

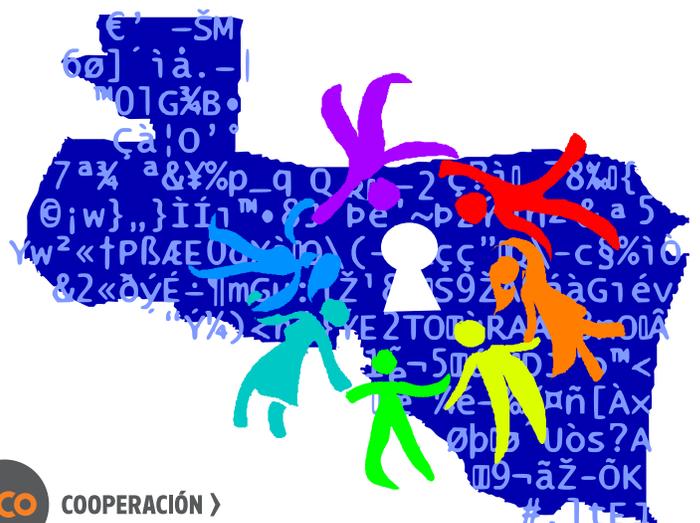
lyjpbQiox
HlqVRomqgghOAGr2Ov9

¿Privacidad digital para defensores y defensoras de derechos humanos?

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

Resumen Ejecutivo

UijeZpj86Z/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.

Las opiniones y criterios contenidos en el material pertenecen a la organización socia y/o a sus autores y no necesariamente representan la visión de la Embajada del Reino de los Países Bajos ni de ICCO Cooperación.



¿Privacidad digital para defensores y defensoras de derechos humanos? 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 by Fundación ACCESO is licensed under a Creative Commons Reconocimiento-CompartirIguual 4.0 Internacional License.



¿Privacidad digital para defensores y defensoras de derechos humanos?

Contenido

Introducción.....	5
1. El derecho a la privacidad.....	10
2. El derecho a la privacidad en las constituciones centroamericanas.....	11
2.1. Derecho a la intimidad y la vida privada.....	11
2.2. Inviolabilidad de las comunicaciones, documentos y domicilio.....	12
2.3. Autodeterminación informativa.....	13
2.4. El derecho al buen nombre y al honor.....	14
3. El derecho a la privacidad digital en otras leyes centroamericanas.....	15
4. Mecanismos de acceso a la justicia para la protección de la privacidad digital en Centroamérica	18
5. Adecuación de las normas centroamericanas a los estándares internacionales.....	19
6. Experiencias e inquietudes del sector técnico y de defensa de derechos humanos.....	21



yjpbQioxwx

Créditos

Coordinadora

Luciana Peri

Autoras y autores

Katitza Rodríguez

Marlon Hernández Anzora

Hedme Sierra-Castro

Jorge Jiménez Barillas

Edy Táborá Gonzales

Mireya Zepeda Rivera

Revisión de contenido

Luciana Peri

Katitza Rodríguez

Diseño y diagramación

Olman Bolaños

Larraitz Lexartza Artza

Corrección filológica

Marcia Ugarte Barquero

sCPRXlyjpbQioxwxvU



Resumen Ejecutivo¹

Luciana Peri
Katitza Rodríguez

Fundación Acceso es una organización sin fines de lucro con sede en Costa Rica con más de 20 años de existencia, que desde el año 2007² trabaja en la región centroamericana con defensores y defensoras de derechos humanos en riesgo, apoyándoles en procesos relacionados con su Seguridad de la Información y la Comunicación (SIC), respondiendo a la misión de:

MISIÓN DE FUNDACIÓN ACCESO

Contribuir a mitigar la permanente y creciente violación a los derechos humanos vinculados a la seguridad física, tecnológica y psico-social de poblaciones en situación de vulnerabilidad y/o riesgo en Centroamérica.

Así, una de las poblaciones con la que trabajamos es con defensores y defensoras de derechos humanos en riesgo. Al respecto, Front Line Defenders, en su informe anual sobre la situación de defensores/as de derechos humanos en el mundo, ha identificado que:

La violencia extrema continuó caracterizando los ataques dirigidos a quienes se atrevieron a levantar la voz por la defensa de los derechos humanos en América Latina y el Caribe. [...] Los/as DDH fueron tomados como objetivo, tanto por actores estatales como no estatales: instituciones del estado, entre ellas las fuerzas de seguridad, paramilitares, grupos criminales, compañías de seguridad privadas o asesinos a sueldo de las compañías nacionales y transnacionales.³

En estos años, Acceso ha ofrecido asistencia técnica y capacitaciones en SIC al sector de defensa de derechos humanos en Guatemala, Honduras y Nicaragua, gracias a lo cual ha mantenido una cercana relación con las y los defensores de la región.

En muchos de estos encuentros, las y los participantes han manifestado inquietudes legales relacionadas con su SIC. De esta forma, las y los facilitadores nos encontrábamos con preguntas tales como: “En mi país ¿es legal cifrar los correos electrónicos?”; “Al intentar cruzar una frontera ¿Los oficiales pueden obligarme a prender mi computadora y enseñarles su contenido?”; “Si la organización para la que trabajo sufre un allanamiento, en el que se decomisan las computadoras ¿Debemos entregar las clave de cifrado?”; “¿Nos estaremos poniendo en riesgo a nosotras mismas y a las personas con las que trabajamos al apoyarles en sus procesos de SIC?”.

Realmente, desde Acceso no podíamos dar respuestas a estas preguntas ya que ninguna persona integrante del equipo era abogada o experta en temas jurídicos. Intentamos obtener la información consultando con personas clave, buscando investigaciones, estudios, o algún material que pudiera servirnos de respaldo, pero

1. El presente resumen ha sido elaborado con la información contenida en los diferentes capítulos que integran la investigación “¿Privacidad digital para defensores y defensoras de derechos humanos? Privacidad digital para defensores y defensoras de derechos humanos? 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”.

2. Con el apoyo de la Agencia Sueca de Cooperación para el Desarrollo Internacional (ASDI) y del Fondo Holandés de Derechos Humanos para Centroamérica, administrado por ICCO Cooperación.

3. Front Line Defenders. “Informe 2015: Defensores/as de derechos humanos en la cuerda floja” (2014, 5), https://www.frontlinedefenders.org/files/annual_report_spanish_2.pdf (consultado: 30 noviembre, 2015)



nos encontramos ante un gran vacío: En ninguno de los países en los que trabajábamos se había producido ningún material sobre este tema y tampoco a nivel centroamericano.

Ante tal panorama, decidimos aceptar el desafío y darnos a la tarea de realizar esta investigación, para lo que planteamos como objetivo general:

OBJETIVO GENERAL DE LA INVESTIGACIÓN

Analizar los marcos legales vigentes en El Salvador, Guatemala, Honduras y Nicaragua relacionados con el derecho a la privacidad digital, en internet y en las telecomunicaciones para determinar si pueden ser utilizados para criminalizar y/o vigilar a defensores y defensoras de derechos humanos en esos países.

¿Por qué los países estudiados son El Salvador, Guatemala, Honduras y Nicaragua?

Dado el contexto en el que se encuentran inmersos los países de la región, la cooperación, en sus diferentes manifestaciones, ha priorizado el apoyo a la misma, particularmente a aquellos que conforman el “Triángulo Norte”, así como a Nicaragua, disminuyendo la cooperación a Costa Rica y Panamá.

Considerando que Acceso trabaja en estos países desde el año 2007, y que las mayores preocupaciones y preguntas planteadas fueron en procesos facilitados en ellos, es que decidimos emprender esta investigación inicial, esperando ampliarla en el futuro a Costa Rica y Panamá donde también consideramos que su implementación resultaría estratégica.

