

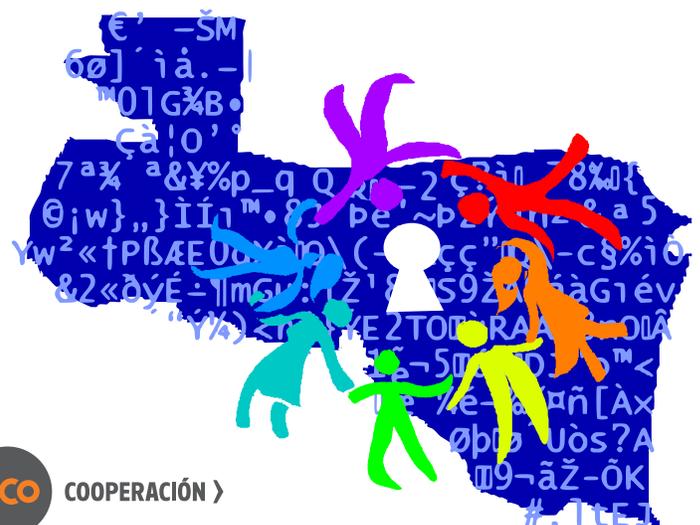
lyjpbQiox
HlqVRomqgghOAGr2Ov9

Digital Privacy for Human Rights Defenders?

A study on how the legal framework of El Salvador, Guatemala, Honduras, and Nicaragua can be used for the protection, criminalization, and/or surveillance of human right defenders.

Executive Summary

hjeZpj86Z/sIDhll vy5WvrrskJ4A1dbQioxwxvU



Reino de los Países Bajos



342.7

F9625p

Fundación Acceso

¿Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos / Peri, Luciana (coord.). -- 1a. ed.-- San José, C.R.: Fundación Acceso, 2015. pdf; 4MB

ISBN 978-9968-862-12-7

1. Derechos humanos. 2. Defensores de derechos humanos. 3. Privacidad digital. 4. Seguridad digital. I. Fundación Acceso. II. Título.

The opinions and criteria contained in the document belong to the partner organization and / or its authors and do not necessarily represent the views of Embassy of the Kingdom of the Netherlands or ICCO Cooperation.



“Digital Privacy for Human Rights Defenders? A study on how the legal framework of El Salvador, Guatemala, Honduras, and Nicaragua can be used for the protection, criminalization, and/or surveillance of human right defenders” by Fundación ACCESO is licensed under a Creative Commons Reconocimiento-CompartirIgual 4.0 Internacional License.



Table of Contents

Introduction.....	5
1. The right to privacy.....	10
2. The right to digital privacy in Central American constitutions.....	11
2.1. The right to intimacy and a private life.....	11
2.2. Inviolability of communications, documents, and place of residence.....	12
2.3. Informational self-determination.....	13
2.4. The right to a good reputation and honor.....	14
3. The right to digital privacy in other Central American legislation.....	15
4. Judicial Remedies for the right to digital privacy in Central America.....	18
5. Adapting Central American laws to international standards.....	19
6. Testimonials and concerns from technical experts and human rights defenders.....	21



yjpbQioxwx

Credits llqVRomqgghOAGr2Ov9VxK/EB

Coordinators

Luciana Peri

Authors

Katitza Rodríguez

Marlon Hernández Anzora

Hedme Sierra-Castro

Jorge Jiménez Barillas

Edy Táborá Gonzales

Mireya Zepeda Rivera

Content Review

Luciana Peri

Katitza Rodríguez

Design and Layout

Olman Bolaños

Larraitz Lexartza Artza

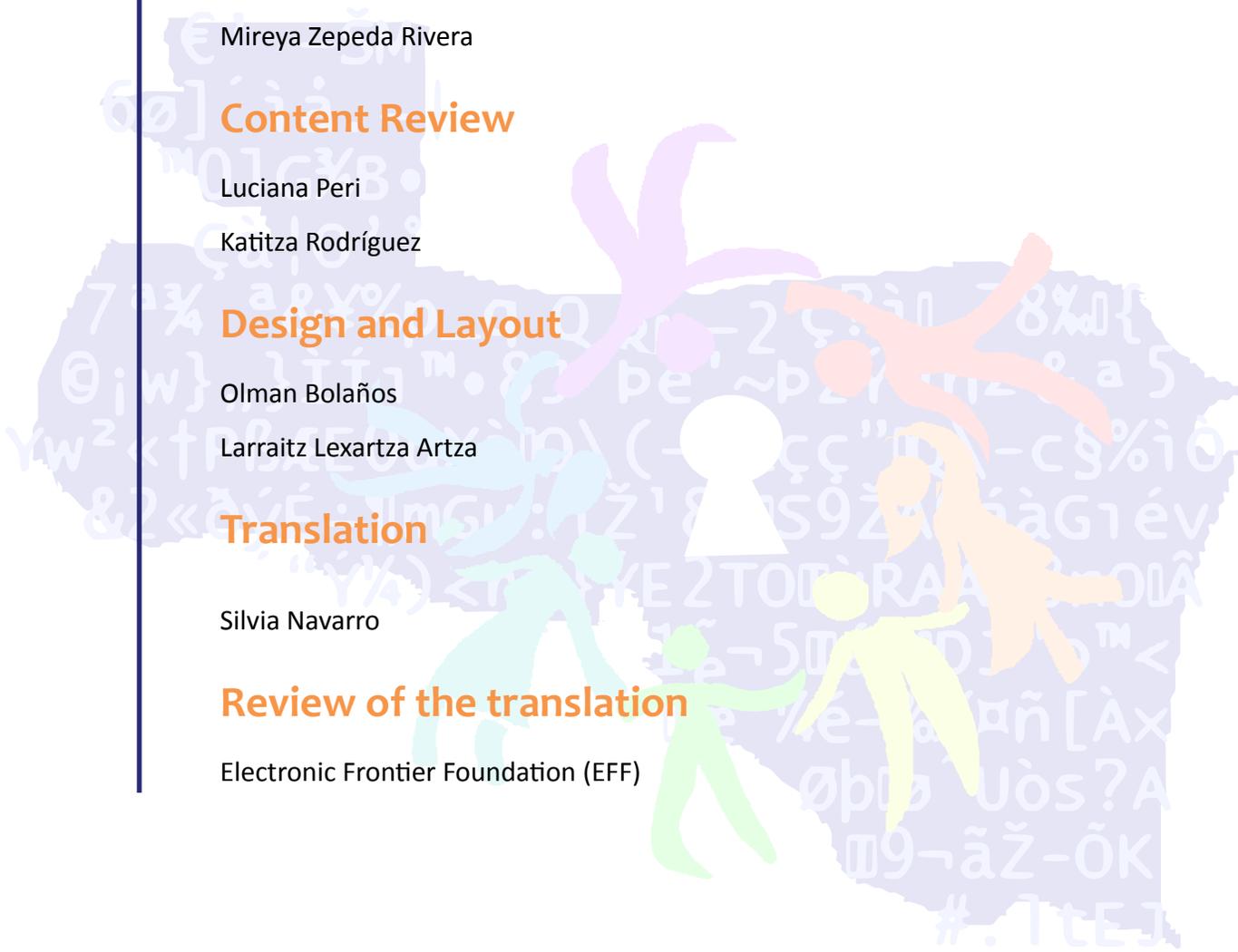
Translation

Silvia Navarro

Review of the translation

Electronic Frontier Foundation (EFF)

