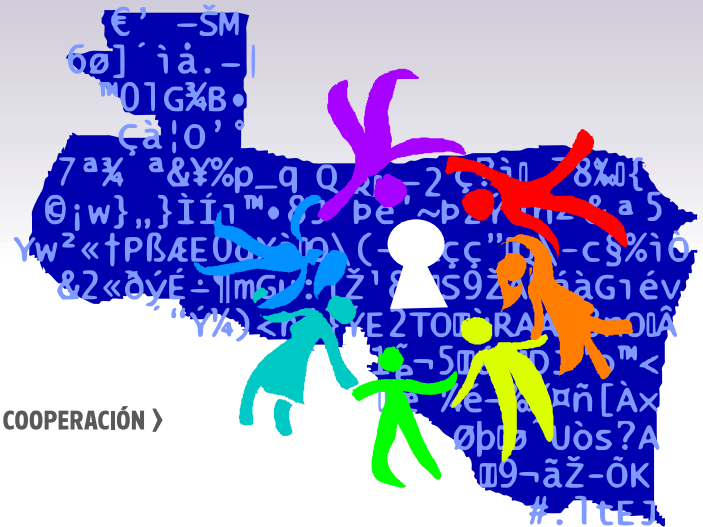
¿Privacidad digital para defensores y defensoras de derechos humanos?

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



Reino de los Países Bajos

FUNDACIÓN Acceso

ICCO COOPERACIÓN

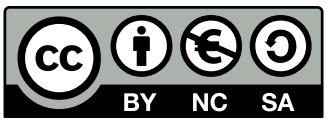
342.7

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.



Créditos

Coordinadora

Luciana Peri

Autoras y autores

Katitza Rodríguez

Marlon Hernández Anzora

Hedme Sierra-Castro

Jorge Jiménez Barillas

Edy Tábora Gonzales

Mireya Zepeda Rivera

Revisión de contenido

Luciana Peri

Katitza Rodríguez

Diseño y diagramación

Olman Bolaños

Larraitz Lexartza Artza

Corrección filológica

Marcia Ugarte Barquero

Índice

INTRODUCCIÓN

1. Justificación 14

2. El derecho a la privacidad en la era digital 20

CAPÍTULO I - ESTÁNDARES INTERNACIONALES

1. Del estado actual de la vigilancia de las comunicaciones y los estándares internacionales de derechos humanos 25

2. Temas más relevantes relacionados a la vigilancia y los estándares internacionales en materia de derechos humanos 29

2.1. Cambios tecnológicos y definiciones 29

2.2. La problemática de los metadatos 32

2.3. De por qué monitorear los datos de alguien es vigilancia 33

2.4. Protejamos la infraestructura de internet 34

2.5. La necesidad de respetar el objetivo legítimo 35

2.6. No a la complicidad de las empresas tecnológicas 36

2.7. Las reglas del juego deben ser conocidas por todas y todos 36

2.8. Notificación y derecho al remedio efectivo 37

2.9. Restaura el principio de proporcionalidad y necesidad 38

2.10. No a la discriminación entre nacionales y extranjeros 40

3. Anonimato 42

3.1. Concepto 42

3.2. Protección del anonimato 42

3.3. Restricciones al anonimato 44

4. Cifrado 46

4.1. Concepto 46

4.2. Protección del cifrado 46

4.3. Restricciones al cifrado 47

5. Conclusiones 49

Anexo I 50

CAPÍTULO 2- EL SALVADOR

1. Antecedentes 61

1.1. Estado de la discusión nacional 61

1.1.1. Delitos informáticos 62
1.1.2. Protección de datos 62
1.1.3. Comercio electrónico 63
1.1.4. Gobierno de internet 64
1.1.5. Documentos e informes 65
1.1.6. Blogs 65
1.2. Brecha digital 67
1.3. Criminalización de defensoras y defensores de derechos humanos 69
1.3.1. Derechos humanos: durante y después de los militares 69
1.3.2. Los Acuerdos de Paz 70
1.3.3. La actualidad: la defensa de los derechos humanos en el auge de la violencia social y el crimen organizado 71
1.4. Conclusiones preliminares 73
2. Marco legal nacional 74
2.1. Tratados internacionales 74
2.2. Constitución de la República de El Salvador 75
2.2.1. Vigilancia 75
2.2.1.1. Salvaguardas constitucionales del derecho a la privacidad en el contexto de la vigilancia a las comunicaciones 75
2.2.1.2. Limitaciones constitucionales al derecho a la privacidad en el contexto de la vigilancia 78
2.2.1.3. Mecanismo de acceso a la justicia en el contexto de vigilancia 79
2.2.2. Anonimato y cifrado 80
2.2.2.1. Salvaguardas constitucionales para la protección del cifrado y el anonimato 80
2.2.2.2. Limitaciones constitucionales al cifrado y el anonimato 83
2.2.2.3. Mecanismos de acceso a la justicia en el contexto del cifrado y el anonimato a nivel constitucional 83
2.3. Leyes, reglamentos y jurisprudencia 83
2.3.1. Vigilancia, cifrado y anonimato en leyes y reglamentos 83
2.3.1.1. Normas en materia penal 84
2.3.1.2. Normas sobre inteligencia y contrainteligencia 86
2.3.1.3. Normas en el sector de telecomunicaciones 8 6
2.3.1.4. Otras normas 87
2.3.2. Sobre allanamientos y registros 89
2.3.3. Supervisión pública 90

2.4. Conclusiones preliminares 92
3. Marco legal nacional y su adecuación a los estándares internacionales 94
3.1. Legalidad 95
3.2. Objetivo legítimo 97
3.3. Necesidad 98
3.4. Idoneidad 99
3.5. Proporcionalidad 99
3.6. Autoridad judicial competente 100
3.7. Debido proceso 100
3.8. Notificación del usuario 101
3.9. Transparencia 101
3.10. Supervisión pública 102
3.11. Integridad de las comunicaciones y sistemas 103
3.12. Garantías contra el acceso ilegítimo y derecho a recurso efectivo 104
3.13. Conclusiones preliminares 105
4. Experiencias e inquietudes del sector técnico y de defensa de derechos humanos 107
4.1. Reseña metodológica 107
4.2 Experiencias (hallazgos y casos paradigmáticos) 108
4.2.1. Vigilancia 108
4.2.2. Anonimato y cifrado 110
4.2.3. Allanamientos y requisas 110
4.2.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones 110
4.3. Inquietudes 112
4.3.1 Vigilancia1 12
4.3.2. Anonimato y cifrado 113
4.3.3. Allanamientos y requisas 113
4.3.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones 113
4.4. Conclusiones preliminares 114
4.4.1. Sobre experiencias 114
4.4.2. Dudas sobre el marco legal 115
5. Conclusiones nacionales 117

Bibliografía 119

CAPÍTULO III - GUATEMALA

1. Antecedentes 125

1.1. Estado de la discusión nacional 125

1.2. Brecha digital 127

1.3. Criminalización de defensoras y defensores de derechos humanos 130

2. Marco legal nacional 133

2.1. Tratados internacionales 133

2.1.1. Fuerza normativa de los tratados internacionales en materia de derechos humanos que pueden ser afectados por la vigilancia de las comunicaciones 133

2.1.2. Tratados en materia de Derechos Humanos ratificados por Guatemala que contienen una protección al Derecho a la privacidad 134

2.2. Constitución Política de la República de Guatemala 134

2.2.1. Vigilancia 134

2.2.1.1. Salvaguardas constitucionales del derecho a la privacidad en el contexto de la vigilancia de las comunicaciones 134

2.2.1.2. Limitaciones constitucionales al derecho a la privacidad en el contexto de la vigilancia de las comunicaciones 141