Dentro de los países que mayor riesgo enfrentan en el continente, el informe de Front Line Defenders señala a Guatemala y Honduras, en cuyos casos reciben especial atención las y los defensores medioambientales y por el derecho a la tierra, las mujeres defensoras, y quienes trabajan por la defensa de la población LGBT. En todos los casos “Las amenazas de muerte fueron la violación más habitual registrada”⁴, así como se denunciaron casos de detención y hostigamiento judicial, homicidios, agresiones físicas, y campañas de estigmatización, punto en el que también se incluye a El Salvador, país en el que “instituciones como FESPAD [...] registran en el primer semestre del 2014, 9 agresiones hacia este sector.”⁵

Por nuestra experiencia de trabajo en la región, sabemos que la situación se extiende a Nicaragua, donde son particularmente perseguidas las defensoras que luchan por la equidad de género, así como las y los defensores que se oponen a la construcción del Canal Interoceánico, y a proyectos mineros u otros que afectan territorios de pueblos indígenas y afrodescendientes. Al respecto

[...] no puede obviarse las constantes amenazas y campañas de difamación y descalificación que impulsa el gobierno [...] Las amenazas, represalias, campañas de desprestigio, señalamientos, estigmatización y agresiones contra los defensores y defensoras son señales claras de la existencia de un patrón sistemático de agresión que trata de desvirtuar su labor calificándolos como opositores del gobierno y/o defensores de delinquentes.⁶

4. Front Line Defenders. “Informe 2015: Defensores/as de derechos humanos en la cuerda floja”, 5.

5. Equipo Regional de Monitoreo y Análisis de Derechos Humanos en Centroamérica. “Informe sobre Derechos Humanos y Conflictividad en Centroamérica 2013-2014”. (El Salvador: Equipo Regional de Monitoreo y Análisis de Derechos Humanos en Centroamérica, 2014), 18, <http://www.fespad.org.sv/wp-content/uploads/2015/01/Dddhh20141.pdf> (consultado: 30 noviembre 2015)

6. Equipo Regional de Monitoreo y Análisis de Derechos Humanos en Centroamérica. “Informe sobre Derechos Humanos y Conflictividad en Centroamérica 2013-2014”, 17.



¿Por qué nos referimos al derecho a la privacidad digital, en internet y en las telecomunicaciones?

Esto es para abarcar la privacidad que resguarda aquella información:

- Almacenada en nuestros dispositivos electrónicos.
- Compartida, comunicada, socializada mediante internet por correos electrónicos, llamadas online, mensajería instantánea, redes sociales, archivos compartidos, etc.
- Compartida, comunicada, socializada mediante llamadas telefónicas o mensajes de texto.

Recordemos que esta información no se refiere únicamente a lo que escribimos, diseñamos, fotografiamos, filmamos, buscamos, miramos, hablamos, es decir, al contenido de nuestras comunicaciones, sino también a todos los datos que se filtran en estas acciones concretas, conocidos como metadatos.

Metadatos

Definición	Ejemplos
Datos vinculados a las comunicaciones que no son el contenido de las mismas	Números de teléfonos de los que recibí llamadas Números de teléfonos a los que efectué llamadas Horario en que recibí y efectué esas llamadas Lugar aproximado desde el que realicé o recibí las llamadas Fecha y hora en las que envié o recibí correos electrónicos Localización desde la que me conecto a internet

Ahora bien, esta información, una vez obtenida, puede ser utilizada con un sinnúmero de intenciones, y resulta importante destacar aquellas situaciones que NO responden a los fines de esta investigación.

- Fines comerciales, es decir, no nos ocuparemos de cuando nuestro comportamiento es monitoreado por las empresas para saber qué vendernos, cómo y cuándo.
- Estafas, fraudes o privacidad bancaria.
- Difamación en línea.

Las acciones que SÍ nos interesan son aquellas ejercidas para criminalizar y/o vigilar a defensores y defensoras de derechos humanos.

La seguridad integral abarca diferentes variables, la más reconocida es la seguridad física, pero también contempla la seguridad psico-social, jurídica y la de la información y la comunicación, es decir, la SIC.

Encontramos que a través de la violación de nuestra SIC, y con ella, de nuestra privacidad en la era digital, aumenta ponencialmente la posible vulneración de la seguridad física, psico-social y/o jurídica, así por ejemplo, la vigilancia de las comunicaciones puede ser utilizada para conocer la ubicación de la persona vigilada y facilitar una amenaza o un ataque directo.



Considerando que el marco que nos guía es el de los derechos humanos, el actor sobre el que nos concentraremos es el Estado, e incluiremos a las empresas privadas únicamente cuando actúen como intermediarias del mismo.

Por ejemplo, esta investigación sí contempla una situación en la que el Estado solicite a la empresa de telefonía que le entregue los registros de nuestras llamadas, pero no abarcaría una situación en la que la empresa de telefonía utilice los registros de nuestras llamadas para saber qué plan vendernos.

Para cumplir con el objetivo general se conformó un equipo de investigación integrado por una coordinadora, una asesora en aspectos jurídicos a nivel internacional, e investigadores/as nacionales en cada uno de los países que abarca la investigación.

A su vez, el camino a seguir para alcanzar el objetivo general fue establecido en los **objetivos específicos**:

OBJETIVOS ESPECÍFICOS DE LA INVESTIGACIÓN

1. Identificar los estándares internacionales relacionados con el derecho a la privacidad digital, en internet y en las telecomunicaciones
2. Conocer los marcos legales nacionales e internacionales vigentes en El Salvador, Guatemala, Honduras y/o Nicaragua relacionados con el derecho a la privacidad digital, en internet y en las telecomunicaciones para determinar si cuentan con ambigüedades y vacíos.
3. Evaluar los marcos legales nacionales e internacionales vigentes en El Salvador, Guatemala, Honduras y/o Nicaragua relacionados con el derecho a la privacidad digital, en internet y en las telecomunicaciones para determinar su consonancia con los estándares internacionales en la materia.
4. Identificar las principales experiencias e inquietudes relacionadas con el derecho a la privacidad digital, en internet y en las telecomunicaciones del sector técnico y de defensa de derechos humanos de El Salvador, Guatemala, Honduras y/o Nicaragua para responderlas desde una perspectiva jurídica.

El presente estudio comienza con una introducción sobre el derecho a la privacidad digital, y continúa con un primer capítulo sobre estándares internacionales para la protección de este derecho, enfocándose en los estándares internacionales en materia de derechos humanos frente a la vigilancia estatal de las comunicaciones, y finalizando con los estándares internacionales vinculados al anonimato y el cifrado, y su relación con la privacidad y la libertad de expresión. Este capítulo busca instruir sobre la privacidad como derecho protegido por el derecho interno de cada país y el derecho internacional de los derechos humanos.

Posteriormente, se presenta un capítulo por país, abarcando El Salvador, Guatemala, Honduras y Nicaragua; cada uno de los cuales se encuentra dividido en apartados que responden a los objetivos específicos planteados en la investigación. De esta forma, los capítulos nacionales comienzan con una introducción en la que se presentan los antecedentes existentes sobre el tema, es decir, qué se ha investigado en el país y desde qué enfoque se ha hecho; se exponen datos sobre la brecha digital para estimar cuál es la población con acceso a internet y/o a las telecomunicaciones, y de esta manera identificar la población cuyo derecho a la privacidad en el área digital puede ser violentado; y se explica la situación de criminalización de defensores y defensoras de derechos humanos a nivel nacional.



Posteriormente, se presenta el marco legal nacional vigente en cada uno de los países, relacionado con el derecho a la privacidad digital, en internet y en las telecomunicaciones. Así, se comienza identificando los tratados internacionales ratificados para pasar a las constituciones nacionales y luego dar lugar a otras leyes, reglamentos y jurisprudencia, como por ejemplo, normas en materia penal, sobre inteligencia y contrainteligencia o aquellas que regulan el sector de telecomunicaciones. En todos los casos se repasan salvaguardas y limitaciones, particularmente relacionadas con vigilancia, anonimato, cifrado y allanamientos, y se señalan los mecanismos de acceso a la justicia.

