights protections in the framework of Colombian data protection measures as compared to their equivalents in the region, and to the relevant standards in the Inter-American Human Rights System. For the latter, the main source was the 2013 report by the Special Rapporteur on Freedom of Expression at the OAS Inter American Commission on Hu-

man Rights. The core question is: Is the Colombian legal framework for data retention one that guarantees human rights within the regional context?

The following reports, coordinated by Katitza Rodríguez, were the main sources used in researching the legal frameworks in each country.

Peru: *Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú* (Octubre, 2015) by Miguel Morachimo.

Mexico: *Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en México* (Oct, 2015) by Luis Fernando García.

Brazil: *State Surveillance of Communications in Brazil and the Protection of Fundamental Rights* (Sept, 2015) by Dennys Antonialli and Jacqueline de Souza Abreu.

Colombia: *Vigilancia de las comunicaciones por la autoridad y protección de los derechos fundamentales en Colombia* (May, 2015) by Juan Camilo Rivera and Katitza Rodríguez.

Argentina: *Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Argentina* (Oct, 2015) by Verónica Ferrari and Daniela Schnidrig.

What makes a human rights restriction legitimate?

According to the Special Rapporteur on Freedom of Expression at the Inter-American Human Rights Commission, measures that affect communications, insofar as they restrict fundamental rights, must be in accordance with the standards and principles set forth on several international documents, and States must review and harmonize their rules to insure that this is the case.

According to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, it is understood that, despite the fact that article 17 of the International Covenant on Civil and Political Rights doesn't specify the conditions that must be met by limitations on the right to privacy, it is clear that any such limitation must comply with the guarantees established for other rights. Thus, admissible limitations to privacy (a) must be legal, (b) must not compromise the essence of the human right, (c) must be necessary in a democracy, (d) must not be discretional, (e) must be necessary for a legitimate aim, and (f) must be proportional, adequate, cause the least harm, and be proportional to the protected interest.

The OAS Rapporteur on Freedom of Expression, commenting on the use of products and services of the Italian company Hacking Team by governments around the world,[2] stated that:

> According to international standards, the use of systems for eavesdropping private communications must be clearly and precisely established in the law, must be truly exceptional and selective, and must be limited in scope to what is strictly necessary to advance imperative goals, such as investigating serious crimes established in the law[3].

Finally, one must take into account the *International Principles on the Application of Human Rights to Communications Surveillance,* developed from deliberations on inter-

national human rights law in the digital environment[4] led by a number of civil society organizations, with the participation of industry representatives and subject matter experts. The principles that must guide the application communications surveillance measures are: legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority, due process, user notification, transparency, public oversight, integrity of communication and systems, safeguards for international cooperation, and guarantees against illegitimate access and right to effective remedy.

This document will be guided by the requirements outlined by the Inter-American Commission on Human Rights Special Rapporteur for Freedom of Expression, which states that a communications surveillance measure is legitimate if:[5]

1. It is established in a law
2. It pursues a legitimate aim
3. It is necessary, adequate, and proportional to the objective pursued.
4. It respects due process and judicial review

Below, we shall explain why data retention is a measure that restricts fundamental rights, and we shall examine the Colombian law in light of each of these requirements.

What is data retention an why is it a restriction of fundamental rights?

Our most personal information, a reflection of our life and our very thoughts, no longer remains exclusively in our private sphere. Now, personal information is also found in databases, built for different purposes and administered by entities both public and private. These databases are fed by constant flows of information. Together, they make up a file about each individual, a "personal dossier".[6] The digital technology on which modern life depends, produces and records constant flows of data. Computers register the time they are turned on, the applications they use, the webpages they visit, and the location from which they are used. Cell phones are constantly aware of their location, and they register incoming and outgoing calls, text messages, and photos. The strength of these data lies in their combination: an analysis based on cross referencing various databases can reveal enough about a person to constitute a violation of their rights. However, this is all part of a sort of concession made by users in exchange for services. The result, in terms of the type of data we produce and those who administer it, is that we become "an open book for governments and corporations"[7]. Therefore, it is necessary to insure respect of those human rights that may be affected by these flows and by the uses of this information.