2.2.1.3. Mecanismos de acceso a la justicia en el contexto de la vigilancia 142

2.2.2. Anonimato y cifrado 143

2.2.2.1. Salvaguardas constitucionales para la protección del cifrado y el anonimato 143

2.2.2.2. Mecanismos de acceso a la justicia en el contexto del cifrado y el anonimato a nivel constitucional 145

2.3. Leyes, reglamentos y jurisprudencia 146

2.3.1. Vigilancia, cifrado y anonimato en leyes y reglamentos 146

2.3.1.1. Normas en materia penal 146

2.3.1.2. Normas sobre inteligencia y contrainteligencia 148

2.3.1.3. Normas en el sector de telecomunicaciones 148

2.3.1.4. Normativas de acceso a la información o transparencia relacionadas al tema de la vigilancia 149

2.3.1.5. Otras normas relacionadas al tema 149

2.3.1.6. Otras normas específicas que regulen el cifrado 150

2.3.1.7. Otras normas de debido proceso y anonimato digital 150

2.3.2. Sobre allanamientos y registros 150

2.3.3. Supervisión pública 151

2.4. Conclusiones preliminares 152

3. Marco legal nacional y su adecuación a los estándares internacionales 154
3.1. Principio de legalidad 155
3.2. Objetivo legítimo 157
3.3. Principios de necesidad, idoneidad y proporcionalidad 157
3.4. Principio de autoridad judicial competente 160
3.5. Debido proceso 161
3.6. Notificación del usuario 162
3.7. Transparencia 162
3.8. Supervisión pública 163
3.9. Integridad de las comunicaciones y sistemas 164
3.10. Garantías contra el acceso ilegítimo y derecho a recurso efectivo 165
4. Experiencias e inquietudes del sector técnico y de defensa de derechos humanos 166
4.1. Metodología 166
4.2. Experiencias (hallazgos y casos paradigmáticos) 167
4.2.1. Vigilancia 167
4.2.2. Anonimato y cifrado 170
4.2.3. Requisas y allanamientos 170
4.2.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones 171
4.3. Inquietudes 172
4.3.1. Vigilancia 172
4.3.2. Anonimato y cifrado 173
4.3.3. Requisas y allanamientos 174
4.3.4. Otros mecanismos para la criminalización vinculada al derechoa la privacidad digital, en internet y en las telecomunicaciones 174
5. Conclusiones nacionales 175
Bibliografía 177

CAPÍTULO IV - HONDURAS

1. Antecedentes 180
1.1. Estado de la discusión nacional 180
1.2. Brecha digital 181
1.2.1. Acceso a computadoras 182

1.2.2. Acceso a teléfonos 182
1.2.2.1. Telefonía fija 182
1.2.2.2.Telefonía móvil 183
1.2.3. Acceso a internet 183
1.2.3.1 Personas suscriptoras de internet con conectividad de banda ancha 183
1.2.3.2 Densidad de personas suscriptoras de internet con conectividad de banda ancha por 100 habitantes 184
1.3. Criminalización de defensoras y defensores de derechos humanos 185
1.4. Conclusiones preliminares 188
2. Marco legal nacional 189
2.1. Tratados internacionales 189
2.2. Constitución Política de Honduras 192
2.2.1. Vigilancia 192
2.2.1.1. Salvaguardas constitucionales del derecho a la privacidad en el contexto de la vigilancia de las comunicaciones 192
2.2.1.2. Limitaciones constitucionales al derecho a la privacidad en el contexto de la vigilancia de las comunicaciones 196
2.2.1.3. Mecanismos de acceso a la justicia en el contexto de la vigilancia 197
2.2.2. Anonimato y cifrado 198
2.2.2.1. Salvaguardas constitucionales para la protección del cifrado y el anonimato 198
2.2.2.2. Limitaciones constitucionales al cifrado y el anonimato 199
2.2.2.3. Mecanismos de acceso a la justicia en el contexto del cifrado y el anonimato a nivel constitucional 200
2.3. Leyes, reglamentos y jurisprudencia 200
2.3.1. Vigilancia, cifrado y anonimato en leyes y reglamentos 200
2.3.1.1. Normas en materia penal 204
2.3.1.2. Normas sobre inteligencia y contrainteligencia 207
2.3.1.3. Normas en el sector de telecomunicaciones 209
2.3.1.4. Normativas de acceso a la información o transparencia 212
2.3.1.5. Otras normas relacionadas al tema (protección de datos) 213
2.3.1.6. Otras normas especificas que regulen el cifrado 220
2.3.1.7. Otras normas de debido proceso que expliquen el proceso para revelar la identidad de la persona anónima si existe 220
2.3.2. Otras normas que regulen el allanamiento de casas/oficinas, registros y secuestro de computadora 220
2.3.2.2. Allanamiento por estado de necesidad 221
2.3.2.3. Registro de sitios públicos 222

2.4. Supervisión pública 222
3. Marco legal nacional y su adecuación a los estándares internacionales 224
3.1. Legalidad 225
3.2. Objetivo legítimo 226
3.3. Necesidad, idoneidad y proporcionalidad 226
3.4. Autoridad judicial competente 227
3.5. Debido proceso 227
de las comunicaciones (art. 19 y 48 de la Ley de Intervención de las Comunicaciones) 228
3.6. Notificación del usuario 228
3.7. Transparencia 228
3.8. Supervisión pública 229
3.9. Integridad de las comunicaciones y sistemas 230
3.10. Garantías para la cooperación internacional 231
3.11. Garantías contra el acceso ilegítimo y recurso efectivo 231
4. Experiencias e inquietudes del sector técnico y de defensa de derechos humanos 233
4.1. Reseña metodológica 233
4.2. Experiencias (hallazgos y casos paradigmáticos) 234
4.2.1. Vigilancia 234
4.2.2. Anonimato y cifrado 235
4.2.3. Allanamientos y requisas 236
4.2.4 Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en Internet y en las telecomunicaciones 236
4.3. Inquietudes 236
4.3.1 Vigilancia 236
4.3.2. Anonimato y cifrado 237
4.3.3. Allanamientos y requisas 237
4.3.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones 237
5. Conclusiones nacionales 238
Bibliografía 241

CAPÍTULO 5 -NICARAGUA

1. Antecedentes 247
1.1. Estado de la discusión nacional 247

1.1.1. Protección de datos personales y habeas data 248
1.1.2. La autodeterminación informativa 249
1.1.3. Documentos e informes 250
1.2. Brecha digital 252
1.3. Criminalización de defensoras y defensores de derechos humanos 255
1.3.1. Institucionalidad democrática 255
1.3.2. Control de medios de comunicación 256
1.3.3. Amenazas, intimidación y criminalización 257
2. Marco legal nacional 258
2.1. Tratados internacionales 258
2.2. Constitución Política de Nicaragua 259
2.2.1. Vigilancia 260
2.2.1.1. Salvaguardas constitucionales del derecho a la privacidad en el contexto de la vigilancia de las comunicaciones 260
2.2.1.2 Limitaciones constitucionales al derecho a la privacidad en el contexto de la vigilancia de las comunicaciones 265
2.2.1.3. Mecanismos de acceso a la justicia en el contexto de la vigilancia 266
2.2.2. Anonimato y cifrado 270
2.2.2.1. Salvaguardas constitucionales para la protección del cifrado y el anonimato 270
2.2.2.2. Limitaciones constitucionales a la protección del cifrado y el anonimato 272
2.2.2.3. Mecanismos de acceso a la justicia en el contexto del cifrado y el anonimato a nivel constitucional 272
2.3. Leyes, reglamentos y jurisprudencia 273
2.3.1. Vigilancia, cifrado y anonimato en leyes y reglamentos 273
2.3.1.1. Normas en materia penal 274
2.3.1.2. Normas sobre inteligencia y contrainteligencia 276
2.3.1.3. Normas en el sector de telecomunicaciones 277
2.3.1.4. Normativas de acceso a la información o transparencia 278
2.3.1.5. Otras normas relacionadas al tema 278
2.3.2. Sobre allanamientos y registros 280
2.3.2.1. Plazo de las intervenciones 280
2.3.2.2. Allanamiento por orden judicial 280
2.3.3. Supervisión pública 281
3. Marco legal nacional y su adecuación a los estándares internacionales 283
3.1. Legalidad 287

3.2. Objetivo legítimo 288
3.3. Necesidad e idoneidad 289
3.4. Proporcionalidad 290
3.5. Autoridad judicial competente 291
3.6. Debido proceso 292
3.7. Notificación del usuario 292
3.8. Transparencia y supervisión pública 293
3.9. Garantías para la Cooperación Internacional 294
3.10. Conclusiones preliminares 294
4. Experiencias e inquietudes del sector técnico y de defensa de derechos humanos 296
4.1. Metodología 296
4.2. Experiencias 297
4.2.1. Vigilancia 297
4.2.2. Anonimato y cifrado 299
4.2.3. Allanamientos y requisas 299
4.2.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones 300
4.3 Inquietudes 301
4.3.1. Vigilancia 301
4.3.2. Anonimato y cifrado 302
4.3.3. Allanamientos y requisas 302
4.3.4 Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones 302

5. Conclusiones nacionales 306
Bibliografía 304

CONCLUSIONES COMPARATIVAS SOBRE EL DERECHO A LA PRIVACIDAD EN LA NORMATIVA CENTROAMERICANA

1. El derecho a la privacidad en las constituciones centroamericanas 310
1.1 Derecho a la intimidad y la vida privada 310
1.2 Inviolabilidad de las comunicaciones, documentos y domicilio 311
1.3. Autodeterminación informativa 313

1.4. El derecho al buen nombre y al honor 314

2. El derecho a la privacidad digital en otras leyes centroamericanas 315

3. Mecanismos de acceso a la justicia para la protección de la privacidad digital en Centroamérica 320

4. Adecuación de las normas centroamericanas a los estándares internacionales 321

INTRODUCCIÓN

1. Justificación

Luciana Peri

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 2007[2] 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 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

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) Disponible en https://www.frontlinedefenders.org/files/annual_report_spanish_2.pdf (consultado: 30 noviembre, 2015)

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 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, y ha disminuido 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]

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)

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 delincuentes.[6]

¿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

a) Almacenada en nuestros dispositivos electrónicos.

b) Compartida, comunicada, socializada mediante internet por correos electrónicos, llamadas online, mensajería instantánea, redes sociales, archivos compartidos, etc.

c) 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

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

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 físicia, 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 intermediaras 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.