En el tercer apartado por país se evalúa la adecuación de estos marcos legales nacionales a los estándares internacionales, particularmente a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, explicados en el primer capítulo.

En el cuarto apartado se presentan las principales experiencias e inquietudes relacionadas con el derecho a la privacidad digital, en internet y en las telecomunicaciones del sector técnico y de defensa de derechos humanos en cada país para dejarlas planteadas con el objetivo de, posteriormente, responderlas desde una perspectiva jurídica. Luego, cada capítulo por país cuenta con un apartado de conclusiones nacionales.

Finalmente, la investigación cierra con un capítulo de conclusiones comparativas sobre el derecho a la privacidad en la normativa centroamericana, exponiendo los resultados relacionados con las constituciones y con otras leyes, así como los vinculados con mecanismos de acceso a la justicia para la protección de la privacidad digital en Centroamérica y la adecuación de las normas centroamericanas a los estándares internacionales.

A efectos de este resumen, organizaremos los resultados obtenidos de la investigación, no por país, sino por temas principales.



1. El derecho a la privacidad

El derecho a la privacidad ha sido históricamente considerado uno de los derechos humanos más difíciles de definir.⁷ La falta de una definición única, sin embargo, no supone que el asunto carezca de importancia. Todo lo contrario, como ya la doctrina internacional ha señalado, “en cierto sentido, todos los derechos humanos son aspectos del derecho a la privacidad.”⁸

La conceptualización de la privacidad ha sido siempre muy debatida y estudiada. Para algunos autores, la privacidad es “el derecho a ser dejado solo (right to be left alone, en inglés).”⁹ Para otros, la clave de la privacidad es el control, el “deseo de las personas de elegir libremente en qué circunstancias, y en qué medida, van a exponer ellos mismos, su actitud y su comportamiento a los demás.”¹⁰

La doctrina jurídica diferencia distintas esferas de protección del derecho a la privacidad. En la esfera positiva toda persona tiene derecho al respeto de su vida privada. En su dimensión negativa, prohíbe la injerencia en la vida privada de una persona, sus comunicaciones, sus documentos, su familia y su domicilio.

La privacidad, como derecho humano, ha sido reconocida en los tratados internacionales de derechos humanos.¹¹ **El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP) señala que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. El artículo también exige que el Estado adopte las medidas de ley necesarias para proteger a toda persona frente a esas injerencias o ataques.**

En su Observación General N° 16 el Comité de Derechos Humanos de Naciones Unidas señaló que el término “ilegales” del artículo 17 del **PIDCP** significa que la *injerencia* autorizada por los Estados solo puede estar prescrita por ley, y que a su vez esa ley debe cumplir con las disposiciones, propósitos y objetivos del Pacto. Además, agrega que con la introducción del concepto de arbitrariedad se pretende garantizar que incluso cualquier injerencia incluida en la ley debe estar también en consonancia con las disposiciones, los propósitos y los objetivos del Pacto.¹²

El derecho a la privacidad como toda libertad fundamental no es un derecho absoluto. El Estado puede restringir esos derechos para proteger la seguridad nacional, el orden público, la salud o la moral pública y los derechos y libertades de terceros. Para ser permisibles, las restricciones deben ser previstas por la ley, deben ser necesarias y proporcionales para perseguir los fines legítimos.

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> (consultado: 16 noviembre, 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> (consultado: 16 noviembre, 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. Declaración Universal de Derechos Humanos, artículo 12, Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares, artículo 14, Convención sobre los Derechos del Niño de Naciones Unidas, artículo 16, Pacto Internacional de Derechos Civiles y Políticos artículo 17; convenciones regionales incluido artículo 10 Del Capítulo Africano Carta sobre los Derechos y el Bienestar del Niño, artículo 11 de la Convención Americana de Derechos Humanos, artículo 4 de los principios de la Unión Africana sobre la Libertad de Expresión, artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre, artículo 21 de la Declaración Derechos Humanos de la ASEAN, Artículo 21 de la Carta Árabe de Derechos Humanos, y artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; Principios de Johannesburgo sobre la Seguridad Nacional, Expresión y Acceso a la Información, Principios de Camden para la Libertad de Expresión y la Igualdad Libre.

12. Naciones Unidas, Observación general N° 16, Derechos de la privacidad (artículo 17), 35° período de sesiones (1988), HRI/GEN/1/Rev.9 (Vol.I), 228, <http://www1.umn.edu/humanrts/hrcommittee/Sgencom16.html> (consultado: 16 noviembre, 2015)



2. El derecho a la privacidad en las constituciones centroamericanas

Las Constituciones de las Repúblicas de Guatemala, El Salvador, Nicaragua y Honduras protegen el derecho a la privacidad. La protección constitucional de este derecho se encuentra dispersa en artículos de la Constitución y jurisprudencia de la Corte Constitucional. Ellos protegen distintos aspectos del derecho a la privacidad como el derecho a la intimidad, el derecho a la vida privada, la inviolabilidad de las comunicaciones, documentos y domicilio, la autodeterminación informativa, la protección de datos o la garantía de habeas data.

2.1. Derecho a la intimidad y la vida privada

La Constitución salvadoreña garantiza expresamente el derecho a la intimidad personal y familiar y a la propia imagen en su artículo 2. La Sala de lo Constitucional de la Corte Suprema de Justicia de ese país ha desarrollado el contenido de este derecho definiéndolo como un derecho fundamental:

Un derecho fundamental estatuido directamente en el artículo 2 inciso segundo de la Constitución, del que son titulares todas las personas, consistente en la preservación de la esfera estrictamente interna y de la privada (que incluye a la familia) frente a intromisiones no consentidas del Estado o de otros particulares. Por tanto, la violación por excelencia – no única- en la dinámica de las sociedades actuales al derecho a la intimidad, es la obtención y/o revelación indeseada por parte de terceros, de datos o informaciones comprendidas en dichas esferas.¹³

En Honduras, tanto la Constitución como la jurisprudencia se refieren al derecho a la intimidad. La Sala de lo Penal de la Corte Suprema define la esfera positiva del derecho a la intimidad “como el derecho de la persona de controlar a su arbitrio la información de índole personal que desee sea conocida y determinar la identidad y el número de personas que desee tengan acceso a ella”, mientras que la misma decisión define su esfera negativa “como el derecho de toda persona a no sufrir o tolerar injerencias de terceros en la vida privada personal y familiar y de rechazar cualquier intento de ello”.¹⁴ La Sala hondureña además señala que entre las múltiples esferas del derecho a la intimidad se encuentran:

sus comunicaciones, mismas que modernamente puede realizar a través del [...] correo electrónico, telefax, teléfono y cualquier otro medio material, electrónico o telemático que permita la comunicación reservada entre dos o más personas a través de texto, audio, imágenes o video, mismas que son de carácter inviolable sin importar lo banal, trivial o insignificantes que puedan ser las comunicaciones [...].¹⁵

Igualmente, la Constitución de Guatemala¹⁶ establece la obligación de respetar la dignidad, intimidad y decoro de las personas ante los registros personales. La Corte Constitucional de este país expuso que el elemento central de protección es la vida privada y su protección frente a injerencias e intromisiones arbitrarias o ilegales.¹⁷

13. Sala de lo Constitucional. Corte Suprema de Justicia de Honduras, Sentencia de Inconstitucionalidad 91- 2007 del 24 de septiembre de 2010.