sCPRXlyjpbQioxwxvU



Executive Summary¹

Luciana Peri
Katitza Rodríguez

Fundación Acceso is a non-profit organization based in Costa Rica that has been around for over 20 years, and since 2007² works in Central America with human rights defenders, supporting them in processes related with their digital security.

FUNDACIÓN ACCESO'S MISSION

To help mitigate the ever-increasing human rights violations of vulnerable populations in Central America as related to their physical, technological, and psycho-social security.

Human rights defenders (HRDs) at risk are one of the populations with whom we work. In this regard, Front Line Defenders, in its annual report on the situation of HRDs in the world, has identified that:

Extreme violence continues to characterize attacks aimed at those who dare to speak in defense of human rights in Latin America and the Caribbean [...] HRDs were targeted by both state and non-state actors: state institutions including security forces, paramilitaries, criminal groups, private security companies or hired assassins from national and transnational companies³

Fundación Acceso has offered technical assistance and digital security trainings to the human rights defenders in Guatemala, Honduras, and Nicaragua, which has allowed us to maintain close relationships with those in the region.

- In many of these meetings, participants have expressed legal concerns related to their digital security and facilitators have had to answer questions such as:
- In my country, is it legal to encrypt my e-mails?
- When I am crossing a border, are migration officers allowed to force me to turn on my computer and show them my digital information?
- If there is a break-in in the organization where I work, and the computers are confiscated, do we have to provide the password to our encrypted e-mails?
- Would we be putting ourselves and the people that we work with at risk by supporting their digital security practices?

1. This summary has been prepared with the information contained in the various chapters of the research "Digital Privacy for Human Rights defenders?" Digital Privacy for Human Rights defenders? A study on how the legal framework of El Salvador, Guatemala, Honduras, and Nicaragua can be used for the protection, criminalization, and/or surveillance of human right defenders."

2. With the support of the Swedish International Development Cooperation Agency (SIDA) and Dutch Human Rights Fund for Central America, administered by ICCO Cooperation.

3. Front Line Defenders. "2015 Annual Report: Human Rights Defenders in the Balance", (2014,5). https://www.frontlinedefenders.org/files/annual_report_spanish_2.pdf (Retrieved: November 16th, 2015)



We realized we couldn't effectively answer their questions because no research had been conducted on these topics in the countries where we were working.

Nevertheless, a large information gap was identified: none of the countries in which Acceso worked, nor the broader Central American region, had produced any material on the topic.

As such, we accepted the challenge and took on the task of developing research aimed to meet the following objective:

GENERAL OBJECTIVE OF THE RESEARCH

To analyze the legal frameworks in El Salvador, Guatemala, Honduras, and Nicaragua related to the right to digital privacy in order to determine whether they can be used to criminalize and / or surveil HRDs in those countries.

Why El Salvador, Guatemala, Honduras, and Nicaragua?

Given the context in which the countries in the region are immersed in, cooperation, in its various manifestations, has prioritized its support particularly to those who make up the "Northern Triangle", as well as Nicaragua. This has decreased cooperation efforts in Costa Rica and Panama.

Taking into consideration the fact that Fundación Acceso has worked in these countries since 2007, and have learned about civil society biggest concerns and needs during the processes facilitated, the decision to undertake our initial research in these locations was made with the expectation that in the future Acceso would extend its research to include Costa Rica and Panama.

Front Line Defenders' report points to Guatemala and Honduras as the countries that face the most risk in the continent—special attention is given to environmental and land rights advocates, woman's rights defenders, and LGBT advocates. The report states that in all cases, "death threats were the single most common violation recorded,"⁴ in addition to arrests and judicial harassment, homicides, physical assaults, and stigmatization campaigns. El Salvador is also included in this last point, since it is a country in which "institutions like FESPAD (for its initials in Spanish) [...] registered nine violations against these groups in early 2014."⁵

From our experience working in the region, we know that the situation extends to Nicaragua, where activists fighting for gender equality are particularly persecuted, as are those opposing the construction of the Interoceanic Canal and mining projects that affect indigenous peoples and Afro-descendants. On that note:

[...] one cannot ignore the constant threats and smear campaigns promoted by the government [...] Threats, retaliation, smear campaigns, accusations, stigmatization, and attacks against defenders are clear signs of the existence of a systematic pattern of aggression that tries to undermine their work and describes them as government opponents and/or criminal defenders.⁶

4. Front Line Defenders. "2015 Annual Report: Human Rights Defenders in the Balance", (2014,5).

5. Regional Monitoring & Analysis of Human Rights in Central America Team. "Report on Human Rights and Conflicts in Central America 2013-2014". (El Salvador: Regional Monitoring and Analysis of Human Rights in Central America Team, 2014), 18.
<http://www.fespad.org.sv/wp-content/uploads/2015/01/Dddhh20141.pdf> (Retrieved: November 30th, 2015)

6. Regional Monitoring & Analysis of Human Rights in Central America Team. "Report on Human Rights and Conflicts in Central America 2013-2014", 17.



Why do we refer to it as the right to digital privacy, Internet, and communications?

We want to ensure that the protections for which we're fighting encompass all of the information that is:

- a) Stored on our electronic devices;
- b) Shared, communicated, and socialized on the Internet through emails, online calls, instant messages, social media, shared documents, etc.; and,
- c) Shared, communicated, and socialized through telephone calls and text messages.

It is important to remember that the information we're trying to protect does not only refer to the content of our communications—what we write, design, photograph, film, search, browse, talk about—but also to metadata, or all the data that is generated by these actions.