2. El derecho a la privacidad en la era digital

Katitza Rodríguez

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]

Referencias a la noción de privacidad se remontan a textos tan antiguos como la Biblia, la cultura hebrea temprana, Grecia clásica y la antigua China.[9] Estas nociones también aparecen durante la época monárquica cuando los reyes utilizaban la privacidad con el fin de proteger aquello que no querían exponer al escrutinio público. Las violaciones a la privacidad también salen a la luz, por ejemplo, el uso de la vigilancia con fines de control político. Así sucedió en la Antigua Roma, cuando Cicerón se percató que sus mensajeros interceptaban sus propias cartas bajo las órdenes de Julio César[10], o en el Reino de los Tudors en Inglaterra,[11] quienes contaban con toda una maquinaria estatal preparada para vigilar y atrapar a quien produjera literatura desafiante contra el reino.

La discusión sobre la utilidad de la vigilancia como mecanismo de control a la población ha sido abordada también en la filosofía. Jeremy Bentham, filósofo británico, propuso el *panóptico*,[12] un edificio circular con una torre central de observación donde el vigilante podía monitorear a todos los reclusos que se encontraban en sus celdas continuamente, sin que los reclusos, por su parte, fueran capaces de ver al inspector. Bentham pensaba que la incertidumbre de estar continuamente vigilados, garantiza el funcionamiento automático del poder sin que se ejerza a cada momento, logrando una vigilancia más eficaz. Sobre el panóptico, el filósofo francés Michel Foucault postuló que este representa la forma en que la disciplina y el castigo funciona en la sociedad moderna. El panóptico es un diagrama del poder en acción porque al ver el plano del panóptico uno se da cuenta de cómo operan los procesos de observación; este perfecciona el ejercicio del poder, por un lado, son menos los que lo ejercen y por otro, más aquellos sobre los que se ejerce.[13]

La conceptualización de la privacidad ha sido siempre muy debatida y estudiada. Para algunos autores,

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 Convenant on Civil and Political Rights*, (New York: Columbia University Press, 1981), https://eff.org/phr2006 (consultado: 16 noviembre, 2015)

9 Marc Rotenberg, Allison Knight, Katitza Rodríguez, Privacy and Human Rights: An International Survey of Privacy Laws and Developments, (EPIC, 2006), https://eff.org/phr2006 (consultado: 16 noviembre, 2015).

10 Anthony Zurcher. Roman Empire to the NSA: A world history of government spying, *Noticias BBC,* 1 de noviembre 2013, http://www.bbc.com/news/magazine-24749166 (consultado: 16 noviembre, 2015)

11 500 Years of History Shows that Mass Spying Is Always Aimed at Crushing Dissent, Washingtonblog, 9 de enero 2014, https://eff.org/crushing-dissent-spying-mass-surveillance-washingtonblog (consultado: 16 noviembre, 2015)

12 University College London, *The Panopticon,* The Bentham Project, https://www.ucl.ac.uk/Bentham-Project/who/panopticon (consultado: 22 noviembre, 2015)

13 Michel Foucault, "Discipline and Punish, Panopticism." In Discipline & Punish: The Birth of the Prison, edited by Alan Sheridan, 195-228. New York: Vintage Books, 1977. http://foucault.info/doc/documents/disciplineandpunish/foucault-disciplineandpunish-panopticism-html (consultado: 22 de noviembre).

la privacidad es "el derecho a ser dejado solo (*right to be left alone*, en inglés)".[14] 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."[15]

La privacidad puede ser entendida, por un lado, como el derecho que tiene toda persona a la inviolabilidad de su intimidad, su vida privada, sus comunicaciones, su domicilio, sus documentos. La privacidad se define como la presunción que el individuo debe tener una esfera de desarrollo autónomo, interacción y libertad, una "esfera privada" con o sin relación con otras y libre de la intervención del Estado y de la intervención excesiva no solicitada de otros individuos no invitados.[16]

Por otro lado, se trata de proteger aquel espacio que cada persona se reserva para sí misma o para su círculo más íntimo. Como algunos otros autores han señalado, "el derecho de mantener ciertos aspectos de la vida privada fuera del alcance de terceros y, por lo tanto, el derecho a construir diferentes "personalidades situacionales.""[17] En otras palabras, la privacidad consiste en el poder de controlar información personal, decidir con quién se comparte y para qué se utiliza con terceros, así como el derecho a que ésta se trate de forma adecuada, para permitir el ejercicio de otros derechos y evitar daños a su titular.[18]

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.[19] 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

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

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

16 Lord Lester y D. Pannick (eds.), Human Rigths Law and Practice (Londres, Butterworth, 2004), párr. 4.82. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G09/178/07/PDF/G0917807.pdf?OpenElement (consultado: 16 noviembre, 2015)

17 Abril P. Pizarro E. La intimidad europea frente a la privacidad americana. *Revista para Análisis de Derecho*. Barcelona, enero 2014, http://derechoaleer.org/media/files/olvido/1031.pdf (consultado: 16 noviembre, 2015)

18 Instituto Nacional de Transparencia, *Acceso a la Información Pública y Protección de Datos Personales, Guía práctica para ejercer el derecho a la protección de datos personales*, (México, s.f.) http://inicio.ifai.org.mx/Publicaciones/01GuiaPracticaEjercerelDerecho.pdf (consultado: 16 noviembre, 2015)

19 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.

Estado adopte las medidas de ley necesarias para proteger a toda persona frente a esas injerencias o ataques.

En su Observación General Nº 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.[20]

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. Esa limitación permisible ha sido desarrollada por el Relator Especial de la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo,[21] quien ha señalado que el artículo 17 del PIDCP debe ser interpretado en el sentido de que contiene los elementos de prueba de la admisibilidad de la limitación:

> Las restricciones no prescritas por la ley son "ilegales" en el sentido del artículo 17, y las restricciones que distan de ser necesarias o no responden a un objetivo legítimo constituyen una injerencia "arbitraria" en los derechos previstos por el artículo 17. Por consiguiente, las limitaciones del derecho a la intimidad o de otras dimensiones del artículo 17 están sometidas a una prueba de admisibilidad, como establece el Comité de Derechos Humanos en su Observación general Nº 27 (1999). Esa observación general hace referencia a la libertad de circulación (art. 12) que es una de las disposiciones que contiene una cláusula limitativa.

Entre los elementos mas importantes en esta cláusula limitativa encontramos, por ejemplo, que toda restricción esté prescrita por ley, no debe comprometer la esencia del derecho necesaria en una sociedad democrática; el poder discrecional de aplicación de la limitación no debe ser ilimitado. Para que una restricción sea admisible, no basta con que se utilice para conseguir fines legítimos, debe ser necesaria para lograrlos. Además, agregar que las medidas restrictivas deben respetar el principio de proporcionalidad, deben ser adecuadas para conseguir su función protectora, deben ser el instrumento menos perturbador de los que permitan conseguir el resultado deseado y deben guardar proporción con el interés que se debe proteger y ser compatibles con los demás derechos

20 Naciones Unidas, *Observación general Nº 16, Derechos de la privacidad (artículo 17), 35º período de sesiones* (1988), HRI/GEN/1/Rev.9 (Vol.I), 228, http://www1.umn.edu/humanrts/hrcommittee/Sgencom16.html (consultado: 16 noviembre, 2015)

21 Martin Scheinin, *Informe del Relator Especial de la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, A/HRC/13/37*, http://www2.ohchr.org/english/bodies/hrcouncil/docs/16session/A.HRC.16.51_sp.pdf (consultado: 16 noviembre, 2015)

consagrados en el Pacto.[22]

El presente trabajo entenderá bajo el concepto de privacidad un conjunto de derechos que comprenden: la protección de datos personales y el derecho a la autodeterminación informativa, la inviolabilidad de las comunicaciones, el domicilio, el derecho a la intimidad y a la vida privada. También incluye el derecho de cada persona de desarrollar, usar y enseñar herramientas de cifrado y el derecho a elegir, leer o comunicarse anónimamente.