14. Sala de lo Penal. Corte Suprema de Justicia, Sentencia número CP-48-2011, 20, <http://www.poderjudicial.gob.hn/Jurisprudencia/Documents/CP-48-2011.pdf> (consultado: 16 noviembre, 2015)

15. Sala de lo Penal de la Corte Suprema de Justicia, Sentencia número CP-48-2011, 20.

16. Guatemala “Constitución Política de Guatemala” Asamblea Nacional Constituyente (1985), artículo 25.

17. Corte de Constitucionalidad. *Inconstitucional GENERAL TOTAL. Expediente 1201-2006*. (Guatemala, 2007)



Por su parte, la Constitución Política de Nicaragua reconoce el derecho a la vida privada y a la de su familia.¹⁸ Conforme al artículo 27 de la Constitución, este derecho aplica tanto para las personas nicaragüenses como para las extranjeras, pues se trata de un derecho estrictamente vinculado a la propia persona, siendo la única limitación el ejercicio de los derechos políticos.¹⁹

Podemos entonces argumentar que el derecho a la intimidad está expresamente recogido a nivel constitucional en estos cuatro países centroamericanos y que los tribunales constitucionales han desarrollado el contenido del derecho en su esfera negativa (injerencia arbitrarias en la vida privada) y positiva (el derecho al respeto de su vida privada).

2.2. Inviolabilidad de las comunicaciones, documentos y domicilio

En las constituciones centroamericanas, el derecho a la inviolabilidad de las comunicaciones y el domicilio es un derecho diferente pero vinculado al derecho a la intimidad. La esencia del derecho es proteger las comunicaciones de una persona, su lugar de residencia u oficina frente a injerencias arbitrarias a la vida privada de las personas y la obligación de las demás de no transgredirlo, incluido el Estado.

La Constitución de El Salvador reconoce expresamente el derecho de protección de la morada y la protección de la correspondencia y telecomunicaciones.²⁰ De la misma manera, la Constitución de Nicaragua reconoce el derecho a la inviolabilidad del domicilio, correspondencia y comunicaciones de todo tipo.²¹

En la Constitución guatemalteca, el derecho a la intimidad fue un derecho reconocido desde la Constitución Federal de 1823, el cual estipulaba el carácter privado de la correspondencia y los documentos y autorizaba ciertas limitaciones al derecho.²² Ese reconocimiento fue luego tomado por la Constitución Federal de Centroamérica de 1824, y su reforma de 1835.²³ Sin embargo, no fue hasta 1879 que la Constitución guatemalteca admitió expresamente la inviolabilidad de los documentos y correspondencia, dejando claro que este derecho solo puede limitarse por medio de juez competente y conforme a los procedimientos que establezca la ley.²⁴

Actualmente, la Constitución vigente de Guatemala reconoce expresamente la inviolabilidad de la vivienda²⁵ y la inviolabilidad de la correspondencia, documentos y libros.²⁶ En el 2007, la Corte Constitucional de este

18. Nicaragua "Constitución Política de Nicaragua" ASAMBLEA NACIONAL (1948), artículo 26.

19. Información tomada del capítulo "Nicaragua" de esta misma publicación, escrito por Mireya Zepeda Rivera.

20. Artículo 23: La correspondencia de toda clase es inviolable, interceptada no hará fe ni podrá figurar en ninguna actuación, salvo en los casos de concurso y quiebra. Se prohíbe la interferencia y la intervención de las comunicaciones telefónicas. De manera excepcional podrá autorizarse judicialmente de forma escrita y motivada. La intervención temporal de cualquier tipo de telecomunicaciones preservándose en todo caso el secreto de lo privado que no guarde relación con el proceso o la información proveniente de una intervención ilegal carecerá de valor (...)El Salvador "Constitución de la República" Asamblea Legislativa (1983),

21. Guatemala "Constitución Política de Guatemala" Asamblea Nacional Constituyente (1985), artículo 26.

22. Información tomada del capítulo "Guatemala" de esta misma publicación, escrito por Hedme Sierra-Castro y Jorge Jiménez.

23. Información tomada del capítulo "Guatemala" de esta misma publicación, escrito por Hedme Sierra-Castro y Jorge Jiménez.

24. Guatemala "Ley Constitutiva de la República de Guatemala" (1879), artículo 37. "La correspondencia de toda persona y sus papeles privados son inviolables. Sólo por auto de juez competente podrá detenerse la primera y aun abrirse, ocuparse los segundos, en los casos y con las formalidades que la ley exige."

25. Artículo 23: Inviolabilidad de la vivienda. La vivienda es inviolable. Nadie podrá penetrar en morada ajena sin permiso de quien la habita, salvo por orden escrita de juez competente en la que se especifique el motivo de la diligencia y nunca antes de las seis ni después de las dieciocho horas. Tal diligencia se realizará siempre en presencia del interesado, o de su mandatario. Guatemala "Constitución Política de Guatemala"

26. Artículo 24: Inviolabilidad de correspondencia, documentos y libros. La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna. Los libros, documentos y archivos que se



país dejó claro que el derecho a la inviolabilidad de la correspondencia protege la intimidad de las personas frente a las injerencias en sus vidas privadas y solo puede limitarse por necesidades sociales e interés público.²⁷

Por su parte, la Constitución y la jurisprudencia de Honduras también protegen la inviolabilidad del domicilio²⁸ y de las comunicaciones.²⁹ Sobre este último derecho, la Sentencia CP-48-2011 de la Sala de lo Penal de la Corte Suprema de Justicia de Honduras definió qué debemos entender por el derecho a la inviolabilidad de las comunicaciones privadas:

aquel que derivado del derecho a la vida privada, prohíbe a los particulares ajenos a la comunicación y principalmente al Estado: el secuestro, la captación, interceptación, apertura, grabación, reproducción o divulgación de una comunicación de carácter privada, sea que dichas acciones se realicen al momento en que la comunicación se esté llevando a cabo (en tiempo real), sea que se realice ex post facto o sea que se realice donde conste el registro de la comunicación, como ser materialmente las cartas, dispositivos de teléfonos o computadoras, o electrónicamente en las cuentas personales de e-mails, buzones de redes sociales, chats, etc. La inviolabilidad de las comunicaciones incluyen la protección de los registros que llevan las empresas públicas o privadas que proporcionan servicios de comunicación y que solo pueden ser utilizados para efectos contables.³⁰

2.3. Autodeterminación informativa

El derecho a la autodeterminación informativa nace en Alemania en 1983 tras una demanda a un proyecto sobre un censo poblacional que permitía procesar los datos personales de miles de alemanes. El Tribunal Alemán afirmó que las nuevas tecnologías eran capaces de procesar los datos de tal manera que se lograba una imagen total y pormenorizada de la persona respectiva, incluso en el ámbito de su intimidad, convirtiendo al ciudadano en un “hombre de cristal”.³¹ El tribunal concluyó que el “derecho general de la personalidad abarca la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida.”³² Los datos personales generalmente se entienden como aquellos datos que pueden identificar o llegar a identificar a una persona determinada.

relacionan con el pago de impuestos, tasa, arbitrios y contribuciones, podrán ser revisados por la autoridad competente de conformidad con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas, con excepción de los balances generales, cuya publicación ordene la ley. Los documentos o informaciones obtenidas con violación de este artículo no producen fe ni hacen prueba en juicio. Guatemala “Constitución Política de Guatemala”

27. Corte de Constitucionalidad. *Inconstitucionalidad General Parcial*. Expediente 2622-2006. (Guatemala, 2007), <http://vlex.com/vid/-423703874> (consultado: 16 noviembre, 2015)

28. Artículo 99: El domicilio es inviolable. Ningún ingreso o registro podrá verificarse sin consentimiento de la persona que lo habita o resolución de autoridad competente. No obstante, puede ser allanado, en caso de urgencia, para impedir la comisión o impunidad de delitos o evitar daños graves a la persona o a la propiedad. Exceptuando los casos de urgencia, el allanamiento del domicilio no puede verificarse de las seis de la tarde a las seis de la mañana, sin incurrir en responsabilidad. La ley determinará los requisitos y formalidades para que tenga lugar el ingreso, registro o allanamiento, así como las responsabilidades en que pueda incurrir quien lo lleve a cabo. Honduras “Constitución de la República” La Gaceta o. 23, 612 (20, enero 1982)