Metadata

Definition	Examples
Data linked to communications that is separate from content	Telephone numbers from which one makes and receives calls. The time of day one makes and receives these calls The approximate location from which one makes or receives these calls The date and time that one sends or receives emails. The location from which one connects to the Internet

Information generated from these actions can be used for many different purposes. Below is a list of communication information usages that we will NOT explore in this report:

- Commercial purposes: We will not concern ourselves with companies monitoring our behavior for marketing and advertising purposes
- Scams, frauds or bank privacy
- Online defamation

The actions that DO concern us are those that criminalize and/or monitor human rights defenders.

We aim to train human rights defenders to think about their own security in a comprehensive manner. Meaning, they should consider not only their physical security, but also their psycho-social, legal, and information and communication security, also known as ISC.

It has been proven that ISC and privacy violations can lead to the possibility of physical and psycho-social violations, and/or legal safety problems. So, for example, the surveillance of communications can be used to know the location of the person under surveillance, facilitating the perpetrator to make a threat or to make a direct attack easier.



The framework that we use as a guide in this report is a human rights framework so the political actors that we will focus on in this report are governments, and in some instances, private companies when acting as an intermediaries.

For example, our research is concerned with a situation where a government requests a person's call records from a phone company, and note a situation where a phone company uses a person's call records to tailor an advertisement that is sent to them

For this report, Fundación Acceso assembled a research team made up of a coordinator, international legal consultant, and national researchers from each of the countries covered by the investigation and established a set of objectives for the research:

SPECIFIC OBJECTIVES OF THE RESEARCH

1. Identify international standards related to the right to digital privacy on the Internet and in communications.
2. Familiarize ourselves with the current national and international legal frameworks in El Salvador, Guatemala, Honduras, and Nicaragua related to the right to digital privacy on the Internet and in telecommunications in order to determine whether there exists ambiguities and/or gaps.
3. Evaluate the national and international legal frameworks in El Salvador, Guatemala, Honduras, and Nicaragua related to the right to digital privacy on the Internet and in telecommunications, in order to determine their compliance with international standards on human rights to communications surveillance.
4. Identify the main concerns related to digital privacy on the Internet and in telecommunications, in El Salvador, Guatemala, Honduras, and Nicaragua, in order to provide answers from a legal perspective.

The report begins with an introduction to the right to digital privacy, and is followed by a first chapter on international standards for the protection of this right, that focuses on international standards on human rights to communications surveillance and concludes with a focus on international standards related to anonymity and encryption, and its relation to privacy and free expression. This chapter aims to establish privacy as a right that is protected by the domestic laws of each country and international human rights law.

Next, each country—El Salvador, Guatemala, Honduras, and Nicaragua—is presented with information that corresponds to the specific objectives outlined for the research. We first establish the existing background on each country and layout what has been investigated and how our researchers conducted their investigation. Also presented is data on the digital divide in order to estimate the portion of the population with access to the Internet and/or telecommunications and, in this way, identify those whose right to privacy in the digital arena can be violated. We also explain the situation of criminalizing human rights defenders at a national level.

Internet and telecommunications. This helps to identify international treaties that have been ratified by each country. We then explore to the national constitutions, as well as other laws, regulations and



precedents, such as rules in criminal matters, intelligence and counterintelligence, or those that regulate the telecommunications sector in each country. In all cases, safeguards and limitations are reviewed, particularly those related to surveillance, anonymity, encryption, and break-ins; and means to judicial remedy are listed.

The third section evaluates, by country, the adequacy of these national legal frameworks as related to international standards, particularly the International Principles on the Application of Human Rights to communications surveillance (explained in Chapter 1).

Then we present testimonials and the main concerns of the technology and humans rights sectors in each country as related to digital privacy rights on the Internet and in telecommunications, with the goal of eventually responding to them from a legal framework perspective at a later date. Then, each country chapter includes a section for national findings.

Finally, the report ends with a comparative chapter on the right to privacy in Central American legislation, outlining conclusions related to the constitutions and other laws, as well as research related to accessing digital privacy protections in Central America and assessing if Central American legal framework complies with international standards.

For the purposes of this summary, the results of the investigation will be organized, not by country, but by major issues.



1. The right to privacy

The right to privacy has been historically considered to be one of the most difficult human rights to define.⁷ However, the lack of a single definition does not mean that the issue is unimportant. On the contrary, as international doctrine has pointed out, “in a sense, all human rights are aspects of the right to privacy.”⁸

Conceptualizing privacy has always been a topic of much debate and study. For some authors, privacy is “the right to be left alone.”⁹ For others, the key to privacy is control, the “desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude, and their behavior to others.”¹⁰

The legal doctrine distinguishes between the different spheres of protection of the right to privacy. On the positive sphere, everyone has the right to their private life to be respected. In its negative dimension, it prohibits interference into all aspects of the person’s private life: their communications, documents, family, and home.

Privacy as a human right has been recognized in international human rights treaties.¹¹ Article 17 of the International Covenant on Civil and Political Rights (ICCPR) states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honor and reputation. The article also requires the government to adopt the necessary legislation measures to protect every person from such interference or attacks.

In its General Comment Nº16, the United Nations Human Rights Committee stated that the term “unlawful” in Article 17 of the ICCPR means that any interference authorized by States can only be prescribed by law, which itself must comply with the provisions, aims, and objectives of the Covenant. Furthermore, it adds that the introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance to provisions, aims, and objectives of the Covenant.¹²

The right to privacy, as any fundamental freedom, is not an absolute right. The government can restrict those rights to protect national security, public order, health, or public morals and the rights and freedoms of others. For this to be allowed, the restrictions must be prescribed by law, and they must be necessary and proportionate in order for legitimate aims to be pursued.

7. Marc Rotenberg, Allison Knight, Katitza Rodríguez. Privacy and Human Rights: An International Survey of Privacy Laws and Developments, Defining Privacy, (EPIC, 2006), <https://eff.org/phr2006> (retrieved: November 16th, 2015)

8. Fernando Volio. Legal personality, privacy and the family, Louis Henkin (ed) The International Bill of Rights, The Covenant on Civil and Political Rights, (New York: Columbia University Press, 1981), <https://eff.org/phr2006> (retrieved: November 16th, 2015)

9. Warren, S. & Brandeis, L. The Right to Privacy. Harvard Law Review, 4(1), 1890, 193-220.

10. Westin, A. Privacidad y Libertad. Nueva York: Atheneum, 1967.

11. Universal Declaration of Human Rights, Article 12; International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, Article 14; Convention on the Rights of the Child United Nations, Article 16; International Covenant on Civil Rights Politicians and Article 17; regional conventions including Article 10 of the African chapter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the principles of the African Union on Freedom of Expression, Article 5 of the American Declaration the Rights and Duties of Man, Article 21 of the Human Rights Declaration of ASEAN, Article 21 of the Arab Charter on Human Rights and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Expression and Access to Information; Camden Principles on Freedom of Expression and the Free Equality.