22 Naciones Unidas, *Comentarios Generales No. 27. Aprobados por el Comité de Derechos Humanos con arreglo al párrafo 4 del artículo 40 del PIDCP, CCPR/C/21/Rev.1/Add.9*, (1999), C%2f21%2fRev.1%2fAdd.9&Lang=en (consultado: 16 noviembre, 2015)

Estándares Internacionales

Katitza Rodríguez[1]

1. Del estado actual de la vigilancia de las comunicaciones y los estándares internacionales de derechos humanos

Desde antes que el denunciante Edward Snowden filtrara su primer documento al periódico británico *The Guardian* sobre la vigilancia masiva conducida por la Agencia de Seguridad Nacional (NSA por sus siglas en inglés) de los Estados Unidos, activistas sobre el derecho a la privacidad ya estaban muy preocupadas por el avance de las técnicas y tecnologías de vigilancia y su impacto en la vida privada de las personas. A partir de aquellas preocupaciones se produce la elaboración de los *Principios Internacionales sobre la Aplicación de los Derechos Humanos sobre la Vigilancia de las Comunicaciones*.[2] Los 13 Principios explican cómo el derecho internacional de los derechos humanos se emplea en el contexto de la vigilancia estatal de las comunicaciones.[3] Ellos se encuentran 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.

La versión final de los 13 Principios fue publicada el 20 de julio del año 2013, las primeras semanas de lo que podríamos denominar la "Era post-Snowden". Desde entonces, los Principios han sido la estrella polar para aquellos que buscan soluciones frente a una cruda realidad en la que, gracias a las grietas de la evolución tecnológica y las protecciones legales obsoletas, los Estados vienen adoptando prácticas de vigilancia sumamente invasivas que corrompen la esencia misma de nuestras libertades fundamentales.[4]

Los 13 Principios han recibido un fuerte apoyo en todo el mundo, impulsado en gran medida por la indignación popular frente al espionaje de la NSA y otras agencias de inteligencia.[5] Desde América Latina a Europa, de Asia al mundo árabe, los activistas han utilizado los Principios en *amicus curiae*, en análisis de políticas públicas, en campañas de incidencia, en medios de comunicación, y han sido

1 Agradecemos los aportes en la elaboración del presente artículo de Ana María Acosta, abogada colombiana y asistente de investigación de la Electronic Frontier Foundation durante el verano de 2015.

2 Ver: https://es.necessaryandproportionate.org/text

3 EFF, artículo 19, Análisis Jurídico Internacional de Apoyo y Antecedentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/AnalisisLegal, Access, Guía de Implementación Universal de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf

4 Katitza Rodriguez, *Un combate contra la vigilancia basado en principios*, (Giswatch, 2014), http://www.giswatch.org/es/report-introduction/un-combate-contra-la-vigilancia-basado-en-principios (consultado: 16 noviembre, 2015)

5 Los Principios Necesidad y Proporcional han sido firmados por mas de 350,000 personas y 450 organizaciones sin fines de lucro,

citados en informes internacionales emitidos por organismos de las Naciones Unidas y la Comisión Interamericana de Derechos Humanos (CIDH).

Algunos resultados de la incidencia de la sociedad civil han tenido sus frutos a nivel internacional. En diciembre de 2013, la Asamblea General aprobó con unanimidad la Resolución "*El derecho a la privacidad en la era digital*". Este documento afirma que "los derechos de las personas también deben estar protegidos en internet, incluido el derecho a la privacidad".[6] La Resolución fue presentada por Brasil y Alemania y patrocinada por más de 50 estados miembros y es la declaración más importante que Naciones Unidas ha emitido sobre el derecho a la privacidad en más de 25 años. Esta declaración solicita expresamente a la Alta Comisionada de las Naciones Unidas para los Derechos Humanos que presente al Consejo de Derechos Humanos un informe sobre la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales. Y así se hizo.

En el excelente informe publicado por la Alta Comisionada, ella ahonda en los temas de vigilancia. Ella explica, por ejemplo, que los "metadatos" o también conocidos como los "datos sobre las comunicaciones" pueden dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona, incluso frente a la información obtenida cuando se accede al contenido de una comunicación privada.[7]

Además, se sumó el informe del Relator para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, Dr. Ben Emerson, quien criticó severamente la vigilancia masiva de las comunicaciones.[8] El Relator también mostró su desacuerdo con la falta de legislación clara y precisa que autorice las facultades de vigilancia, y la necesidad que esta se rija por los principios de proporcionalidad, necesidad, supervisión pública, autorización judicial, y transparencia. En un nuevo informe publicado en Septiembre del 2015, el Dr. Emerson recalcó explícitamente que las medidas que interfieran con el derecho a la privacidad deben "cumplir con los criterios de necesidad y proporcionalidad."[9] Además dejó claro que la vigilancia a gran escala, que a menudo se justifica aduciendo la lucha contra el terrorismo, se ha utilizado en varios Estados

6 Naciones Unidas, *Resolución de la Asamblea General de las Naciones Unidas, El derecho a la privacidad en la era digital, UN Doc. A / RES/68/167*, (2013), https://eff.org/UN-A-RES-68-167 (consultado: 16 noviembre 2015)

7 Navy Pillay, *Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. El derecho a la privacidad en la era digital, UN Doc. A/HRC/27/37*, (2014), https://eff.org/A-HRC-27-37 (consultado: 16 noviembre, 2015)

8 Ben Emerson, *Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, UN Doc. A/69/397 sobre* el uso de la vigilancia digital a gran escala en la lucha contra el terrorismo, (2014), https://eff.org/A-69-397 (consultado: 16 noviembre, 2015)

9 Ben Emerson, *Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, UN Doc. A/70/371 sobre las consecuencias negativas que tienen para la sociedad civil la legislación contra el terrorismo y otras medidas (2015), párrafo16,* http://www.un.org/ga/search/viewm_doc.asp?symbol=A/70/37 (consultado: 22 noviembre, 2015)

para "vigilar a grupos de la sociedad civil, defensores de los derechos humanos y periodistas.[10]

Y por su parte, el nuevo Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas; David Kaye, también contribuyó al debate cuando publicó dos informes sumamente relevantes. El primero aborda la utilización del cifrado y el anonimato en las comunicaciones digitales,[11] mientras que el segundo se ocupa de la protección de las fuentes de información y los denunciantes de irregularidades.[12] También emitieron comunicaciones conjuntas el Relator y la Relatora de Libertad de Expresión de Naciones Unidas y la Comisión Interamericana de Derechos Humanos, dejando clara la falta de regulación adecuada en esta materia en varios países incluida América Latina.[13]

Las campañas pro-privacidad continuaron en el ámbito de las Naciones Unidas. En esta oportunidad, organizaciones de la sociedad civil solicitaron la creación de una Relatoría dedicada especialmente al derecho a la privacidad, ya que era uno de los derechos civiles y políticos que no contaba con una Relatoría especializada.[14] Es así que en julio de 2015, el Presidente del Consejo de Derechos Humanos de la ONU designó al primer Relator del Derecho a la Privacidad, el Sr. Joseph Cannataci. La designación se basó en la Resolución 03/2015 del Consejo de Derechos Humanos, que instó al nombramiento de un Relator Especial sobre el derecho a la privacidad por un período de tres años.[15]

En la "Era post-Snowden", los debates se dieron incluso en espacios regionales y nacionales. Por ejemplo, una comisión parlamentaria alemana investigó el alcance y los antecedentes del espionaje de la NSA en Alemania.[16] Defensores y defensoras de la privacidad desafiaron las actividades de vigilancia de los Estados Unidos en tribunales locales, mientras que también lo desafiaron en el Reino Unido ante el tribunal británico[17] y el Tribunal Europeo de Derechos Humanos.

---

10 Ben Emerson, *Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, UN Doc. A/70/371 sobre las onsecuencias negativas que tienen para la sociedad civil la legislación contra el terrorismo y otras medidas (2015), paragraph 16,* http://www.un.org/ga/search/viewm_doc.asp?symbol=A/70/37 (consultado: 22 noviembre, 2015)

11 David Kaye, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión que aborda la utilización del cifrado y el anonimato en las comunicaciones digitales, UN Doc. A/HRC/29/32 sobre el anonimatoy el cifrado*, (2015), https://eff.org/A-HRC-29-32 (consultado: 16 noviembre, 2015)

12 David Kaye, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión sobre la protección de las fuentes de información y los denunciantes de irregularidades, UN Doc. A/70/361*, (2015) https://eff.org/A-70-361 (consultado: 16 noviembre, 2015)

13 Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión, disponible en: https://eff.org/OEA-ONU-comunicado-conjunto-vigilancia-2013

14 Los relatores desempeñan un papel fundamental en promover el desarrollo de un entendimiento común y una interpretación sustantiva de un derecho en particular.