29. Artículo 100: Toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial. Honduras “Constitución de la República”

30. Sala de lo Penal. Corte Suprema de Justicia, Sentencia número CP-48-2011, 20.

31. Ver: Observatorio Iberoamericano de Protección de Datos <http://oiprodat.com/2013/03/15/configuracion-juridica-del-derecho-a-la-autodeterminacion-informativa/>

32. Alemania, Sentencia del 15 de Diciembre 1983. Ley del Censo. Derecho a la personalidad y dignidad humana.



En Honduras, la Constitución no reconoce expresamente el derecho a la protección de datos o la autodeterminación informativa. Sin embargo, su protección se encuentra recogida a través de la garantía constitucional del *habeas data*, mismo que existe a partir de 2013.³³

Artículo 182. El Estado reconoce el derecho [...] de Hábeas Data. [...] únicamente puede promover la acción la persona cuyos datos personales o familiares consten en archivos, registros públicos o privados de la manera siguiente: [...] 2) Toda persona tiene el derecho de acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados, y en caso de que fuere necesario, actualizarla, rectificarla y-o enmendarla.

En Guatemala, la Constitución no protege expresamente la protección a los datos personales. Sin embargo, la Corte de Constitucionalidad ha definido qué es un dato personal y reconocido los derechos a actualizar sus datos, rectificarlos si son erróneos, a mantenerlos en reserva o confidencialidad y a excluirlos de determinada información que pueda considerarse sensible para el interesado.³⁴

En Nicaragua, la protección de datos personales se encuentra recogida en la garantía constitucional establecida en el artículo 26.3 de la Constitución Política de ese país, que determina que toda persona tiene derecho a conocer toda información personal que sobre ella se haya registrado en las entidades de naturaleza privada y pública, así como el derecho de saber por qué y con qué finalidad se tiene dicha información.³⁵

La jurisprudencia constitucional sí reconoce la autodeterminación informativa y establece de manera supletoria al recurso de amparo como mecanismo de garantía constitucional ante la ausencia de *Habeas Data*.³⁶

2.4. El derecho al buen nombre y al honor

El derecho al buen nombre, honor u honra reconoce que toda persona debe gozar de la reputación que ha construido socialmente frente a otros. Este derecho tiene dos aspectos: el buen nombre y el honor u honra. El primero se relaciona con la reputación que tiene el individuo.³⁷ El segundo consiste en reconocer la dignidad que merece como ser humano por parte de los demás miembros de la sociedad.

En el contexto de la vigilancia, estos derechos pueden verse vulnerados cuando el contenido de las comunicaciones electrónicas, ilícitamente obtenidas, son hechas públicas de forma tal que afecten el honor o la buena reputación de los titulares de la información privada que se hace pública.

Si bien países en Centroamérica reconocen expresamente este derecho,³⁸ tanto este desarrollo como las tensiones entre el derecho a la privacidad y la libertad de expresión están fuera del alcance de la presente investigación.

33; Honduras "Reforma a la Constitución de la República", decreto 237-2012 del 23 de enero de 2011, https://www.oas.org/dil/esp/Constitucion_de_Honduras.pdf (consulta: 16 noviembre, 2015)

34. Información tomada del capítulo "Guatemala" de esta misma publicación, escrito por Hedme Sierra-Castro y Jorge Jiménez.

35. Información tomada del capítulo "Nicaragua" de esta misma publicación, escrito por Mireya Zepeda Rivera.

36. Información tomada del capítulo "El Salvador" de esta misma publicación, escrito por Marlon Hernández Anzora

37. Sentencia C-489/02: la Corte Constitucional de Colombia define este derecho como: "el derecho al buen nombre, como expresión de la reputación o la fama que tiene una persona, se lesiona por las informaciones falsas o erróneas que se difundan sin fundamento y que distorsionan el concepto público que se tiene del individuo.

38. Nicaragua "Constitución Política de Nicaragua" Asamblea Nacional (1948), artículo 26,



3. El derecho a la privacidad digital en otras leyes centroamericanas

En Centroamérica no existe un solo cuerpo legislativo que contenga toda normativa que autorice la actividad de vigilancia por parte del Estado. Estas se encuentran dispersas entre la Constitución, decisiones judiciales y leyes. Asimismo, las garantías legales que protegen a las personas frente a la interferencia con el derecho a la privacidad y libertad de expresión se encuentran también dispersas, entre Constitución, leyes e incluso tratados internacionales.

En todos los países, además de la Constitución, podemos identificar como fuentes relevantes para la protección, criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos los siguientes instrumentos jurídicos:

- Código Penal
- Código Procesal Penal
- Ley de Acceso a la Información Pública
- Ley de Telecomunicaciones

En los ordenamiento de los cuatro países en estudio, el Código Procesal Penal (CPP) regula la intervención de las comunicaciones.

Por ejemplo, en **Nicaragua**, el CPP establece que procederá la interceptación de comunicaciones telefónicas o de otras formas de telecomunicaciones cuando se trate de terrorismo; secuestro extorsivo; tráfico de órganos y de personas con propósitos sexuales; delitos relacionados con estupefacientes, psicotrópicos y otras sustancias controladas; legitimación de capitales o lavado de dinero y activos, y tráfico internacional de armas, explosivos y vehículos robados. En estos casos la solicitud debe provenir del Fiscal General de la República o del Director General de la Policía Nacional y será autorizada por juez competente.³⁹

En **Guatemala**, el Código Procesal Penal establece que se podrá ordenar la interceptación y el secuestro de la correspondencia (postal, telegráfica o tele-tipográfica) dirigida al imputado o remitida por él, bajo una orden expedida por el juez. En este caso, el contenido será enviado al tribunal competente, y una vez recibida la correspondencia interceptada, el tribunal abrirá la correspondencia, haciendo constar en acta todas las diligencias actuadas.⁴⁰

El Código Procesal Penal **salvadoreño** establece que cuando se requiera intervenir las telecomunicaciones de una persona que está siendo investigada o procesada, deberán cumplir con las respectivas garantías constitucionales y el debido proceso para que esta información pueda ser incorporada en un proceso judicial y constituyan prueba (Art. 176).⁴¹

Más específicamente, en el caso de **Guatemala**, la mayor parte de la regulación relacionada con intervención de las comunicaciones se encuentra en la Ley Contra la Delincuencia Organizada y en la Ley de la Dirección General de la Inteligencia Civil, en la que se aclara que se pueden intervenir las comunicaciones en activ-

39. Información tomada del capítulo "Nicaragua" de esta misma publicación, escrito por Mireya Zepeda Rivera.

40. Guatemala "Código Procesal Penal" Organización de los Estados Americanos(1992), artículos 203, 204, 205, http://www.cicad.oas.org/fortalecimiento_institucional/legislations/PDF/GT/decreto_congresional_51-92_codigo_procesal_penal.pdf (consultado: 01 diciembre, 2015)

41. El Salvador "Código Procesal Penal" Asamblea Legislativa (2009), artículo 176.



idades del crimen organizado con énfasis en la narcoactividad y en la delincuencia común cuando hubiera peligro para la vida, la integridad física, la libertad, y los bienes de personas determinadas. Una diferencia importante entre ambos tipos de intervención es que la información recogida mediante la Ley de Inteligencia solo tiene carácter preventivo, por lo que no podrá ser utilizada como prueba.⁴²

En ambos casos, la solicitud solo puede realizarla el Ministerio Público, y para la Ley contra la Delincuencia Organizada la autorización será dada por los jueces de primera instancia del ramo Penal, mientras que para la aplicación de la Ley de Inteligencia la autorización estará a cargo de una Sala de la Corte de Apelaciones.