12. UNUnited Nations, General Comment Nº 16, Right to privacy (article 17), 35th session (1988), HRI/GEN/1/Rev.9 (Vol. I), 228. <http://www1.umn.edu/humanrts/hrccommittee/Sgencom16.html> (retrieved: November16th, 2015)



2. The right to digital privacy in Central American constitutions

The constitutions of the Republics of Guatemala, El Salvador, Nicaragua, and Honduras protect the right to privacy. The constitutional protection of this right is scattered among constitutional articles as well as a legal precedents of the Constitutional Court. They protect different aspects of the right to privacy, like: the right to intimacy; the right to a private life; the inviolability of communications, documents and place of residence; informational self-determination; data protection; or the habeas data guarantee.

2.1. The right to intimacy and a private life

El Salvador's constitution expressly guarantees the right to personal and family privacy, as well the self-image privacy, in Article 2. The Constitutional Chamber of the Supreme Court of that country has developed the content of this right and has defined it as a fundamental right:

A fundamental right, established directly in Article 2, section two of the Constitution, which applies to all people and consists of the preservation of the strictly domestic and private areas (that include family) against non-consensual invasions of privacy from the Government or other individuals. Therefore, the violation of the right to privacy, in the dynamics of modern societies, is, but is not limited to, obtaining and/or disclosing data or information included in such areas by third parties.¹³

In Honduras, both the constitution and the law refer to the right to privacy. The Criminal Chamber of the Supreme Court defines the positive area of the right to privacy as “the right of the individual to control, at their judgment, information of a personal nature that they want to make known and to determine the identity and number of people who they want to have access it,” while the same decision defines its negative area as “as the right to not suffer or tolerate interference of third parties in personal and family privacy and to reject any attempt to do so.”¹⁴ The Chamber of Honduras points out that, among the many areas of the right to privacy, these are:

their communications, which can be performed through [...] email, fax, television, telephone, and any other material, electronic, or telematic communication means that allows private communication between two or more people via text, audio, images, or video, which are of inviolable nature, no matter how banal, trivial, or insignificant the communications may be [...].¹⁵

Similarly, the constitution of Guatemala¹⁶ establishes the obligation to respect dignity, privacy, and decency of people's personal records. The Constitutional Court of this country explains that the main element of protection is the private life and its protection from arbitrary or illegal interference and meddling.¹⁷

13. Constitutional Chamber. Supreme Court of Honduras, Decision on Constitutionality 91- 2007 of September 24, 2010.

14. Criminal Division. Supreme Court, Sentence number CP-48-2011, 20, <http://www.poderjudicial.gob.hn/Jurisprudencia/Documents/CP-48-2011.pdf> (Retrieved: November 16th, 2015)

15. Criminal Chamber of the Supreme Court, Sentence number CP- 48-2011, 20.

16. Guatemala “Constitution of Guatemala” National Constituent Assembly (1985), Article 25.

17. Constitutional Court. Unconstitutional General ToTal. Case file 1201-2006 (Guatemala, 2007).



Meanwhile, the constitution of Nicaragua recognizes the right to a private life and family privacy.¹⁸ Under Article 27 of the constitution, this right applies to both Nicaraguan people as well as foreigners because it is a right that is strictly linked to the person, the only limitation being the exercise of political rights.¹⁹

It can be argued that the right to privacy is stated expressly on a constitutional level in these four Central American countries and that the constitutional courts have developed the content of this right in its negative (arbitrary interference in private life) and positive (the right to respect private life) areas.

2.2. Inviolability of communications, documents, and place of residence

In the Central American constitutions, the right to privacy of communications and a place of residence are different, but linked under the realm of the right to privacy. The essence of the right to privacy is to protect the communications of a person, and their place of residence or work, against arbitrary interference from others, including government.

The constitution of El Salvador expressly recognizes the right to a private residence and the protection of correspondence and telecommunications.²⁰ Similarly, the constitution of Nicaragua recognizes the right to the inviolability of residence, correspondence, and communications of any kind.²¹

In Guatemala's constitution, the right to privacy has been recognized since the Federal Constitution of 1823, which granted the privacy of correspondence and documents and authorized certain limitations of the right.²² The recognition of this right was later taken over by the Federal Constitution of Central America in 1824, and its reform in 1835.²³ However, it was not until 1879 that the constitution expressly admitted the inviolability of documents and correspondence, making it clear that this right can only be limited by a ruling from a competent judge and in accordance with the procedures established by law.²⁴

The current constitution of Guatemala expressly recognizes the inviolability of the residence²⁵ and the inviolability of correspondence, documents, and books.²⁶ In 2007, the its Constitutional Court made it clear

18. Nicaragua "Constitution of Nicaragua" National Assembly (1948), article 26.

19. Information taken from the "Nicaragua" chapter of this publication, written by Mireya Zepeda Rivera.

20. Article 23: All correspondence is inviolable, if intercepted it cannot be used as proof nor may it appear in any proceedings, except in cases of insolvency and bankruptcy. The interference and intervention of telephone communications is prohibited. In certain circumstances, it may be authorized by a court in writing and with grounds. The temporary intervention of any kind of telecommunications while preserving, in any event, the secrecy of what is private that is unrelated to the process or the information obtained from an illegal intervention will have no value (...) El Salvador "Constitution of the Republic" Legislature (1983).

21. Guatemala "Constitution of Guatemala" National Constituent Assembly (1985), Article 26.

22. Information taken from the chapter "Guatemala" in this publication, written by Hedme Sierra-Castro and Jorge Jiménez.

23. Information taken from the chapter "Guatemala" in this publication, written by Hedme Sierra-Castro and Jorge Jiménez.

24. Guatemala "Constitutive Act of the Republic of Guatemala" (1879), Article 37. The correspondence and private papers of any person are inviolable. The first can only be withheld, and even opened, by a competent judge and the second only in the cases where the formalities required by law are met.