Telecommunications services is one of the areas that produces the most data. Gradually, more and more governments are forcing service providers to retain these data and to hand them over for various purposes. Governments' interest in this point lies mainly in the fact that users depend on telecommunications companies on two levels: (1) on the service provision itself, and (2) on the safeguarding of data that flow through the connection[8]. Retention obligations determine the data that must be maintained about connections made with landline telephones, cellphones, and the internet, establishing the type of data that operators must keep, the time it must be retained for, under what conditions, and who is authorized to access such data.

Data gathered are, for example, the number that receives the call, the call's duration, the geographical location of the device, and its unique identifiers (IMEI and IMSI) in mobile or land lines, as well as IP internet connections. That is, simply, different from gathering communication contents, and have therefore been called "metadata", that is, data about the data communicated. This classification can make us erroneously conclude that metadata or subscriber identification data, deserves lesser protection than that granted to the communication contents itself.[9] Data aggregation can in fact be more revealing than the content of such communication[10]. For this reason, it has been established that data retention is a measure that restricts and affects the rights to privacy and freedom of expression[11].

Below, we shall explain the requirements of (1) legality, (2) legitimate aim, (3) necessity, adequacy and proportionality, and (4) judicial review and due process. For each, we will analyze the Colombian regulation and compare it with data retention in Peru, Mexico, and Brazil.

I. Legality

Any restriction of the right to privacy or freedom of expression, such as that entailed by mandatory retention of telecommunications data must (1) be prescribed by law in the formal and material sense, and (2) must be clear and precise[12].

Law in the formal and material sense

On the first point, it is clear that the requirement is only met when the restriction is imposed by means of a regulation established by the democratically elected legislative body, and in accordance with the procedure provided in the respective constitution. An administrative provision would not satisfy the requirement.

In the legal systems studied, we find a mix of regulations and laws in the material sense that apply to various aspects of data retention.

In Colombia, data retention is established in two such places:

1. Decree No. 1704 of 2012, dealing with data retention for criminal investigations.

2. Law No. 1621 of 2013, dealing with data retention for intelligence activities.

In this sense, Colombia is no different from the other countries studied, since it unfortunately combines laws in the formal and material sense with decrees and other regulations.

Peru: Law No. 27.336 (2002) regulates the retention of source records of call details and billing. Legislative Decree No. 1182 (2015) regulates the retention of traffic data,

and the identification and location of terminals. The Criminal Procedural Code (Legislative Decree No. 957 of 2004) regulates access to device geolocation by the investigative body.

Brazil: Brazil has two administrative resolutions that regulate data retention for landline telephones (Resolution No. 426/05 of ANATEL) and mobile devices (Resolution No. 477/07 of the same organ), Law No. 12.850 on data retention and access in both telephony modalities, and Law No. 12.965 or Internet Civil Framework, on Internet traffic data access and retention.

Mexico: This country is an exception in this regard, since the retention regime is entirely etched into law in the formal and material sense through the Federal Telecommunications and Radio Broadcast Law (2014) and the National Criminal Procedure Code (CNPP), which substitutes the Federal Criminal Procedure Code (CFPP).

Argentina: Two things bare mentioning in this point: First, that this country has no explicit legal basis for data retention. Nonetheless, the Telecommunications Services Quality Regulation, issued by the Communications Secretary -the Federal Authority in charge of Information and Communications technology- mandates that providers make available to the authorities all information they deem relevant for quality assessment[13]. Article 8 of said regulation mandates the retention of data gathered by providers that may help assess service quality.

The second is that the only case in which data retention for criminal investigation purposes was ruled unconstitutional. Law No. 25.873 and its regulatory decree No. 1563 of 2004 mandate telecommunications services providers to "record and systematize affiliation and domicile data for users and customers, and traffic records for communications directed through them" for a period of 10 years and for access by Judicial authorities or the Public Ministry. These rules were deemed unconstitutional by the National Appeals Court for Contested Administrative Procedure for violating the requirements of legality, necessity and proportionality.

The Court considered inadmissible the vagueness of an appeal to the common interest in support of the rules in question, given the degree to which they would affect citizens' interests[14]. Regarding the legality requirement, it opined that it isn't clear what are traffic data, and therefore they could be confused with the content of communication. Moreover, it determined that it wasn't clear which authorities, and under what conditions, would have access to the data. It made clear that access to data would require judicial authorization.

It also made a statement regarding the proportionality of the measure and said that "there is no doubt that the rule in question places under suspicion every telecommunications services user for the very long period of 10 years," which is all the more

serious in the case of digital communications since "all movements are recorded." therein. It also pointed out that the measure was not admissible since, even though not all procedures could merit its use, it isn't clear which judicial procedures it was authorized for.