Tanto en **El Salvador** como en **Honduras** encontramos una ley que regula muy específicamente la limitación del derecho a la privacidad mediante la vigilancia estatal, nos referimos a la Ley para la Intervención de las Comunicaciones,

En **Honduras**, en **enero de 2011**, con la entrada en vigencia de la Ley de Intervención de las Comunicaciones Privadas, se derogaron las normas del Código Procesal Penal sobre intervención de las comunicaciones. Esta nueva ley tiene por finalidad “establecer el marco legal de regulación procedimental de la intervención de las comunicaciones”⁴³ y constituir “una herramienta esencial en la lucha contra la criminalidad tradicional, y sobre todo contra la criminalidad organizada o no convencional”;⁴⁴ es decir que la ley tiene aplicabilidad en la investigación de cualquier delito.⁴⁵

En **El Salvador** se especifica que podrá hacerse uso de la facultad de la ley en un listado que incluye 14 delitos⁴⁶, más todos los delitos previstos en la misma ley, más todos los delitos conexos con cualquiera de los anteriores, por lo que su aplicabilidad también es muy amplia.⁴⁷

En ambos casos, se regula la intervención de:

Cualquier tipo de transmisión, emisión, recepción de signos, símbolos, señales escritas, imágenes, correos electrónicos, sonidos o información de cualquier naturaleza por hilos, radioelectricidad, medios ópticos u otro sistema electromagnético, quedando comprendidas las realizadas por medio de telefonía, radiocomunicación, telegrafía, medios informáticos o telemáticos, o de naturaleza similar.

42. Información tomada del capítulo “Guatemala” de esta misma publicación, escrito por Jorge Jiménez Barillas y Hedme Sierra-Castro.

43. El Salvador “Ley Especial para la Intervención de las Comunicaciones” Asamblea Legislativa (2010), artículo 1.

44. El Salvador “Ley Especial para la Intervención de las Comunicaciones”, artículo 1.

45. Información tomada del capítulo “Honduras” de esta misma publicación, escrito por Edy Tábora Gonzales.

46. El Art. 5 regula de manera taxativa en que delitos únicamente se podrá hacer uso de la facultad de intervención: 1) Homicidio y su forma agravada. 2) Privación de libertad, Secuestro y Atentados contra la Libertad Agravados. 3) Pornografía, Utilización de personas menores de dieciocho años e incapaces o deficientes mentales en pornografía, y Posesión de pornografía. 4) Extorsión. 5) Concusión. 6) Negociaciones Ilícitas. 7) Cohecho Propio, Impropio y Activo. 8) Agrupaciones Ilícitas. 9) Comercio de Personas, Tráfico Ilegal de Personas, Trata de Personas y su forma agravada. 10) Organizaciones Internacionales delictivas. 11) Los delitos previstos en la Ley Reguladora de las Actividades Relativas a las Drogas. 12) Los delitos previstos en la Ley Especial contra Actos de Terrorismo. 13) Los delitos previstos en la Ley contra el Lavado de Dinero y de Activos. 14) Los delitos cometidos bajo la modalidad de crimen organizado en los términos establecidos en la ley de la materia. 15) Los delitos previstos en la presente Ley. 16) Los delitos conexos con cualquiera de los anteriores.

47. Información tomada del capítulo “El Salvador” de esta misma publicación, escrito por Marlon Hernández Anzora.



En el caso de Honduras se agrega “así como la comunicación que se efectúe a través de cualquier medio o tipo de transmisión”.

En El Salvador, el Fiscal General de la República será la única autoridad facultada para solicitar la intervención de las telecomunicaciones directamente o a través del Director del Centro de Intervención, y en Honduras la solicitud puede ser realizada por el Ministerio Público, el Procurador Privado a través de este y por la Procuraduría General de la República, y la misma será autorizada por los órganos jurisdiccionales en materia Penal, sean nacionales o seccionales, a diferencia de El Salvador, donde la autorización será dada por cualquiera de los jueces de instrucción con residencia en la capital del país.

En ambos países, las leyes coinciden en establecer como principios para la intervención de las comunicaciones:

- Jurisdiccionalidad
- Proporcionalidad
- Confidencialidad
- Temporalidad

En Honduras se agrega el principio de necesidad e idoneidad, mientras que en El Salvador se incluye la limitación subjetiva.

Por otro lado, en **Nicaragua** destaca la Ley de Protección de Datos Personales, que no encontramos en ninguno de los otros países, y que en Honduras actualmente solo es un anteproyecto; asimismo, también es importante destacar el recurso de *habeas data*.

En Nicaragua, a raíz del Caso Infortnet en el que, sin consentimiento de las personas, se obtenían datos sobre su solvencia económica y se comercializaban a empresas para que estas ofreciesen sus productos, se decidió aunar esfuerzos y legislar sobre el tema de la protección de datos personales. De esta forma, en el año 2012 se aprueba la Ley de Protección de Datos Personales⁴⁸, que tiene por objeto la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa.⁴⁹

La Ley de Protección de Datos Personales, en su artículo 8, determina cuatro categorías de datos personales:

- Datos personales sensibles
- Datos personales relativos a la salud
- Datos personales informáticos
- Datos personales comerciales

Datos personales informáticos:

Son los datos personales tratados a través de medios electrónicos o automatizado, Cada una de estas categorías tendrá diferentes características y su recolección y procesamiento girará en dependencia del caso.

48. Nicaragua “Ley de Protección de Datos Personales” La Gaceta No. 61 (2012)

49. Nicaragua “Ley de protección de datos personales”, artículo 1.



Aunado a esto, para garantizar el resguardo y protección de los datos personales, en el año 2013 se reforma la Ley de Amparo⁵⁰ en la que se adiciona el recurso de habeas data con el objetivo de evitar la publicidad ilícita de los mismos; en dicho recurso se contempla el derecho de exigir de parte agraviado y/o agraviada que la información sea modificada, bloqueada, actualizada e incluso eliminada, cuando la misma se relacione con datos personales sensibles y se presuma falsedad, inexactitud o la ilegalidad en el acceso de la información, o cuando se trate de información que lesione los derechos constitucionales. La reforma a la Ley de Amparo establece que el recurso de habeas data,

...se crea como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya una invasión a la privacidad personal y tenga relevancia con el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar.⁵¹

El recurso de *habeas data* hace referencia al derecho legítimo del individuo a “la libre disposición de los datos personales”⁵². Esto significa tener el control como individuo sobre el uso y manejo de los datos personales propios que han sido almacenados en distintos lugares; en otras palabras, el ejercicio de la libertad informativa consiste en tener la capacidad de controlar la información que nos concierne. En concreto, existen dos vías de controlar esta información, por un lado, consintiendo explícita e individualmente la captación y el tratamiento de los datos por terceros y, por otro lado, por aquella autorización regida por ley. Sin embargo, ni el consentimiento ni la habilitación legal suponen la pérdida del poder sobre los datos, ya que existe una serie de derechos que complementa la autodeterminación informativa⁵³ (derecho de cancelación del tratamiento de datos personales, derecho de rectificación de los datos que no sean exactos, derecho a ser informado de la recogida de datos personales, derecho de acceso a los datos personales recogidos, entre otros).⁵⁴

4. Mecanismos de acceso a la justicia para la protección de la privacidad digital en Centroamérica

En todos los países existen dos mecanismos fundamentales de acceso a la justicia en el contexto de la vigilancia por violación de derechos fundamentales: el recurso de amparo y el recurso de inconstitucionalidad.