25. Article 23: Inviolability of the home. The home is inviolable. No one may enter the home of another person without their permission, except with a written warrant from a competent judge in which the reason of the diligence is specified and it can never be before 6am nor after 6pm. Such diligence must always be performed in the presence of the interested party or his representative. Guatemala "Constitution of Guatemala"

26. Article 24: Inviolability of correspondence, documents and books. The correspondence, documents and books of every person are inviolable. They can only be revised or seized with a warrant signed by a competent judge and should include legal formalities. The secrecy of correspondence, telephone, radio, and wire communications, as well as all other products of modern technology, is guaranteed. Books, documents and files that relate to the payment of taxes, fees and other dues, may be reviewed by the competent authority in accordance with the law. Is punishable to disclose the amount of taxes paid, profits, losses, costs, and any other information concerning the revised accounting of an individuals or legal entities, except for the balance sheets, whose publication is mandated by law. Documents or information obtained in



that the right to confidentiality of correspondence protects the privacy of individuals against interference into their private lives and can only be limited by social needs and/or public interest.²⁷

Meanwhile, the constitution and legal precedent of Honduras also protects the inviolability of the place of residence²⁸ and communications.²⁹ On the latter, the sentence CP- 48-2011 of the Criminal Chamber of the Supreme Court of Honduras defined what is meant by the right to inviolability of private communications:

The one that, derived from the right to privacy, prohibits individuals outside of the communication, and primarily the government, from: seizing, recruiting, intercepting, opening, recording, reproducing, or disclosing private communications whether such actions are done at the time the communication is being carried out (in real time), or ex post facto, which means that it is done using a record of the communication after the fact, such as letters, phone devices or computers, or electronically on personal email accounts, social media, mailboxes, chats, etc. The inviolability of communications include the protection of records kept by public or private companies that provide communications services and can only be used for accounting purposes.³⁰

2.3. Informational self-determination

The right to informational self-determination arose in Germany in 1983 after a lawsuit on a population census project allowed the personal data of thousands of Germans to be processed. The German Court stated that new technologies were able to process data so that a complete and detailed picture of the person was achieved, including areas of privacy, transforming the citizen into a “glass man.”³¹ The court concluded that “this basic right warrants the capacity of the individual, derived from the idea of self-determination, to decide for themselves when and within what limits they will proceed to disclose situations involving their life.”³² Personal data is generally understood as data that can identify or be able to identify a particular person.

In Honduras, the constitution does not expressly recognize the right to data protection or informational self-determination. However, its protection is included within the constitutional guarantee of habeas data, which has existed since 2013:³³

violation of this article are not to be used as precedents or to serve as evidence in a trial. Guatemala “Constitution of Guatemala”

27. Constitutional Court. Partial General Unconstitutionality. Case file 2622-2006. (Guatemala, 2007), <http://vlex.com/vid/-423703874> (Retrieved: November 16th, 2015)

28. Article 99: The place of residence is inviolable. No entry or search may take place without consent of the inhabitant or by resolution of a competent authority. However, a forceful entry can be made in case of emergency, to prevent the act or impunity of a crime, or to avoid serious damage to people or property. Except for emergency cases, the forceful entry into the residence cannot be done from six o'clock in the evening until six o'clock in the morning, without incurring liability. The law will determine the requirements and formalities in order for the entry, search, or for a forceful entry to take place, as well as the responsibilities incurred by who carries it out. Honduras “Constitution of the Republic” La Gaceta. 23, 612 (January 20th, 1982)

29. Article 100: Every person has the right to the inviolability and secrecy of communications, in particular of postal, telegraphic, and telephonic communications, except for a judicial decision. Honduras “Constitution of the Republic”

30. Criminal Division. Supreme Court, Sentence number CP-48-2011, 20.

31. See: Iberoamerican Data Protection Observatory <http://oiprodat.com/2013/03/15/configuracion-juridica-del-derecho-a-la-autodeterminacion-informativa/>

32. Germany, December 15th 1983 Sentence. Census Act. Right to a personality and human dignity.

33. Honduras “Amendment to the Constitution of the Republic”, decree 237-2012 of January 23rd 2011, https://www.oas.org/dil/esp/Constitucion_de_Honduras.pdf



Article 182. The State recognizes [...] the Habeas Data right. [...] the action can only be carried out by the person whose personal or family data is stated in archives, or public or private records, as follows: [...] 2) Every person has the right to access information about themselves or their assets in an unobstructed and non-strenuous manner, whether it is contained in databases, or public or private registries, and, if necessary, update, correct and/or amend it.

In Guatemala, the constitution does not expressly offer personal data protection. However, the Constitutional Court has defined what personal data is and has recognized the need to update their data, to correct it if incorrect, to keep it confidential or in reserve, and to exclude it from certain given information that may be considered sensitive for the interested party.³⁴

In Nicaragua, the protection of personal data is contained in the constitutional guarantee established in Article 26.3 of its constitution, which determines that every person has the right to know about all the personal information that has been collected on them by private and public entities, as well as the right to know why and for what purpose that information was been collected.³⁵

The constitutional legal precedent does recognize informational self-determination and establishes temporarily a constitutional protection act as a constitutional guarantee mechanism in the absence of *Habeas Data*.³⁶

2.4. The right to a good reputation and honor

The right to a good reputation, honor, or a good name recognizes that every person should enjoy the reputation they have built socially in front of others. This right has two aspects: a good reputation and honor. The first relates to the reputation that every individual has.³⁷ The second is recognizing the dignity that each person deserves from other members of society as a human being.

In the context of surveillance, these rights can be violated when the content of electronic communications, illegally obtained, are made public in a way that may affect the honor or reputation of the owners of the private information that has been made public.

While countries in Central explicitly recognize that right,³⁸ this development as well as the tensions between the right to privacy and freedom of expression, are beyond the scope of this investigation.

(retrieved: November 16th, 2015)

34. Information taken from the “Guatemala” chapter of this publication, written by Hedme Sierra-Castro and Jorge Jiménez.

35. Information taken from the “Nicaragua” chapter of this publication, written by Mireya Zepeda Rivera.

36. Information taken from the “El Salvador” chapter of this publication, written by Marlon Hernandez Anzora

37. Sentence C -489 /02, the Constitutional Court of Colombia defines this right as “the right to a good name, as an expression of the reputation or the fame that a person has, is hindered with false or wrong information that is unfounded spread and distorts the public’s perception of the individual.”

38. Nicaragua “Constitution of Nicaragua” National Constituent Assembly (1948), Article 26.



3. The right to digital privacy in other Central American legislation

In Central America there is not a single legislative body that contains all regulations that authorize government surveillance. The regulations are scattered throughout the constitution, court decisions, and laws. Furthermore, the legal guarantees that protect individuals against the interference on privacy and freedom of expression are also scattered among the constitution, laws, and even international treaties.

In all countries, in addition to their constitutions, we've identified relevant sources for the protection, criminalization, and/or digital surveillance of human rights defenders:

- Penal Code
- Criminal Procedure Code
- Law on Access to Public Information
- Telecommunications Law

In the arrangement of the four countries studied, the Criminal Procedure Code (CPC) regulates the interception of communications.