15 Naciones Unidas. Resolución del Consejo de Derechos Humanos, El derecho a la privacidad en la era digital, UN Doc. A/HRC/28/L.27, (2015), https://eff.org/A-HRC-28-L27 (consultado: 16 noviembre, 2015)

16 Comités alemanes de investigación investiga el escándalo de espionaje de la NSA, disponible en: https://eff.org/german-inquiry-nsa

17 "GCHQ-NSA intelligence sharing unlawful, says UK surveillance tribunal", *Privacy International*, 6 de febrero, 2015, https://www.privacyinternational.org/node/482 (consultado: 16 noviembre, 2015)

América Latina no se ha quedado atrás en términos de litigio estratégico. La Red en Defensa de los Derechos Humanos en México ha iniciado un proceso de inconstitucionalidad contra una norma que busca retener los datos de las comunicaciones de la población entera mexicana que usa el teléfono e internet. Data, una organización uruguaya, ha presentado un *amicus curiae* citando también los Principios, buscando acceder a la normativa que regula el nuevo programa de vigilancia adquirido por el Ministerio del Interior. De acuerdo a la prensa uruguaya, el programa denominado El Guardián incrementará exponencialmente la capacidad del Estado uruguayo de vigilar llamadas telefónicas, correos electrónicos y redes sociales.[18]

En el marco de esta compleja situación internacional se enmarca el presente trabajo de investigación en cuatro países de Centroamérica coordinado por Fundación Acceso. Una de las secciones de la investigación busca evaluar a la luz de los estándares internacionales de derechos humanos, los marcos normativos del derecho a la privacidad, anonimato y el cifrado frente a la vigilancia estatal. Para ello, los y las investigadoras utilizaron los *Principios Internacionales sobre la Aplicación de los Derechos Humanos sobre la Vigilancia de las Comunicaciones* como guía práctica para evaluar si la normativa de vigilancia en Guatemala, Honduras, El Salvador y Nicaragua cumplen o no con los estándares en materia de derechos humanos. Esta investigación entonces continúa el trabajo iniciado por grupos de la sociedad civil para implementar a nivel nacional aquellos avances en materia de derechos humanos logrados a nivel internacional.

18 Scrollini, Tudurí, Rodríguez, *Vigilancia estatal de las comunicaciones y protección de los derechos fundamentales en Uruguay,* (2015).

2. Temas más relevantes relacionados a la vigilancia y los estándares internacionales en materia de derechos humanos

A continuación, explicaremos algunos de los aspectos mas importantes detrás de los *Principios Internacionales sobre la Aplicación de los Derechos Humanos sobre la Vigilancia de las Comunicaciones.* Una explicación más profunda de los fundamentos jurídicos procedentes de la jurisprudencia de derechos humanos y los documentos de Naciones Unidas y del sistema interamericano se encuentran en el informe "Análisis Jurídico Internacional de Apoyo y Antecedentes, documento producido como material de apoyo para los Principios."[19]

2.1. Cambios tecnológicos y definiciones

Hace unos años atrás, la vigilancia estatal de las comunicaciones era una tarea laboriosa y compleja que necesitaba de muchas personas. La policía secreta oficial de la Alemania nazi (Gestapo), por ejemplo, tenía 40.000 funcionarios que vigilaban a un país de 80 millones de personas, mientras que la policía secreta de la ex Alemania del Este (Stasi) empleó 102.000 para controlar una población solamente de 17 millones.[20] La Stasi también llevaba un cuidadoso registro de las y los ciudadanos objeto de vigilancia, consignándose numerosos datos sobre su vida privada.[21] En las últimas décadas la tecnología ha logrado que se pueda hacer mucho más con mucho menos despliegue logístico, haciendo que actualmente conducir la vigilancia sea mucho más sencillo. Más aún, Estados con una gran pobreza a nivel nacional han reservado jugosos presupuestos para la adquisición de estas herramientas tecnológicas.[22]

En este contexto, existe una mayor cantidad de información que dejamos cada vez que usamos un teléfono celular, una computadora o cualquier dispositivo electrónico. Estos datos sobre nuestra

19 EFF, Artículo 19.

20 John O. Koehler, Stasi, *La historia no dicha de la policía secreta de Alemania del Este*, (West View Press,1999), https://www.nytimes.com/books/first/k/koehler-stasi.html (consultado: 16 noviembre, 2015)

21 Funder, A. *Stasiland: Stories from Behind the Berlin Wall,* (London: Granta.2004).

22 EFF, *American Sues Ethiopian Government for Spyware Infection* (2014), https://www.eff.org/es/press/releases/american-sues-ethiopian-government-spyware-infection (consultado: 22 noviembre, 2015).

comunicación, también conocidos como metadatos, revelan información muy sensible: con quién nos comunicamos y con qué frecuencia, con quién hemos estado y en qué lugar, a dónde vamos todo los viernes al medio día, y cuándo abandonamos ese hábito. Los metadatos son, entonces, aquellos datos vinculados a las comunicaciones que no son el contenido del mismo. Una reciente investigación de la Universidad de Stanford, señaló que los metadatos revelan información muy sensible "que se pueden discernir a partir de una cantidad relativamente pequeña de metadatos".[23] Con los metadatos es posible inferir información sensible aunque no puedas acceder al contenido del mensaje. Por ejemplo, pueden saber que:

- ..llamaste a una línea de sexo telefónico a las 2:24 a.m. y que hablaste durante 18 minutos. Pero no saben de qué fue lo conversado.
- ...llamaste a una línea de prevención de suicidios desde un puente ... Pero el asunto se mantiene secreto.
- ...recibiste un correo electrónico de un servicio de análisis de VIH, que entonces llamaste a tu médico y miraste una página de apoyo de grupos con VIH, todo en la misma hora. Pero no saben qué había en el correo ni de qué hablaste por teléfono. [...]

No olvidemos que ahora es mucho mas sencillo y barato almacenar gran cantidad de información, procesarla y analizarla para determinar patrones de comportamiento a través del tiempo.

- ...llamaste a un ginecólogo, que hablaste por media hora y que durante el día buscaste en internet el número telefónico de una clínica de aborto. Pero nadie sabe de qué asunto has conversado.[24]

Debemos tener en cuenta, además, que un gran porcentaje de nuestras comunicaciones son intermediadas por empresas que hacen el papel de terceras partes. Si antes guardábamos nuestras cartas, documentos o informes en nuestra oficina o casa, ahora nuestras comunicaciones o documentos se encuentran en la nube en servidores de empresas intermediarias o se transmiten a través de ellas. Estas empresas de internet o telefonía juegan un papel muy importante pues tienen la capacidad de identificar al usuario que usa sus sistemas. Mientras más información recopilan las empresas, más motivos tiene el Estado para querer acceder a esa información. Como hemos visto en los informes de transparencia de grandes empresas de internet que recopilan una gran información personal, el número de solicitudes gubernamentales de datos hacia esas empresas en el mundo solo va en aumento.[25]

23 Jonathan Mayer, *MetaPhone: The Sensitivity of Telephone Metadata*, (2014) http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/ (consultado: 16 noviembre, 2015)

24 EFF, *Por qué los metadatos son importantes*, (2015): https://ssd.eff.org/es/module/por-qu%C3%A9-los-metadatos-son-importantes (consultado: 16 noviembre, 2015)

25 Véase informe de transparencia de Googe, disponible en: http://www.google.com/transparencyreport/userdatarequests/countries, Twitter, disponible en: https://transparency.twitter.com/information-requests/2015/jan-jun y Yahoo, disponible en: https://transparency.yahoo.com/government-data-requests/index.htm, Dropbox, disponible en: https://www.dropbox.com/transparency

Recordemos también que existe una gran cantidad de información que las personas publican abierta y voluntariamente en redes sociales, la cual puede ser fácilmente recolectada, almacenada y analizada por el Estado o por cualquiera.

Por otro lado, se ha desarrollado una industria global de la vigilancia de aproximadamente cero dólares en el 2001 a una mega industria de US$5 mil millones al año,[26] y que está lista para satisfacer la demanda del Estado.

Las tecnologías de vigilancia ofrecidas oscilan desde la vigilancia masiva realizada a poblaciones enteras al mismo tiempo que se han desarrollado técnicas mucho más invasivas que meramente escuchar una conversación en tiempo real. Por ejemplo, las agencias de inteligencia de un Estado realizan acciones encubiertas usando un "software malicioso", o también conocido como *malware*. Este software permite interrumpir el funcionamiento del ordenador, recopilar información sensible, o permite encender el micrófono o la cámara de una computadora o grabar cada letra presionada en el teclado. Recientemente, ha habido varios informes revelando el uso de estas herramientas que permiten espiar a activistas, periodistas y disidentes.[27] También se ha multiplicado el uso de receptores IMSI (*IMSI catchers* o también conocidos como *Stingrays*), un receptor disfrazado de torre de telefonía celular legítima que engaña a un teléfono móvil a conectarse al receptor IMSI con el fin de rastrear la ubicación de un teléfono móvil en tiempo real. Hemos visto su despliegue en varios países, desde Colombia[28] hasta Estados Unidos.[29]

Mientras avanza la tecnología, el derecho, sin embargo se ha quedado atrás. Muchos países están adoptando normas que busca debilitar, en vez de reforzar, las garantías necesarias para limitar la vigilancia a lo necesario y proporcional con un sistema de rendición de cuentas y transparencia sólido que permita proteger a la sociedad de cualquier abuso de poder.