En Honduras se suma el recurso de *habeas data*, cuya finalidad es que la información se pueda actualizar, rectificar y/o suprimir

En esta misma línea, en Nicaragua en el año 2013 se integra el recurso de habeas data como mecanismo de protección frente a la violación del derecho a la autodeterminación informativa y protección de datos personales, siendo el derecho que asiste a toda persona en caso de:

1. Negarse el responsable del fichero a revelar la información solicitada por el ciudadano, este está legitimado a interponer la acción dirigida a la exhibición de los registros, públicos o privados, en los

50. Nicaragua “Ley de Amparo” La Gaceta del 08, abril 2013.

51. Nicaragua “Ley de Amparo” artículo 6.

52. Osvaldo Alfredo Gozaíni, “Hábeas Data. Protección de los datos personales. Doctrina y Jurisprudencia”. (Argentina: Rubinzal Culzoni Editores, 2011), 67.

53. Pablo Lucas Murillo de la Cueva, “Perspectivas del derecho a la autodeterminación informativa”. Revista de Internet, Derecho y Política, 5, (2007): 18-32.

54. Información tomada del capítulo “Nicaragua” de esta misma publicación, escrito por Mireya Zepeda Rivera.



cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud.

2. Oponerse el titular del fichero a suprimir, rectificar o actualizar los datos personales, la acción va encaminada a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación, por ejemplo, afiliación a partido político, creencia religiosa, etcétera.

Que el responsable del fichero de datos se niegue a proveer al ciudadano el derecho de oponerse a figurar en ficheros de datos, aun cuando los datos hayan sido recabados de fuentes accesibles al público⁵⁵.

5. Adecuación de las normas centroamericanas a los estándares internacionales

Los más altos estándares de protección del derecho a la privacidad en relación con la vigilancia de las comunicaciones, reconocidos en la jurisprudencia y doctrina de los órganos de protección internacional de derechos humanos y los tribunales constitucionales alrededor del mundo, han sido recogidos para elaborar los “Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones”, en adelante los 13 Principios.⁵⁶

Los 13 Principios son una propuesta novedosa, producto de una consulta global con grupos de la sociedad civil y expertos internacionales en temas de privacidad, tecnología y vigilancia de las comunicaciones, y están firmemente enraizados en el derecho internacional de los derechos humanos y la jurisprudencia comparada. Su objetivo es proporcionar a grupos de la sociedad civil, funcionarios públicos, jueces y órganos legislativos un marco para evaluar si las leyes o prácticas de vigilancia son compatibles con los estándares internacionales de derechos humanos.⁵⁷

Los 13 Principios han sido citados en el informe del Grupo de Revisión del presidente de los Estados Unidos sobre Inteligencia y Tecnologías de las Comunicaciones,⁵⁸ el informe de la Comisión Interamericana de Derechos Humanos,⁵⁹ el Reporte sobre Anonimato y Cifrado del Relator sobre Libertad de Expresión de Naciones Unidas,⁶⁰ y el Reporte de Privacidad en la Era Digital del Alto Comisionado de Derechos Humanos de Naciones Unidas,⁶¹ entre otros.

55. Jovanka Durón Chow. “Los ataques de la informática y la protección de datos personas en Nicaragua”. Revista Encuentro, No. 71, (2005),15-16.

56. Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Accesible en: <https://es.necessaryandproportionate.org/text>

57. Para una descripción de cada uno de los principios y su fundamento como instrumento del derecho internacional de derechos humanos, ver el capítulo de Estándares Internacionales de Derechos Humanos. Katitza Rodríguez, Estándares Internacionales de Derechos Humanos en Materia de Privacidad.

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

59. Comisión Interamericana de Derechos Humanos. Relatoría Especial para la Libertad de Expresión, Libertad de Expresión e Internet. Resolución OEA/Ser.L/V/II.CIDH/RELE/INF.11/13, 31 de diciembre de 2013, párr. 15 y 16, http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf (consultado: 14 abril, 2015)

60. Naciones Unidas. Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión. Resolución A/HRC/29/32, 22 de mayo de 2015, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc, (consultado: 14 septiembre, 2015)

61. Naciones Unidas. Asamblea General. El derecho a la privacidad en la era digital. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, resolución, A/HRC/27/37, 30 de junio de 2014, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_sp.doc



En cada uno de los países los estándares internacionales son respetados en diferentes grados, pero en ninguno de ellos puede afirmarse que sean incorporados en su totalidad.

En **El Salvador** existe un marco jurídico (constitucional, legislación secundaria, tratados suscritos, jurisprudencia) con importantes garantías, muchas de ellas en concordancia con los estándares internacionales de derechos humanos aplicables en contextos de vigilancia de las telecomunicaciones. A pesar de ello, hay una fragilidad institucional y una coyuntura político-social que permite que -a pesar de tener un marco jurídico que establece garantías- muchas de estas normas puedan ser perfectamente irrespetadas, burladas o desconocidas por quienes detentan poder público.⁶²

Por otra parte, la discusión sobre las nuevas tecnologías de la información y la comunicación es aún muy preliminar y no prioritaria en el país, haciendo que la novedosa propuesta de estándares internacionales prácticamente sea desconocida. Esto a raíz de que ni siquiera está abierto un debate en la opinión pública sobre vigilancia en las telecomunicaciones. A pesar de la aprobación y entrada en vigor de la Ley de Intervención a las Comunicaciones, el debate sobre el respeto de la legalidad y los derechos fundamentales en la aplicación de esta es francamente menor, existiendo muy poco control ciudadano de parte de los medios y de las organizaciones de defensa de derechos humanos en este aspecto.⁶³

A pesar de contar con importantes leyes a favor de la transparencia como la Ley de Acceso a la Información Pública (LAIP), existe aún una cultura de secretismo y arbitrariedad arraigada en las instituciones y funcionarios públicos, lo cual permite que existan ciertas normativas de carácter secreto que significan una afrenta no solo a los principios internacionales de legalidad y transparencia, sino también a las garantías constitucionales en la formación de ley según la Constitución de la República.⁶⁴

Cualquier limitación que se haga al derecho a la privacidad de las comunicaciones únicamente puede realizarse por medio de una ley clara y precisa, conforme a las obligaciones internacionales suscrita por los cuatro Estados materia de esta investigación. Analizando estas obligaciones, en el caso de Guatemala, notamos que la Ley Contra la Delincuencia Organizada no es clara ni precisa respecto al tipo de comunicaciones que se pueden interceptar, y la Ley de la Dirección General de Inteligencia Civil guatemalteca tampoco es clara ni precisa sobre las causales y formalidades legales que se deben cumplir.⁶⁵

En consonancia con lo anterior, las leyes que establezcan medidas de vigilancia deben perseguir objetivos legítimos en una sociedad democrática. Las leyes guatemaltecas que limitan el derecho a la privacidad de las comunicaciones deben utilizarse únicamente cuando sea estrictamente necesario y de manera proporcional con respecto al objetivo que se persigue. A pesar de esto, la Ley Contra la Delincuencia Organizada, la Ley de la Dirección General de Inteligencia Civil y el Código Procesal Penal no cumplen a cabalidad con los principios de necesidad, idoneidad y proporcionalidad, y por ello deben ser reformadas.⁶⁶

Por otra parte, a las personas que se les está limitando su derecho a la privacidad se les debe respetar el debido proceso, lo cual incluye ser notificadas de ello. Para asegurar que el abuso de parte de las autoridades

62. Información tomada del capítulo "El Salvador" de esta misma publicación, escrito por Marlon Hernández Anzora.

63. Información tomada del capítulo "El Salvador" de esta misma publicación, escrito por Marlon Hernández Anzora.

64. Información tomada del capítulo "El Salvador" de esta misma publicación, escrito por Marlon Hernández Anzora.

65. Información tomada del capítulo "Guatemala" de esta misma publicación, escrito por Jorge Jiménez Barillas y Hedme Sierra-Castro.