For example, in **Nicaragua**, the CPC states that communications interceptions are allowed in cases of terrorism; kidnapping, organ trafficking and human trafficking for sexual purposes; crimes related to narcotics, psychotropic substances and other controlled substances; asset or money laundering; and international trafficking of weapons, explosives, and stolen vehicles. In these cases, the interception request must come from the Attorney General's Office or the General Director of the National Police and must be authorized by a judge.³⁹

In **Guatemala**, the Criminal Procedure Code establishes that the interception and seizure of correspondence (postal, telegraphic or telephonic) addressed towards the defendant or sent by them, can be ordered, under an order issued by a judge. In this case, the content will be sent to the competent court and, once the intercepted correspondence is received, the court will open the correspondence, stating on record all the proceedings that took place.⁴⁰

The Criminal Procedure Code of **El Salvador** states that, if it's necessary to intercept the communications of a person being investigated or prosecuted is, the interception must comply with the country's appropriate constitutional guarantees and due process so that this information can be incorporated into a judicial process and constitute as proof (Art. 176).⁴¹

More specifically, in the case of Guatemala, most of the regulations related to communications interceptions can be found in the Law Against Organized Crime and the Law of the Civil Intelligence General Direction, which clarifies that communications can be intercepted in intelligence gathering related to organized crime (with emphasis on narcotics activity and common crime), when there is danger to life,

39. Information taken from the chapter "Nicaragua" of this publication, written by Mireya Zepeda Rivera.

40. Guatemala "Criminal Procedure Code" Organization of American States (1992), articles 203, 204, 205, http://www.cicad.oas.org/fortalecimiento_institucional/legislations/PDF/GT/decreto_congresional_5192_codigo_procesal_penal.pdf (Retrieved: December 1st, 2015)

41. El Salvador "Criminal Procedure Code" Legislative Assembly (2009), article 176.



physical integrity, liberty, and property of certain people. An important difference between the two types of intervention is that the information gathered by the Intelligence Law is only used for prevention, so it cannot be used as evidence.⁴²

In both cases, the Public Prosecutor is the only one that can make requests and, for the Law against Organized Crime, authorization is given, in the first instance, by judges of the Criminal Court, while, for the implementation of the Law on Intelligence, authorization is given by a Chamber of the Court of Appeals.

Both in El Salvador and Honduras, we found a law that regulates, very specifically, the limitation of the right to privacy by state surveillance, referred to as the Act for the Interception of Communications.

In Honduras, with the implementation of the Intervention of Private Communications Law, the rules of the Criminal Procedure Code on the interception of communications were abolished in January 2011. This new law aims to “establish the legal framework of procedural regulation for the interception of communications”⁴³ and constitute “an essential tool in the fight against traditional crime, especially against organized or non-conventional crime”;⁴⁴ this means that the law applies in the investigation of any crime.⁴⁵

In El Salvador, it specifies that the law can be used in a list that includes 14 crimes⁴⁶, plus all offenses included under the same law, plus all crimes related to any mentioned above, so its applicability is also very broad.⁴⁷

In both cases, regulation exists for the intervention of:

Any kind of transmission, emission, signal reception, symbol, written sign, image, email, sound, or information of any nature through wire, radio, optical, or other electromagnetic systems, including those being made by means of telephone, radio, telegraphy, computer, or electronic means, or of similar nature.

Honduras adds “as well as any communication that takes place through any means or type of transmission.”

In El Salvador, the Attorney General of the Republic is the only authority that can request the intervention of telecommunications directly, or through the Director of the Intervention Center. In Honduras the request may be made by the Public Prosecutor, or, through him, by the Private Attorney and by Attorney

42. Information taken from the “Guatemala” chapter of this publication, written by Hedme Sierra-Castro and Jorge Jiménez.

43. El Salvador “Special Law for Intervention of Communications” Legislative Assembly (2010), Article 1.

44. El Salvador “Special Law for Intervention of Communications”, article 1.

45. Information taken from the chapter “Honduras” of this publication, written by Edy Tabora Gonzales.

46. Article 5 provides exhaustively the only offenses that may use means of intervention: 1) Murder and its aggravated form. 2) Aggravated Imprisonment, Kidnapping and attempts Against Liberty. 3) Pornography, use of under eighteen and incapable or mentally deficient people in pornography, and Possession of pornography. 4) Extortion. 5) Extortion. 6) Illegal negotiations. 7) Proper, improper and active bribery. 8) Illegal groups. 9) People Trade, Smuggling of People, Trafficking in People and its aggravated form. 10) International criminal organizations. 11) Offenses under the Law regulating the Drug on Activity. 12) Offenses under the Special Law Against Acts of Terrorism. 13) Offenses under the Anti- Money and Assets Laundering Law. 14) Crimes committed in the form of organized crime in the terms established under this law. 15) The offenses under this Law. 16) Offenses related to any of the above.

47. Information taken from the “El Salvador” chapter of this publication, written by Marlon Hernandez Anzora.



General of the Republic, and it has to be authorized by a court in criminal matters, whether it is national or sectional, unlike El Salvador where authorization is given by any of the investigating judges residing in the capital of the country.

In both countries, the laws agree to establish as principles for intervention of communications:

- Jurisdiction
- Proportionality
- Confidentiality
- Transitoriness

In Honduras the principle of necessity and appropriateness is added, while in El Salvador a subjective limitation is included.

On the other hand, in Nicaragua the Personal Data Protection Law is highlighted, which is not found in any of the other countries and is currently only a draft in Honduras. It is also important to mention the habeas data appeal.

In **Nicaragua**, following the Infonet Case where, without the people's consent, data on their financial solvency was obtained and marketed to companies so that they could offer them their products, a decision was made to join forces and legislate on the personal information protection issue. In this way in 2012, the Personal Data Protection Law,⁴⁸ was approved, which aims to protect natural or legal persons against the processing, automated or not, of their personal data in public or private archives in order to guarantee the right to personal and family privacy and the right to informational self-determination.⁴⁹

The Personal Data Protection Law, Article 8, identifies four categories of personal data:

- Sensitive personal data
- Health related personal data
- Computerized personal data
- Commercial personal data

Computerized personal data:

Personal data processed through electronic or automated means.

Each of these categories has different characteristics and their collection and processing will change depending on the case.