Así, en la era digital cuando hablamos de vigilancia no nos limitamos a la mera interceptación de las comunicaciones sino que además esta abarca una serie de actividades: monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona.[30] Más aún, cuando hablamos de

26 Jennifer Valentino-DeVries, Julia Angwin and Steve Stecklow, "Document Trove Exposes Surveillance Methods", *Wall Street Journa*l, 2011, http://www.wsj.com/articles/SB10001424052970203611404577044192607407780 (consultado: 16 noviembre, 2015)

27 Veáse: CitizenLab, Communities @ Risk: Targeted Digital Threats Against Civil Society, disponible en: https://targetedthreats.net/media/1-ExecutiveSummary.pdf Véase también, Bahrain Watch, Bahrain Government Hacked Lawyers and Activists with UK Spyware, disponible en: https://bahrainwatch.org/blog/2014/08/07/uk-spyware-used-to-hack-bahrain-lawyers-activists/

28 Privacy International, *Demanda y oferta: La industria de la vigilancia al descubierto*, (Bogotá, 2015), https://www.privacyinternational.org/sites/default/files/DemandSupply_Espanol.pdf (consultado: 16 noviembre, 2015)

29 Hanni Fakhouri, *Stingrays Go Mainstream,* (EFF, 2015), https://www.eff.org/es/deeplinks/2015/01/2014-review-stingrays-go-mainstream (consultado: 16 noviembre, 2015)

30 Véase Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, "Cambios de Tecnología y Definiciones", disponible en: https://es.necessaryandproportionate.org/text

comunicaciones no nos limitamos al envío de correos electrónicos sino a toda serie de actividades, interacciones y transacciones transmitidas vía red. Estas definiciones fueron incorporadas en los 13 Principios para explicar a qué nos referimos cuando hablamos de vigilancia en la era digital.

2.2. La problemática de los metadatos

Los 13 Principios dejan claro la necesidad de proteger los metadatos y todo tipo de información privada sujeta de protección. Esta información, sujeta de protección, es definida por los Principios como "toda información que incluye, refleja, surge de, o se refiere a las comunicaciones de una persona y que no está fácilmente disponible y accesible para el público en general."[31]

Como mencionamos anteriormente, los metadatos pueden incluir la ubicación del teléfono celular, datos de navegación, y los registros de búsqueda, y es tan invasiva (o tal vez más) que la lectura del contenido de un correo electrónico o el escuchar las llamadas telefónicas en tiempo real. Lo importante no es la calidad técnica del tipo de datos que se recolecta, sino el efecto de esa información sobre la privacidad de la personas.

Por lo tanto, la ley debe exigir altos estándares para el acceso del gobierno a estos datos en procesos penales. Esto significa que la solicitud sea necesaria, idónea y proporcional, previa orden judicial emitida por un tribunal (u otra autoridad judicial imparcial e independiente), siempre que el acceso revele información privada acerca de las comunicaciones individuales. Esto incluye revelar la identidad de una persona si los datos no son públicos; quién se ha comunicado con quién; cuándo, desde dónde, por cuánto tiempo, entre otros metadatos.

Teniendo en cuenta las capacidades de vigilancia de comunicaciones actuales es necesario que los metadatos sean tratados con el mismo nivel de protección que el contenido de las comunicaciones. Al respecto la Alta Comisionada de Derechos Humanos ha aclarado en su informe sobre la privacidad en la era digital que:

> 19. En la misma línea, se ha sugerido que la interceptación o la recopilación de datos acerca de una comunicación, en contraposición al contenido de la comunicación, no constituyen en sí mismas una injerencia en la vida privada. Desde el punto de vista del derecho a la privacidad, esa distinción no es convincente. La agregación de la información comúnmente conocida como "metadatos" puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada. [...] El reconocimiento de esa evolución ha dado lugar a iniciativas para reformar las políticas y prácticas existentes a fin de asegurar una mayor protección de la privacidad.[32]

31 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, "Principio de Proporcionalidad", (2013).

32 Navy Pillay, *Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.*

Entonces, para evaluar la necesidad, idoneidad y proporcionalidad de una medida de vigilancia es importante primero comprender el carácter invasivo de la misma al revelar información protegida y la finalidad para la que el Estado desea dicha información. En otras palabras, debemos asegurarnos que la legislación alusiva a la vigilancia de las comunicaciones proteja la privacidad en todos sus aspectos y dimensiones.

Los Principios Necesidad y Proporcionalidad resuelven este problema aclarando en la sección definiciones cuál es la información protegida o la información sujeta de protección legal.

2.3. De por qué monitorear los datos de alguien es vigilancia

Gran parte de la vigilancia estatal a gran escala revelada en los últimos años depende de la confusión sobre si se ha producido una vigilancia real. Algunos han sugerido que si la información solo es recolectada más no vista por una persona, no se ha producido una invasión de la privacidad. Otros argumentan que las computadoras que analizan todas las comunicaciones en tiempo real, por palabras claves y otros selectores, no es vigilancia. Estas interpretaciones pueden ser la diferencia entre la vigilancia proporcional y particularizada versus la vigilancia masiva de la población entera. Las definiciones importan.

Es por eso que los 13 Principios han dejado claro que la "Vigilancia de las Comunicaciones" comprende el monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas.[33]

Sobre esta materia, la Alta Comisionada de Derechos Humanos señaló que toda captura de datos es potencialmente una injerencia en la vida privada, independientemente si luego se consultan o utilizan esos datos.[34]

La actualización del informe de 2007 de la Comisión de Venecia sobre el control democrático de los servicios de seguridad y el informe sobre la supervisión democrática para las agencias de señales de inteligencia de 2015 dio luces al tema, confirmando que el término vigilancia estratégica a menudo se utiliza para indicar que la inteligencia de señales (*signal intelligence)* incluye el monitoreo de comunicaciones ordinarias.[35]

33 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, "Principio de Proporcionalidad", (2013).

34 Navy Pillay, *Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, párrafo 20.

35 Concilio de Europa, *Comisión Europea para la Democracia a través de la ley, actualización del informe de 2007 de la Comisión de Venecia sobre el control democrático de los servicios de seguridad y el informe sobre la supervisión democrática para las agencias de señales de inteligencia de 2015* (Estrasburgo: Concilio de Europa, 2015), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//ES (consultado: 16 noviembre, 2015)

El Dr. Ben Emerson, Relator para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, se suma a los comentarios de la Alta Comisionada explicando:

> 55. Al aplicar el enfoque adoptado por el Tribunal de Justicia de la Unión Europea se desprende que la recopilación y conservación de los datos de tráfico de las comunicaciones constituye una injerencia en el derecho a la privacidad, independientemente de si posteriormente una autoridad pública accede a ellos y los analiza o no.[36]

Esto se establece con claridad en la Sentencia de la Corte Europea de Derechos Humanos, Amman versus Suiza del 16 de febrero del 2000 como citamos a continuación:

> 69. La Corte reitera que el almacenamiento por una autoridad pública de información relativa a la vida privada de una persona equivale a una injerencia en el sentido del artículo 8. El posterior uso de la información almacenada no influye en esta apreciación [...][37]

En la sentencia de la Corte Europea, S y Marper v Reino Unido del 04 de Diciembre del 2008, una vez más la Corte dejo claro:

> 121. El Gobierno sostiene que la retención no puede ser considerada como si tuviera un efecto directo o significativo en los demandantes a menos que la coincidencia con la base de datos fueran a implicarlos en la comisión de un delito en una ocasión futura. El Tribunal no es capaz de aceptar este argumento y reitera que la mera retención y almacenamiento de datos personales por las autoridades públicas, no obstante su obtención, han de ser considerados como teniendo un directo impacto en la vida privada del individuo en cuestión, independientemente si posteriormente se hace uso de los datos [...][38]

Los 13 Principios recogen los antecedentes previos y definen en la sección de "Cambios Tecnológicos y Definiciones" qué significa vigilancia en el entorno moderno y qué significa comunicaciones en la era digital para así dejar sentado el ámbito de aplicación de los estándares de derechos humanos en el contexto de la vigilancia.

2.4. Protejamos la infraestructura de internet

Los 13 Principios sostienen la necesidad de proteger la infraestructura critica de internet. Ninguna ley debe imponer agujeros de seguridad en nuestra tecnología con el fin de facilitar la vigilancia.

36 Ben Emerson, *Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*.
37 Corte Europea de Derechos Humanos. Sentencia Amman versus Suiza del 16 de febrero de 2000, 69.
38 Corte Europea. Sentencia S y Marper v Reino Unido del 04 de diciembre de 2008, 121.