66. Información tomada del capítulo "Guatemala" de esta misma publicación, escrito por Jorge Jiménez Barillas y Hedme Sierra-Castro.



sea el mínimo, se debe contar con transparencia en las estadísticas de las limitaciones a este derecho y con verdaderos mecanismos independientes de supervisión.⁶⁷

En el caso de **Honduras**, la Ley Especial de Intervención a las Telecomunicaciones cuenta con normas restrictivas ambiguas y abiertas que permiten solicitudes de vigilancia en internet y en las telecomunicaciones por cualquier delito y, lo más grave, sin necesidad de un peso probatorio para valorar la necesidad y proporcionalidad de la intervención; incluso la ley prevé la intervención cuando se sospecha que la persona investigada ha participado en la comisión de un delito; además, sumamos la no independencia del órgano jurisdiccional que autoriza las vigilancias, por lo que con normas ambiguas y abiertas y sin controladores públicos independientes, existe un ancho margen para la discrecionalidad en la interpretación del vigilante. Esta misma ley incorpora algunos de los principios establecidos en los estándares internacionales relacionados a la privacidad en materia de actividades de vigilancia como por ejemplo la proporcionalidad, necesidad y el de autoridad jurisdiccional autorizante, sin embargo pierden su contenido cuando otras normas los contradicen o no se cuenta con mecanismos de control y supervisión de la actividad de vigilancia, por lo que no hay cumplimiento de los estándares ya sea por una omisión o por incorporación inadecuada.⁶⁸

En **Nicaragua**, la adecuación de la normativa nacional respecto a los estándares internacionales en el contexto de la privacidad digital es un desafío. La falta de voluntad política, de garantías judiciales, centralización del poder y la criminalización de la defensa de derechos humanos son características del actual gobierno de Nicaragua que constantemente son mencionadas por el sector civil del país. A pesar de haberse normado y legislado en materia de protección de datos personales durante el año 2012, la inexistencia de instituciones que den cumplimiento a los procedimientos que dicha norma manda a crear resulta un indicador de precariedad de acceso a la justicia en Nicaragua.⁶⁹

6. Experiencias e inquietudes del sector técnico y de defensa de derechos humanos

Para alcanzar el objetivo de identificar las principales experiencias e inquietudes relacionadas con el derecho a la privacidad digital, en internet y en las telecomunicaciones del sector técnico y de defensa de derechos humanos, se realizaron entrevistas y grupos focales.

Las experiencias, opiniones y dudas presentadas surgen de personas que trabajan en la defensa de derechos humanos, lo cual las convierte en actores válidos para hablar sobre sus experiencias en cuanto a vigilancia y criminalización por medio de internet y las telecomunicaciones. Sin embargo, por el tipo de metodología utilizada no podemos hacer generalizaciones a partir de sus respuestas, sino más bien plantearlas como lo que son: experiencias, dudas y percepciones que viven de primera mano personas en el ejercicio de la defensa de derechos humanos en el país.

Experiencias

En el plano de la vigilancia, en **El Salvador**, las intervenciones telefónicas hacia opositores políticos y defensores de derechos humanos vienen dándose desde el conflicto armado en el país, y la preocupación por la

67. Información tomada del capítulo “Guatemala” de esta misma publicación, escrito por Jorge Jiménez Barillas y Hedme Sierra-Castro.

68. Información tomada del capítulo “Honduras” de esta misma publicación, escrito por Edy Tábora Gonzales.

69. Información tomada del capítulo “Nicaragua” de esta misma publicación, escrito por Mireya Zepeda Rivera.



intervención en sus telecomunicaciones ha aumentado debido a la actual lógica *manodurista* en la gestión de las políticas de seguridad pública, bajo la cual este tipo de invasiones a la privacidad podría ser normalizado o visto como necesario no solo por parte de los funcionarios públicos, sino también por parte de la ciudadanía.

En **Honduras** la actual situación de vigilancia en internet y en las comunicaciones comenzó con el golpe de Estado en el año 2009, sobre todo la vigilancia selectiva hacia opositores políticos y defensores/as de derechos humanos, la cual es agudizada en momentos cercanos a las votaciones populares, en discusiones de leyes importantes y en momentos de protestas.

En ambos países se identifican experiencias como *hackeos* e intentos de *hackeo* de cuentas de correo y redes sociales, así como del *hackeo* y/o clonación de páginas web institucionales a través del envío de solicitudes masivas.

En Nicaragua, la vigilancia e interceptación de las comunicaciones telefónicas y electrónicas ha sido una práctica sostenida tanto a defensores de derechos humanos como a personajes de la oposición y en Guatemala, nueve de diez personas manifestaron que sus teléfonos celulares han sido interceptados y/o utilizados como micrófonos y que conocen otras personas activistas de derechos humanos a quienes les ha sucedido lo mismo.

Respecto a allanamientos y requisas, en El Salvador, al menos dos de las organizaciones en las que trabajan las personas defensoras de derechos humanos entrevistadas han sufrido allanamientos ilegales por personas desconocidas durante el contexto de casos simbólicos, en los que se sustrajeron computadoras con información sensible sobre los mismos.

En **Guatemala**, la mayoría de las personas entrevistadas dijeron conocer al menos un caso de allanamiento a organizaciones de derechos humanos, muchos de los cuales se han producido en situaciones específicas de denuncia, extrayendo computadoras, discos duros, memorias USB y discos compactos con información sensible.

En **Nicaragua**, dos personas entrevistadas resaltaron los casos de allanamientos arbitrarios que las organizaciones para las cuales laboran han sufrido en los últimos años, mismos que se enmarcan dentro de un proceso acelerado de agudización de la crisis de gobernabilidad democrática en el país, cuestionada por la legitimidad de las instituciones.

En **Honduras**, dos de las personas entrevistadas manifestaron que la Policía realizó allanamientos a un periodista y a una organización de derechos humanos y en ambos casos decomisaron las computadoras.

Sobre otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones, en **El Salvador**, opositores políticos y/o personas defensoras de derechos humanos han sido chantajeadas con información personal obtenida a través de intervenciones a sus telecomunicaciones, con el objetivo de que bajen su perfil público y/o modifiquen sus posturas críticas.

En **Nicaragua**, otro tipo de vigilancia indirecta consiste en el seguimiento que se hace a las movilizaciones o protestas con el objetivo de despojar a las y los activistas y defensores de cámaras, teléfonos, tablets y equipos computarizados que luego son utilizados para intimidar, extraer información y publicarla en portales elaborados para desprestigiar el trabajo que realiza el sector de defensa de los derechos humanos.



Según la percepción y experiencia de las y los entrevistados ¿Cuáles son los actores involucrados en la vigilancia digital?

El Salvador	Guatemala	Honduras	Nicaragua
<ul style="list-style-type: none"> • Presidencia de la República a través del Organismo de Inteligencia del Estado y de la Secretaría de Participación Ciudadana, Transparencia y Anticorrupción • Fiscalía General de la República • Empresas telefónicas • Equipos de personas ligadas a los partidos mayoritarios • Embajada de los Estados Unidos de América en San Salvador. 	<ul style="list-style-type: none"> • Gobierno, particularmente a través del Ejército 	<ul style="list-style-type: none"> • Dirección de Inteligencia a través de la Unidad de Intervención de las Comunicaciones • Departamentos de investigación de la Policía • Empresas telefónicas. 	<ul style="list-style-type: none"> • Miembros de la Policía Nacional • Ejército de Nicaragua • Grupos de choques partidarios • Juventud Sandinista • Funcionarios de la Dirección General de Impuestos (DGI) • Inspectores del Instituto de Seguridad Social (INSS) • Funcionarios de telecomunicaciones (TELCOR) • Empresas proveedoras de servicios • Oficiales de Migración y Extranjería • Diputados/as • Magistrados/as • Líderes políticos del partido de gobierno en los barrios • Periodistas oficialistas.



Reino de los Países Bajos



COOPERACIÓN >