In addition to this, to ensure the safeguard and protection of personal data, in 2013 the Protection Act⁵⁰ was reformed to include the habeas data appeal in order to prevent illicit advertising. In this appeal, the aggrieved party has the right to demand that the information is modified, blocked, updated, and even eliminated when it relates to sensitive personal data and falsehood, inaccuracy, or illegality is presumed in the access of the information, or in the case that the information infringes constitutional rights. The amendment to the Protection Law establishes that the habeas data appeal:

... is created to guarantee protection of personal data in files, registers, data banks, or other technical means, publicly or privately, whose advertising constitutes an invasion of personal

48. Nicaragua "Personal Data Protection Law" La Gaceta No. 61 (2012)

49. Nicaragua "Personal Data Protection Law", article 1.

50. Nicaragua "Ley de Amparo" La Gaceta, April 8th, 2013.



privacy and has relevance to processing sensitive data of people in their intimate and family environment.⁵¹

The habeas data appeal refers to the legitimate right of the individual to “freely control their personal data”⁵². This means a person has control over the use and management of their own personal data that has been stored in different places; this allows them to exercise informational freedom—to have the ability to control the information that concerns them. Specifically, there are two ways one can control this information. On the one hand, third parties must obtain explicit and individual consent to capture and process data and, on the other hand, legal authorization must be obtained. However, neither consent nor legal authorization involve the loss of power over the data, since there is a series of rights that complement informational self-determination⁵³ (the right to cancel the processing of personal data, the right to rectify data that is not accurate, the right to be informed of the collection of personal data, the right to access the personal data collected, among others).⁵⁴

4. Judicial Remedies for the right to digital privacy in Central America

All of the countries featured in this report have two fundamental judicial remedies against human rights violations in the context of surveillance: a writ of protection (writ of amparo) or an appeal on the grounds of unconstitutionality.

Honduras guarantees the right to a habeas data appeal; its purpose to ensure that personal information can be updated, modified and/or deleted.

Similarly, the right to a habeas data appeal was integrated in Nicaragua as a protection mechanism against violations on the right to informational self-determination and the protection of personal data—the right that assists every person in cases where:

1. the person responsible for the data storage refuses to disclose the information requested by the citizen so the citizen may seek judicial remedy in order to access the public or private records in which their personal or family group data is included, in order to ensure their accuracy.
2. the person responsible for the data storage refuses to delete, correct or update the personal data, so the citizen may seek judicial remedy in order to correct the data, eliminate inaccurate, outdated, or discriminatory, for example, data that reveals a political party affiliation, religious belief, and so on.
3. The person responsible for the data storage refuses to provide citizens the right to object to appear in databases, even if the data has been collected from sources available to the public⁵⁵.

51. Nicaragua “Ley de Amparo” article 6.

52. Osvaldo Alfredo Gozáini, “Habeas Data. Protection of personal data. Doctrine and legal precedence”. (Argentina: Rubinzal Culzoni Editores, 2011), 67.

53. Pablo Lucas Murillo de la Cueva, “Perspectives of the right to informational self-determination”. *Internet, Derecho y Política Magazine*, 5, (2007): 18-32.

54. Information taken from the “Nicaragua” chapter of this publication, written by Mireya Zepeda Rivera.

55. Jjovanka Durón Chow. “The informational attacks and personal data protection in Nicaragua”. *Encuentro Magazine*, No. 71, (2005), 15-16.



5. Adapting Central American laws to international standards

The highest standards protecting the right to privacy with regard to communications surveillance are outlined in case law and international doctrine. These decisions have been assembled to develop the “International Principles on the Application of Human Rights to Communications Surveillance,” henceforth the 13 Principles.⁵⁶

The 13 Principles are an innovative framework that attempts to clarify how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques. They are the outcome of a global consultation with civil society groups, industry, and international experts in communications surveillance law, policy, and technology. These principles can provide civil society groups, industry, States, and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with international human rights standards.⁵⁷

The 13 principles have been cited in the report from the Review Group on Intelligence and Communications Technology for the President of the United States,⁵⁸ the report of the Inter-American Commission on Human Rights,⁵⁹ the Report on Anonymity and Encryption from the special Rapporteur for Freedom of Expression of the United Nations,⁶⁰ and Privacy in the Digital Age from the High Commissioner for Human Rights of the United Nations,⁶¹ among others.

Each of the countries we researched respect international human rights standards to some degree, but none of the countries have incorporated these standards entirely into their legal frameworks.

El Salvador’s legal framework (constitutional, secondary legislation, signed treaties, legal precedent) offers important guarantees, many of them in accordance with international standards on human rights to communications surveillance. However, there is an institutional fragility and social-political situation that, despite having a legal framework that establishes these guarantees, allows for many of these standards to be disrespected, circumvented, or violated by those who hold public office.⁶²

More over the country does not prioritize discussion on new information and communications technology. This makes adopting innovative proposals on international standards difficult—such an idea is foreign to lawmakers and civil society due to the lack of public debate and knowledge on the subject. Despite adopting and enforcing the law on Intervention of Communications, any debate surrounding the law and

56. International Principles on the Application of Human Rights to Communications Surveillance. Accessible at: <https://necessaryandproportionate.org/principles>

57. For a description of each of the principles and their foundation as an international law instrument of human rights, see the chapter on International Standards of Human Rights. Katitza Rodriguez, *International Human Rights Standards on Privacy*.

58. See: http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf

59. Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression, *Freedom of Expression and Internet*. Resolution OEA/Ser.L/V/II.CIDH/RELE/INF.11/13, December 31st de 2013, par. 15 and 16. http://www.oas.org/es/cidh/expression/docs/informes/2014_04_08_Internet_WEB.pdf (retrieved: April 14th, 2015)

60. United Nations. Human Rights Counsel. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Resolution A/HRC/29/32, May 22nd 2015, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc, (retrieved: September 14th, 2015)

61. United Nations. General Session. The right to privacy in the digital age. Annual report of the United Nations High Commissioner for Human Rights, resolution, A/HRC/27/37, June 30th 2014, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

62. Information taken from the “El Salvador” chapter of this publication, written by Marlon Hernandez Anzora



its application to fundamental rights is frankly less important.⁶³

Despite having important transparency laws, like the Law on Access to Public Information (LAIP in Spanish), there is still a culture of secrecy and arbitrariness rooted within institutions and among public officials. This allows for the existence of certain secret regulations, which violate not only to the international principles of legality and transparency, but also the constitutional guarantees according to the Constitution of the Republic.⁶⁴

Any limitation to the right to communications privacy can only be authorized with a clear and precise law, in accordance with international obligations that the four countries in this report have signed. When analyzing these obligations, we see that Guatemala's Law against Organized Crime is neither clear nor precise about the type of communications that can be intercepted and its Law from the General Management of Civil Intelligence is also neither clear nor precise about the grounds and legal requirements that must be met in order to intercept communications.⁶⁵