Clarity

As part of the legality requirement, data retention regimes should be clear regarding the type of data affected by the measure and the time during which they shall be retained. Colombia, for the case of criminal investigation, mandates telecommunications service providers to retain subscriber information and device location data in real time[15]. In the case of intelligence activities, it requires the retention of "communications activity histories for telephone subscribers, technical identification data for subscribers subject to the operation" as well as location data[16].

The meaning of "communications history" is unclear, as is the scope of the general clauses employed in these rules (e.g., "among others", or "any other information"). Regarding the time, in both cases data must be retained for a period of 5 years, even though it isn't clear whether location data must be recorded for later consultation.

For the remaining countries there are also serious lapses in clarity. For example, in Peru, the meaning of "data derived from telecommunications" isn't clear[17], and neither is the exact nature of location data[18]. In Brazil, there is a vague requirement for the retention of "all data relevant to service provision, including billing data[19]." Mexico, on the other hand, makes an exhaustive list of which data are subject to retention, from subscriber information to the start and end times of communications, and the numbers involved[20].

On the other hand, Colombia also doesn't make clear whether data retention obligations also apply to internet traffic data, since, although the relevant articles -Decree 1704 and Law 1621- are directed at "telecommunications networks and services providers" or "telecommunications services operators", the data alluded to seems to be related to mobile or landline telephony.

Brazil has perhaps the clearest legislation in this regard, since it has specific regulations or legislation for each communication channel, namely landline telephony, mobile, and internet.

Facts and authorities

The legality requirement demands that a measure that restricts fundamental rights, such as data retention, be clear regarding the circumstances that merit the collection of, or access to the data, the authorities enabled to access the data, the conditions

that must be verified before accessing the data, and the authorities responsible for reviewing such verification.

In Colombia, in regard to criminal investigation, any investigation merits access to retained data. The order to hand over the data must come from the National Prosecutor General, and its execution is in the hands of the designated "Judicial Police group"[21]. For intelligence activities, the only restriction imposed by the rule is the existence of an "authorized operation", although there is no way to determine what facts merit the conduction of an intelligence operation, nor who can provide such authorization. Moreover, with such an ambiguous rule, there is a good number of authorities that could legitimately request this information, being members of the intelligence community[22].

Mexico is another bad example in terms of which authorities can access data. The Federal Telecommunications and Radio Broadcast Law (Article 189) has a general clause according to which "providers of applications and content services are mandated to comply with any founded and supported written request, in the terms established by law." Both traffic and location data must be handed, according to the LFTR, to the vaguely defined "competent authorities", including "security and justice authorities", as stated in article 189 (section III of article 190, first subsection).

Specifically, the Federal Criminal Procedure Code (Art. 133c.) determines that the Prosecutor General of the Republic may request access to geolocation data in real time when investigating organized crime, crimes against health, kidnapping, extortion, or threats. However, the National Criminal Procedure Code (Art. 291), which will replace the CFNP, leaves open the possibility that any investigation makes use of location data.

Brazil has the same problems, even with respect to internet data: the Civil Internet Framework doesn't specify which authorities can access the retained information. On the one hand, it states (article 10, paragraph 3) that "administrative authorities with legal mandate" may access subscriber information. On the other hand, article 22 establishes that access to connection records and internet applications shall be authorized to "the interested party" as part of evidence gathering for civil or criminal investigations.

With respect to the reasons and conditions for accessing data, Peru is more specific than other countries regarding cell-phone geolocation data. The regulations determine that a specialized Police unit in charge of data requests may access these data when the following conditions apply[23]: (1) in the case of *flagrante delicto*, (2) when the crime under investigation is subject to penalty above four years of imprisonment, and (3) when access to the data constitutes a necessary means for the investigation. The Prosecutor, on its part, may access geolocation data when it investigates the possible

commission of an act punishable by a term of imprisonment above four years, and under the conviction of absolute necessity[24].

II. Compelling objectives

The second requirement that must be met by any measure that is restrictive of fundamental rights is that it is employed to achieve compelling objectives authorized by the American Convention. These objectives are: (1) protection of the rights of others, (2) national security, (3) public order (4) public health, and (5) morals. The interpretation of these aims must be in accordance with the principles of a democratic society. That is, States cannot interpret them freely[25].