Al respecto, la Alta Comisionada expresó su opinión diciendo: "42. [...] La promulgación de leyes que obligan a las empresas a preparar sus redes para la interceptación es motivo de especial preocupación, en particular porque crea un ambiente que facilita las medidas de vigilancia exhaustiva."[39]

Banalizar la seguridad de cientos de millones de personas inocentes que dependen de tecnologías seguras con la finalidad de garantizar la capacidad estatal de vigilancia contra unos pocos delincuentes es una política miope y perversa. El supuesto que subyace a esos esfuerzos, que ninguna comunicación puede ser realmente segura, es incoherentemente peligrosa, pues deja a la gente inocente a merced de la policía como también de los criminales.

2.5. La necesidad de respetar el objetivo legítimo

La realidad moderna ha mostrado gracias a las revelaciones de Snowden, que las agencias de inteligencia de Estados Unidos y Reino Unido están involucradas en un ámbito mucho más amplio que las actividades de vigilancia relacionadas con la seguridad nacional o la lucha contra el terrorismo. Por ejemplo, en los Estados Unidos la NSA y sus socios han utilizado sus poderes expansivos de espionaje con motivos políticos y económicos que poco tienen que ver con la seguridad del Estado y sus ciudadanos. Peor aún, recientemente ha sido revelado que la información recogida por las agencias de inteligencia de los Estados Unidos es rutinariamente reutilizada, en secreto, por agencias del orden como la Agencia de Control de Drogas (DEA por sus siglas en inglés), pasando por alto de manera efectiva los controles y equilibrios impuestos a esos organismos nacionales.

El informe de la Alta Comisionada de Derechos Humanos enfatiza este punto, señalando:

> Muchos marcos nacionales carecen de "limitaciones de uso", permitiendo así la recopilación de datos para un objetivo legítimo, pero su uso posterior para otros. La inexistencia de limitaciones de uso efectivas se ha exacerbado desde el 11 de septiembre de 2001, y la línea que separa la justicia penal de la protección de la seguridad nacional se ha difuminado significativamente. El intercambio resultante de datos entre las fuerzas del orden, los organismos de inteligencia y otros órganos del Estado corre el riesgo de violar el artículo 17 del Pacto, ya que las medidas de vigilancia que pueden ser necesarias y proporcionadas para un objetivo legítimo pueden no serlo para otros fines.[40]

Los 13 Principios concuerdan al estipular que la vigilancia debe ser necesaria y proporcional al objetivo que se pretende abordar. Igualmente importante, los Principios prohíben la reutilización sin restricciones de información. En otras palabras, prohíbe que la agencia de inteligencia comparta con una agencia policial información que fue recolectada para un propósito específico (seguridad nacional) y luego fue reutilizada para un propósito distinto (combatir o prevenir el crimen).

39 Navy Pillay, *Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.*
40 Navy Pillay, *Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*.

2.6. No a la complicidad de las empresas tecnológicas

Los 13 Principios aclaran que no hay margen para la cooperación voluntaria de las empresas de tecnología y agencias de inteligencia o la policía a menos que exista una orden judicial que cumpla con los principios de legalidad, necesidad, idoneidad y proporcionalidad.

El reporte de la Alta Comisionada Navy Pillay construye sobre este punto afirmado las obligaciones que las empresas tienen cuando existen excesos en las solicitud de vigilancia:

> 43. [...] Los Principios Rectores sobre las empresas y los derechos humanos, aprobados por el Consejo de Derechos Humanos en 2011, proporcionan un marco internacional para prevenir y combatir los efectos adversos vinculados con las actividades empresariales en los derechos humanos. La responsabilidad de respetar los derechos humanos se aplica a todas las operaciones de la empresa en todo el mundo, independientemente de la ubicación de sus usuarios, y existe independientemente de si el Estado cumple con sus obligaciones de derechos humanos.[41]

2.7. Las reglas del juego deben ser conocidas por todas y todos

Los 13 Principios dejan claro que la base legal y la interpretación de los poderes de vigilancia deben ser públicas. La falta de transparencia en las leyes y prácticas de vigilancia reflejan una falta de cumplimiento de los derechos humanos y el imperio de la ley.

Al respecto la Alta Comisionada concuerda dejando claro que las normas y las interpretaciones secretas no cumplen con los requisitos necesarios para considerarse ley: “29. Por consiguiente, las normas y las interpretaciones secretas —incluso las interpretaciones judiciales secretas— del derecho no cumplen los requisitos necesarios para considerarse "ley"[42]." Lo mismo sucede con las leyes o normas que conceden a las autoridades ejecutivas, como los servicios de seguridad e inteligencia, una facultad discrecional excesiva; el alcance de la facultad discrecional otorgada y la manera de ejercerla deben indicarse (en la propia ley o en directrices vinculantes publicadas) con una claridad razonable.

Las leyes secretas, sobre vigilancia o cualquier otra aspecto, son inaceptables. El Estado no debe adoptar o aplicar una práctica de vigilancia sin el derecho del público de conocer sus límites. Por otra parte, la ley debe ser lo suficientemente clara y precisa, asegurando además que los individuos están enterados de su existencia y que pueden prever su aplicación. Cuando las personas no conocen la existencia de una norma, su interpretación o su aplicación, es efectivamente secreta. Una norma secreta no es una norma legal.

41 Navy Pillay, *Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*.
42 CCPR/C/USA/CO/4, párr. 22.

2.8. Notificación y derecho al remedio efectivo

Antes de internet, la policía llamaba a la puerta de la afectada por la medida de vigilancia, mostraba su orden judicial, y le proporcionaba una razón para allanar su casa. La afectada podría ver la búsqueda que se producía y si la información recogida iba más allá del alcance de la orden judicial.

La vigilancia electrónica, sin embargo, es mucho más sutil y subrepticia. Los datos pueden ser interceptados o almacenados directamente por una empresa intermediaria de las comunicaciones, desde proveedoras de servicios de telecomunicaciones (Telefónica, Claro) hasta proveedoras de contenido (Facebook o Twitter) sin que el individuo se entere. Por lo tanto, a menudo es imposible saber si una ha estado sujeta a una medida de vigilancia, a menos que la evidencia conduzca a cargos criminales. Como resultado las personas inocentes son las menos propensas a descubrir que su privacidad ha sido invadida.

El principio de notificación recogido por los 13 Principios es clave en la lucha contra la vigilancia ilegal o su extralimitación. El Principio de Notificación consiste en notificar a la persona afectada la solicitud de vigilancia con el tiempo y la información suficiente para que ella pueda apelar la decisión, excepto si pone en peligro la investigación en cuestión. Las personas incluso deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización.

Sorprendentemente, el informe de la Alta Comisionada de Derechos Humanos estableció ciertas características que los recursos efectivos por las violaciones de la privacidad mediante actividades de vigilancia deben cumplir. Esos recursos deben ser "conocidos y accesibles para cualquier persona que afirme de manera defendible que se han violado sus derechos[43]", Esto significa que el aviso es de vital importancia y que la gente debe ser advertida para impugnar la legalidad del programa de vigilancia sin tener que demostrar que su comunicación en particular fue vigilada o recolectada:

> 40. Los recursos efectivos por las violaciones de la privacidad mediante actividades de vigilancia digital pueden tener diversas formas judiciales, legislativas o administrativas, aunque suelen compartir ciertas características. En primer lugar, esos recursos deben ser conocidos y accesibles para cualquier persona que afirme de manera defendible que se han violado sus derechos. Por lo tanto, la notificación (de que se ha creado un régimen de vigilancia general o medidas de vigilancia específicas) y la legitimación (para impugnar tales medidas) se convierten en cuestiones fundamentales para determinar el acceso a un recurso efectivo. Los Estados adoptan diferentes enfoques de la notificación: mientras que algunos requieren la notificación *a posteriori* a las personas objeto de vigilancia, una vez que concluyen las investigaciones, muchos regímenes no prevén la notificación.[44]

43 Incluir cita del informe de la Alta Comisionada.

44 Navy Pillay, *Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*.

En efecto, cualquier retraso en la notificación tiene que ser autorizada por un tribunal y proceder siempre que exista un riesgo real para la investigación en cuestión o daño a la persona.

2.9. Restaura el principio de proporcionalidad y necesidad

La vigilancia de las comunicaciones es un acto altamente intrusivo que interfiere con las libertades fundamentales y amenaza los cimientos de una sociedad democrática. Por ello, toda autorización que faculta el poder ejercer la vigilancia debe contar con la aprobación previa de una entidad judicial independiente e imparcial que determine si ese acto específico de vigilancia cumple con el requisito de proporcionalidad.