The laws that establish surveillance measures must pursue legitimate objectives in a democratic society. The Guatemalan law that limits the right to communications privacy should be used only when strictly necessary and proportional to the objective that is pursued. Despite this, the Law Against Organized Crime, the Law from the General Management of Civil Intelligence, and the Criminal Procedure Code do not fully comply with the principles of necessity, appropriateness, and proportionality, and therefore must be reformed.⁶⁶

In addition, in cases where a person's right to privacy has been limited due to communications surveillance, they must be granted due process-- this includes the right to notification. To ensure minimal abuse by authorities, the agencies that are tasked with intercepting communications must be transparent and release statistics on the instances in which they've violated the right to privacy. There must also be a proper, truly independent supervising mechanism in place.⁶⁷

In Honduras, the special law for Telecommunications Interception contains ambiguous and open restrictions that allow law enforcement to request for the surveillance of Internet activity and communications for any crime and, more seriously, to do so without probable cause or evidence that would allow them to assess the necessity and proportionality of the intervention. The law authorizes the intervention when a person under investigation is suspected to have participated in the commission of a crime. When a law this ambiguous fails to require an independent court in the decision to authorize surveillance the process will lack the necessary independent public oversight mechanisms required and leave a wide margin for abuse.. Although this law incorporates some of the same principles established in the 13 Principles, such as proportionality, necessity, and judicial authorization it loses its power when it is contradicted by other rules or there exists no control mechanisms to supervise surveillance activities. As such, we conclude that

63. Information taken from the "El Salvador" chapter of this publication, written by Marlon Hernandez Anzora.

64. Information taken from the "El Salvador" chapter of this publication, written by Marlon Hernandez Anzora.

65. Information taken from the chapter "Guatemala" in this publication, written by Hedme Sierra-Castro and Jorge Jiménez.

66. Information taken from the chapter "Guatemala" in this publication, written by Hedme Sierra-Castro and Jorge Jiménez.

67. Information taken from the chapter "Guatemala" in this publication, written by Hedme Sierra-Castro and Jorge Jiménez.



Honduras does not fully comply with the international human rights standards to communications surveillance, either because of omission or inadequate incorporation.⁶⁸

Nicaragua does not pay adequate respect to international standards on the right to digital privacy in its national legislation. The lack of political will or judicial guarantees, the centralization of power, and the criminalization of human rights defenders are characteristic of Nicaragua's current government. Despite the fact that personal data protection was regulated and written into law in 2012, the absence of institutions that can ensure compliance to the procedures that the legislation requests to create is an indicator of the precariousness of access to justice in Nicaragua.⁶⁹

6. Testimonials and concerns from technical experts and human rights defenders

In order to achieve the objective of identifying the main concerns regarding the right to digital privacy, on the Internet and in telecommunications within the technical and human rights sectors, we conducted several interviews and focus groups.

The experiences, opinions, and questions that were collected come from people working to defend human rights, which makes them valid participants in this discussion about surveillance and criminalization online and through communications. However, due to the type of methodology used, we cannot make generalizations from their answers, but rather raise them for what they are: experiences, doubts, and perceptions that human rights defenders in the country have experienced firsthand.

Experiences

Since the armed conflict in the country, El Salvador has wiretapped members of the political opposition as well as human rights defenders. These victims are increasingly concerned with the security of their communications due to the current authoritarian management of public security policies where, under which, such invasions of privacy may be normalized or seen as necessary, not only by public officials but also by citizens.

In Honduras the current situation of Internet and communications surveillance began with the coup in 2009, at a time when political opponents and human rights defenders were the targets of surveillance. These invasive practices were exacerbated during the elections and during the discussions of important laws, and during times of protest.

In both countries similar experiences were identified by human rights defenders; many were the victims of hacking or attempts at hacking email accounts and social networks, as well as hacking and/or cloning institutional web pages through massive request forms.

In Nicaragua, surveillance and the interception of telephone and electronic communications has been sustained practice carried out on both human rights defenders as well as political oppositionists. In Guatemala, nine out of ten people said that their cell phones were intercepted and/or used as microphones and that they know other human rights activists who have experienced the same thing.

68. Information taken from the chapter "Honduras" of this publication, written by Edy Tabora Gonzales.

69. Information taken from the "Nicaragua" chapter of this publication, written by Mireya Zepeda Rivera.



Regarding raids and searches, in El Salvador, at least two organizations that employed human rights defenders we interviewed, have suffered illegal raids by unknown people, in which computers with sensitive information were seized.

Most of our interviewees in Guatemala said that they were familiar with at least raid to a human rights organizations where computers, hard drives, USB sticks and CDs with sensitive information were seized.

In Nicaragua, two people that were interviewed highlighted cases of arbitrary raids on organizations for which they work that had occurred in recent years. These raids have been part of an increasing intensity of the democratic governance crisis in the country.

In Honduras, two of our interviewees said that the police conducted raids on a journalist and a human rights organization and that, in both cases, computers were seized.

Other instances of digital privacy violations in the region include political opponents and/or human rights defenders in El Salvador being blackmailed through the use of personal information obtained through communications interceptions, with the purpose of defaming them and/or discrediting their positions.

In Nicaragua, another type of indirect surveillance consists of monitoring political movements or protests in order to separate the activists and defenders from their cameras, phones, tablets and computer equipment so that those conducting surveillance can use the information on those devices to intimidate them by extracting and publishing information to portals that are made to discredit the work that has been done by the human rights sector.



According to the perception and experience of those interviewed Who are the actors involved in digital surveillance?

El Salvador	Guatemala	Honduras	Nicaragua
<ul style="list-style-type: none"> • Presidency of the Republic through the government Intelligence Agency and the Secretary of Citizen Participation, Transparency and Anti-Corruption • General Prosecutor of the Republic • Telephone companies • Teams of people tied to mayor political groups • US Embassy in El Salvador 	<ul style="list-style-type: none"> • The government, especially through the army 	<ul style="list-style-type: none"> • Intelligence agencies through the Communication Intervention Unit • Investigation departments of police offices • Telecommunications companies 	<ul style="list-style-type: none"> • Members of the national police • Nicaraguan army • Clashing political party supporters • Sandinista youth • Officials from the General Tax Directorate (DGI for its initials in Spanish) • Inspectors from the Social Security Institute (INSS for its initials in Spanish) • Telecommunications officials • ISPs • Immigration officials • Congress • Magistrates • Political leaders of the ruling party in neighborhoods • Government-supporter journalists





Reino de los Países Bajos



COOPERACIÓN >