Protecting the rights of others entails the existence of a clear threat, and requires that the measure is not imposed to protect the same rights it affects. Similarly, less restrictive measures must be employed before affecting any rights[26].

Maintaining public order, understood as ""the conditions that assure the normal and harmonious functioning of institutions based on a coherent system of values and principles", requires the existence of demonstrably "real and objectively verifiable causes that present the certain and credible threat of a potentially serious disturbance of the basic conditions for the functioning of democratic institutions". Therefore, justifications based on hypothetical facts or situations, or on threats lacking the necessary degree of seriousness are not acceptable[27].

National security, in turn, must not be defined in terms that are incompatible with a democratic society. For example, in a way that justifies attacks on political dissidents, journalists, or human rights defenders with political objectives or to hamper their work. The criteria for considering that a case merits application must be clearly defined[28].

Analyzing the legality requirement leads us to the conclusion that the jurisdictions studied, including Colombia, don't fully meet the compelling objective requirement for imposing data retention measures. For example, regulations in Brazil (resolutions no. 426/05 and 477/07) and Peru (Law No. 27.336) impose the measure for telecommunications services providers, and guarantee access to these data for security bodies. The Mexican legislation simply orders data retention within the framework of a law that regulates the telecommunications sector more broadly, without specific reference to the reasons for retention.

Although the Colombian legislation imposes retention and guarantees access to data only as part of a criminal investigation or intelligence activities, it is far from determining clearly the national security or public order threat that the measure could mitigate. Intelligence agencies may access retained data by means of general clauses,

which in practice entails the imposition of restrictions with objectives that are neither compelling nor urgent, and thus the violation of the legality principle. Therefore, there is no certainty about the scope of the facts that justify the measure. Mexico stands out for having a list of what it considers threats to national security in its National Security Law (Art. 5).

The following requirement deals with the necessity, adequacy and proportionality of a measure *in order to achieve its compelling objectives*. For this reason, if the connection between the measure and the objectives is not sufficient, as is the case in the legislations analyzed, it will be very difficult to affirm that the measure is necessary, adequate and proportional.

III. Necessity, adequacy and proportionality

The third requirement that must be met by a measure that restricts fundamental rights to be considered legitimate is that it can demonstrate necessity, adequacy and proportionality.

The necessity of a rights restriction must be certain and urgent, which imposes a burden beyond it being useful, reasonable, or timely for achieving compelling objectives. Besides, the measure must be limited to what is essential to achieve the objective, meaning that the imposition of less restrictive measures must be considered. Therefore, the measure must only be authorized for exceptional cases[29].

Data retention, by its very nature, and as it appears on the legislations studied, is a measure that affects the rights to privacy and freedom of expression, among others, and operates constantly on communications services users' data. The passive nature of this measure precludes completely the necessity requirement, since it doesn't limit its operation to exceptional cases. On the other hand, the vagueness of rules governing access to retained data doesn't reassure us that the measure is used in exceptional cases only. In Colombia, law enforcement agencies may access all retained data in the course of an investigation for any crime, as can intelligence agencies in any situation they consider necessary. The same will occur in Mexico when the new National Criminal Procedure Code enters into effect. In Peru and Brazil, the general clauses on cooperation with intelligence agencies don't specify which exceptional cases would warrant the use of the measure.

The adequacy requirement seeks that the measure is "effectively conducive to attaining the legitimate and compelling objectives in question[30]". As is clear from this analysis, the lack of precision in the terms referred to in the measure, and the lack of a strong connection between the measure and compelling objectives, make it impossible to determine its adequacy.

Proportionality derives from evaluating (1) the degree of affectation of rights entailed by the measure, (2) the importance of satisfying the right protected by the measure, and (3) whether such satisfaction justifies the restriction of other rights[31]. The application of communications surveillance measures should be authorized only in the presence of certain risk against protected rights (such as security), and when society's interest in maintaining these rights is higher than that of maintaining the rights that are affected[32].

Establishing the proportionality of the measure in each legislation in the abstract is difficult, since it requires the evaluation of particular social, cultural and legal contexts. However, one must take into account the fact that these legislations call for the retention of some or all of the following data: information about the subscriber, traffic data for landline, mobile, and internet communications, and the location of terminals; also, that a broad range of authorities may have access to them, and that the reasons for such access aren't clear. Moreover, the time for such retention appears to be arbitrary. In Colombia, the only mention of such period establishes 5 years, which leads us to conclude that it refers to any type of data. Peru establishes 3 years, whereas Mexico establishes 2 years. In Brazil, mobile or landline telephone data must be retained for 5 years, and Internet data for 1 year.

For the moment, only in Brazil is there a debate before the courts on the legality and proportionality of the retention measure imposed by Law No. 12,850 on organized crime, since, according to the plaintiffs, the need for judicial authorization for accessing traffic data isn't clear, and the authorities take advantage of this to demand all types of data retained by operators.

Arguments with which the E.U. Court of Justice ruled invalid Directive 2006/24/EC on data retention are relevant here, since they point to many of the problems found with the retention regimes analyzed[33]. On the proportionality of the measure, the ruling points out that the target population turns out to be any person who makes use of communication media, namely the entire European population. In this context, the Court finds that there are no limits to the application of the measure in function of the objective pursued. In particular, there is no limit to geographic areas, persons, or types of communication subject to the measure in relation to the objective pursued or the gravity of the events under investigation.

Discounting the legitimacy of data retention for the purposes of oversight of telecommunications services providers (Peru and Brazil) or for indeterminate purposes (Mexico), we found no adequate limits on this measure when employed in criminal investigation and to provide information to intelligence agencies. There is no limit regarding which persons can be affected, or for how long. In Colombia, there is no limit on the types of crimes whose investigation can be aided by retained data.

Under these conditions, the proportionality of data retention is clearly put into question, since society's interest in investigating crime, on its own, doesn't justify affecting to such degree the right to privacy and freedom of expression of the persons to whom it is applied. To this, one must add that the effectiveness of data retention lies, if anywhere, in facilitating the investigation of past events, but little can it do to prevent the commission of future crimes[34].

IV. Due process and judicial review

To be legitimate, a restriction of rights must respect "guarantees pertaining due process and judicial review[35]." This comprises, in general, the possibility of judicial authorization and control, notification to the user affected by the measure, and the submission of transparency reports on the use of the measure.

Judicial review

Data retention rules should be clear regarding the conditions that warrant access to retained data, and the authorities that may do so. When these requirements are met, it is the judicial authorities who shall decide whether the measure is: adequate to achieve the objective, sufficiently restrictive so as not to infringe upon rights beyond what is necessary, and proportional with respect to the interest being defended[36]. In short, it is the judicial authorities who shall insure that the application of restrictive measures occurs within the constitutional and democratic framework.

As opposed to communications interception, data retention is automatic and covers the entire population. Therefore, the activity of data collection itself requires no prior judicial review of its necessity and proportionality. Judicial review of access to retained data, or to geolocation data varies between countries.

In contrast with other countries, access to retained data or device geolocation requires no judicial authorization in Colombia. It is also not subject to subsequent judicial review, neither in the context of criminal investigation, nor for intelligence activities. In Mexico, similarly to what happens in Colombia, access to retained traffic data in as determined by the LFTR, and to geolocation data (Federal Criminal Procedural Code) requires no judicial authorization. The National Criminal Procedural Code will require authorization to access geolocation data.

On the other hand, Peru does require that the Police request judicial authorization to access retained traffic data (Second final complementary provision of Decree No. 1182), and geolocation data (Decree No. 1182. Article 5). The same applies to Intelligence agencies (article 32 of Decree No. 1141).

Legislation in Brazil, although it isn't clear regarding what must be done with telephone data, establishes that access to internet connection and application data shall

be authorized by a judge only for criminal or civil investigations when there is (1) good indication of guilt, (2) justification of the usefulness of the records for the investigation, and (3) a specification of the period for which the records are requested[37].

Notification to the user

This requirement also includes due process guarantees so that persons affected by the measure can defend themselves adequately[38]. Therefore, notifying the user is an essential part of their defense, since otherwise they may not know they have been monitored, and thus submit adequate appeals to mitigate the effects of such surveillance.

The only country that provides for user notification in one case is Peru, specifically for cases of access to location data through the procedure established on article 230 of the Criminal Procedural Code. Such notification is to be conducted after the measure has been applied, and only "if the investigation's objective permits it, and as long as it doesn't jeopardize the life and health of others", which shall be determined by the corresponding judge (Art. 231). However, this procedure is not established in Decree No. 1182 nor in Law No.27.336.

Transparency

In order for surveillance activities by States to be transparent, and for citizens to be able to exert proper review, it is required that States disclose "general information on the number of requests for interception and surveillance that have been approved and rejected, and should include as much information as possible, such as—for example—a breakdown of requests by service provider, type of investigation, time period covered by the investigations, etc.[39]". Likewise, service providers should publish reports that specify the procedures they follow upon receiving a request from the authorities, as well as the type and number of requests[40].

Mexico is the only country that provides for the publication of transparency reports. Article 70 XLVIII of the General Transparency and Access to Public Information Law mandates authorities to publish a list of requests made to Internet service and application providers regarding communications interception, data registry and geolocation. The report must contain: the aim of the investigation, the time scale, its legal foundation, and the existence of judicial authorization when relevant.

Service providers could be mandated to present a six-monthly report on access requests for traffic and geolocation data, specifying the number of requests received, accepted, and rejected. This will be the case if the fourteenth guideline of the Draft "Guidelines for cooperation in matters of security and justice" presented by the Federal Telecommunications Institute is applied, in accordance with the mandate granted by article 190 of the LFTR.

Conclusions

Judging by international standards for the protection of human rights for communications surveillance, the data retention regimes studied in this document are illegitimate. This is true for Colombia as well as the other countries mentioned.

In the first place, most regimes are set down in a mix of laws and decrees, for which data retention hasn't always been subject to discussion in the various legislatures. As for its legality, the Colombian legislation uses particularly ambiguous terms regarding the authorities that can access retained data. Then main problem, however, isn't legality, since it may well be that a law that violates fundamental rights is approved. The problem lies in the lack of legitimate aims, thus making data retention neither necessary nor proportionate. With the exception of Mexico, no country defines what is national security, which is the objective pursued when data retention is used as a tool for intelligence work. Colombia, as with other countries, simply names this objective without explaining or limiting its scope. Therefore, if the objective sought by the measure is not legitimate, we cannot speak of necessity and proportionality, since these requirements only exist in relation to such objective. By its very nature, a blanket order to retain data is automatic, and doesn't undergo judicial review, and thus it cannot meet the international standards mentioned here. This situation, in conjunction with the lack of user notification and the scant implementation of transparency obligations, means that the use of data retention is still in the shadows, and therefore the public has little information to determine the usefulness of such measure.

Data retention must be one of the most broadly used surveillance techniques in the region, or at least one of the first tools used by the authorities, judging by the way in which legislation to legalize it has become widespread. Of the 5 countries studied, 4 have legislated this technique, and these aren't the only legislations of this type in the region. Countries such as Honduras and Chile also have data retention rules, and a detailed analysis would certainly unveil many more.

However, the existence of legislation that regulates the use of data retention is, on its own, no guarantee of the protection of human rights. Legislation of this type must meet a series of conditions to make the practice legitimate. None of the legislations we saw passes muster under such analysis. Data retention law in Peru, Colombia, Mexico and Brazil are too permissive, too broad, and provide so few guarantees that it isn't possible to rely on them as a legal framework for the protection and respect of their citizens' human rights, as we've attempted to show in this document. On the other hand, the Argentinean legislation was ruled unconstitutional, precisely after it was established that it wasn't clear nor proportional.

It is concerning that, in terms of surveillance techniques, preference is given to a strictly instrumental vision of technology, that pays no heed to its true potential usefulness. If an assessment of this type were done, the residual nature of data retention, as compared to more targeted and less invasive techniques, would become evident. The legal framework offered by the IAHRC and other analyses, such as the *International Principles on the Application of Human Rights to Communications Surveillance* should help promote legislations that offer true guarantees to the citizenry, while improving the legal certainty on which authorities must rely to perform their work.

It would be advisable for Colombia and the remaining countries to demonstrate their strong commitment to the protection of human rights and to dismantle the current data retention regime. The European Union and Argentina have shown that data retention is a mass surveillance measure that places the entire citizenry under suspicion, and that affects the privacy of their communication, making it neither necessary nor proportionate to defend objectives such as national security, nor the interests of criminal procedures. If sectors of society or the government consider that data retention can be established without violating fundamental rights, a debate should take place to discuss each of the aspects highlighted here as shortcomings of this practice. Until then, data retention as practiced today must be considered an illegitimate citizen surveillance measure.

Notes

1. IAHRC (2013). *Libertad de expresión e internet*. OEA/Ser.L/V/II.149 Doc.50, Chapter IV, par. 154.
2. Castañeda, J. (2025). When the State hacks. Retrieved from: https://karisma.org.co/wp-content/uploads/2015/12/When-the-State-hackea-D.pdf
3. OAS Inter-American Human Rights Commission Special Rapporteur for Freedom of Expression (July 21, 2015). Press release on the acquisition and implementation of surveillance programs by Governments in the hemisphere. Retrieved from http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&lID=2.
4. *International Principles on the Application of Human Rights to Communications Surveillance*. Retrievedfrom https://es.necessaryandproportionate.org/text.
5. CIDH (2013). *Libertad de expresión e internet*. OEA/Ser.L/V/II.149 Doc.50, Chapter IV, parag. 55.
6. Solove, D.J. (2004). *The digital person technology and privacy in the information age*. New York, U.S.: New York University Press.
7. Schneier, B. (2015). Data and Goliath: the hidden battles to collect your data and control your world. New York, U.S.: W. W. Norton.
8. Kerr, I.R., Gilbert, D. & McGill, J. (2006). The medium and the message: personal privacy and the forced marriage of police and telecommunications providers. *Criminal Law Quarterly*, 51(4).
9. Electronic Frontier Foundation & American Civil Liberties Union Brief *Amicus Curiae* en Kalyman v. Obama, August 20, 2014. Available at https://www.eff.org/document/eff-and-aclu-amicus-brief-klayman.
10. UN High Commissioner for Human Rights Report (2014). *The right to privacy inthe digital age*. A/HRC/27/37, par. 19.

11. United Nations General Assembly. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. A/HRC/23/40, par. 148
12. *Supra* (note 1), Chapter IV, par. 58.
13. Federal Planning, Public Investment, and Services Ministry (July 1, 2013). Resolution No. 5. Retrieved from http://infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/216915/norma.htm.
14. National Appeals Chamber for Contested Administrative Federal Procedure (November 29, 2005). *Halabi v. The National State*.
15. Decree No. 1704 of 2012, articles 4 and 5.
16. Law No. 1621 of 2013, article 44.
17. Law No. 27.336 (2002)
18. Legislative Decree No.1182, first and second final complementary provisions.
19. Resolution No. 426 of 2005, article 22.
20. Federal Telecommunications and Radio Broadcast Law (LFTR for its acronym in Spanish), Article 190 III.
21. Decree No. 1704 of 2012, articles 4 and 5.
22. In Colombia, the following are intelligence agencies: the National Intelligence Directorate, the Financial Information and Analysis Unit, the Police Intelligence Directorate, and the corresponding Chiefs of Staff of the Armed Forces: the National Army, the National Navy, and the Air Force. *See* Decree No. 857 of 2014.
23. Legislative Decree No. 1182. Articles 3 and 4.
24. Criminal Procedural Code, article 230, sections 1 and 4.
25. CIDH, *op. cit.* (note 1), Chapter IV, par. 157; CIDH (2009). *Annual Report of the Special Rapporteur for Freedom of Expression.* OEA/Ser.L/V/II Doc.51, Chapter III, par. 76.
26. *Supra*, Chapter III, par.77-80.
27. *Supra*, Chapter III, par. 81-83.
28. *Supra* (note 1), Chapter IV, par. 60 and 157.
29. *Supra* (note 39), Chapter III, par. 85-87 & *Supra* (note 1), Chapter IV, par. 64, 160 and 162.
30. *Supra* (note 39), Chapter III, par. 88.
31. *Supra* (note 1), Chapter IV, par. 90.

32. UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and OAS IHRC Special rapporteur for freedom of expression (June 21, 2013). *Joint statement on surveillance programs and their impact of freedom of expression*. Point 9.

33. European Union Court of Justice (April 8, 2014). *Digital Rights Ireland Judgment* 56, 57, 59 and 63.

34. Breyer, P. (2005). Telecommunications data retention and human rights: the compatibility of blanket traffic data retention with the ECHR. *European Law Journal*, 11(3).

35. *Supra* (note 1), Chapter IV, par. 65.

36. *Supra* (note 1), Chapter IV, par. 165.

37. *Civil Framework*. Law No.12.965 of 2014, articles 10(3), 13(5), 15(3) and 22.

38. *Supra* (note 1), Chapter IV, par. 164.

39. *Supra* (note 1), Chapter IV, par. 168.

40. *Supra* (note 1), Chapter IV, par. 168 and 169.