Para aclarar esta materia, citamos a la Alta Comisionada de Derechos Humanos, Navy Pillay, donde ella explicó (el subrayado es nuestro):

> 25. En relación con la necesidad de una medida, el Comité de Derechos Humanos, en su Observación general Nº 27, sobre el artículo 12 del Pacto Internacional de Derechos Civiles y Políticos, destacó que "l*as restricciones no deben comprometer la esencia del derecho* […]; no se debe invertir la relación entre derecho y restricción, entre norma y excepción"[45]. El Comité explicó además que "no basta con que las restricciones se utilicen para conseguir fines permisibles; deben ser necesarias también para protegerlos". Por otro lado, las medidas deben ser proporcionadas: "el instrumento menos perturbador de los que permitan conseguir el resultado deseado"[46]. Cuando existe un objetivo legítimo y se han establecido las salvaguardias apropiadas, puede permitirse a un Estado realizar actividades de vigilancia bastante perturbadoras; sin embargo, incumbe al gobierno demostrar que la injerencia es necesaria y proporcional al riesgo concreto de que se trate. Así pues, los *programas de vigilancia en masa o "a granel" pueden considerarse arbitrarios, aunque persigan un objetivo legítimo y hayan sido aprobados sobre la base de un régimen jurídico accesible*. En otras palabras, no es suficiente que las medidas tengan por objeto encontrar determinadas agujas en un pajar; *lo importante es el impacto de las medidas en el pajar, en comparación con el riesgo de que se trate; es decir, si la medida es necesaria y proporcionad*a.[47]

Nos parece importante citar al respecto al Dr. Ben Emerson, Relator para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en las Naciones Unidas, quien se posicionó contra la vigilancia masiva a gran escala:

> 18. Suponiendo, por consiguiente, que sigue existiendo un derecho al respeto de la privacidad de las comunicaciones digitales [y esto no puede negarse [véase la resolución 68/167 de la Asamblea General]], la adopción de tecnología de *vigilancia a gran escala sin duda menoscaba la esencia misma de ese derecho* [véanse los párrs. 51 y 52]. Su uso es

45 CCPR/C/21/Rev.1/Add.9, párrs. 11 a 16. Véase también Tribunal Europeo de Derechos Humanos, *Handyside v. the United Kingdom*, párr. 48; y *Klass v. Germany*, párr. 42.
46 CCPR/C/21/Rev.1/Add.9, párrs. 11 a 16.
47 Navy Pillay, *Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*.

> potencialmente incompatible con el principio básico de que los Estados adopten los medios menos perturbadores disponibles cuando invaden los derechos humanos protegidos [véase el párr. 51], excluye cualquier evaluación individualizada de la proporcionalidad [véase el párr. 52], y está rodeado de argumentos de confidencialidad que dificultan enormemente cualquier otro tipo de análisis de proporcionalidad [véanse los párrs. 51 y 52]. Los Estados que realizan vigilancia a gran escala hasta ahora no han conseguido justificar públicamente su necesidad en detalle y con pruebas, y casi ningún Estado ha promulgado legislación nacional que autorice expresamente su uso [véase el párr. 37].
>
> Desde el punto de vista del artículo 17 del Pacto, esto prácticamente equivale a derogar por completo el derecho a la privacidad de las comunicaciones digitales. Por estos motivos, la vigilancia a gran escala de los datos de tráfico y de contenido de las comunicaciones digitales es una gran amenaza para una norma establecida del derecho internacional [...].[48]

La actualización del informe de 2007 de la Comisión de Venecia sobre el control democrático de los servicios de seguridad y el informe sobre la supervisión democrática para las agencias de señales de inteligencia del 2015 se pronunció sobre el tema, sosteniendo:[49]

> 35. [...] Inteligencia de Señales o SIGINT es un término colectivo que se refiere a medios y métodos para la interceptación y análisis de la radio (incluyendo satélite y teléfono celular) las comunicaciones por cable y transmitidas. Tradicionalmente, la inteligencia de señales se utiliza principalmente para obtener inteligencia militar y, en segundo lugar, la inteligencia extranjera o diplomática. Por lo tanto, era principalmente el dominio de las agencias de inteligencia militar o externos. Sin embargo, como resultado de los procesos de la globalización, junto con la creación de la Internet, la frontera entre seguridad interior y exterior ya no es tan clara. Además, al menos desde los ataques terroristas del 11 de septiembre de 2001, se ha llegado a entender que las amenazas significativas a la seguridad nacional pueden ser planteadas por los actores no estatales... [...][50]

En la Sentencia del caso S and Marper v United Kingdom del 4 de diciembre de 2008, la Corte Europea de Derechos Humanos se pronunció sobre la naturaleza indiscriminada de la retención de datos:

> 119. En este sentido, la Corte es sacudida por la naturaleza indiscriminada de la fuerza de la retención en Inglaterra y Gales. El material puede ser retenido con independencia de la naturaleza o la gravedad de la infracción que origino que se sospechara originalmente del individuo o de la edad del presunto delincuente; huellas dactilares y muestras se pueden tomar - y retenidos - de una persona de cualquier edad, detenido en relación con una falta registrable, que incluye delitos menores o no sancionables con prisión. La retención

48 Véase A/HRC/27/37, párr. 25, en el que la Alta Comisionada para los Derechos Humanos observó que "no es suficiente que las medidas tengan por objeto encontrar determinadas agujas en un pajar; lo importante es el impacto de las medidas en el pajar, en comparación con el riesgo de que se trate; es decir, si la medida es necesaria y proporcionada."

49 Concilio de Europa, *Comisión Europea para la Democracia a través de la ley, actualización del informe de 2007 de la Comisión de Venecia sobre el control democrático de los servicios de seguridad y el informe sobre la supervisión democrática para las agencias de señales de inteligencia de 2015,*18.

50 *Concilio de Europa, Comisión Europea para la Democracia a través de la ley, actualización del informe de 2007 de la Comisión de Venecia*, 35.

> no es limitada en el tiempo; el material se conserva indefinidamente cualquiera que sea la naturaleza o gravedad de la infracción de la que se sospechó la persona. Por otra parte, existen pocas posibilidades para un individuo absuelto a tener los datos extraídos de la base de datos nacional o los materiales destruidos (véase el párrafo 35 supra); en particular, no existe ninguna disposición para una revisión independiente de la justificación de la retención de acuerdo con los criterios definidos, incluyendo factores tales como la gravedad de la infracción, las detenciones anteriores, la fuerza de la sospecha contra la persona y cualquier otras circunstancias especiales.[51]

El Principio de Proporcionalidad requiere que el Estado demuestre como mínimo, que (1) Exista un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo; (2) Exista un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la la Información Protegida; (3) Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica; (4) La información a la que se accederá estará limitada a lo relevante y material para el serio crimen o la amenaza especifica al fin legitimo alegado; (5) Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud; (6) La información será accesada solo por la autoridad especifica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización, y (7) Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales."[52]

2.10. No a la discriminación entre nacionales y extranjeros

Los Estados pueden conducir la vigilancia de las comunicaciones dentro y fuera de sus fronteras. Sin embargo, el marco jurídico interno de algunos países otorgan mayor protección a los derechos de privacidad de los ciudadanos y residentes frente a los no ciudadanos y no residentes. Como resultado, muchos gobiernos se involucran de manera rutinaria en la vigilancia masiva a gran escala de las comunicaciones internacionales. Sobre este tema es importante recalcar que la Alta Comisionada de Derechos Humanos ha aclarado en su informe sobre la privacidad en la era digital[53] que todos y todas son iguales ante la ley:

> 36. El derecho internacional de los derechos humanos es explícito en relación con el principio de no discriminación. El artículo 26 del Pacto Internacional de Derechos Civiles y Políticos dispone que "todas las personas son iguales ante la ley y tienen derecho sin discriminación a igual protección de la ley" y añade que, "a este respecto, la ley proscribirá toda discriminación y garantizará a todas las personas protección igual y efectiva contra cualquier discriminación

51 Veáse: http://hudoc.echr.coe.int/eng?i=001-90051

52 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, "Principio de Proporcionalidad", (2013).

53 Navy Pillay, I*nforme de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*.

por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social.

Esas disposiciones deben leerse juntamente con el artículo 17, que establece que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada" y que "toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques", así como con el artículo 2, párrafo 1. En este sentido, el Comité de Derechos Humanos ha subrayado la importancia de adoptar "medidas para que toda interferencia en el derecho a la intimidad se ajuste a los principios de legalidad, proporcionalidad y necesidad, con independencia de la nacionalidad o el emplazamiento de las personas cuyas comunicaciones estén bajo vigilancia directa.[54]

En la opinión del Relator para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, Ben Emerson explicó:

43. Este trato diferenciado en cualquiera de sus dos formas es incompatible con el principio de no discriminación previsto en el artículo 26 del Pacto, principio que también es inherente a la noción misma de proporcionalidad[55]. Además, el uso de programas de vigilancia a gran escala para intervenir las comunicaciones de quienes se encuentran en otras jurisdicciones suscita serios interrogantes sobre la accesibilidad y la previsibilidad de las leyes que rigen la injerencia en el derecho a la privacidad, y sobre la imposibilidad de que las personas sepan que podrían ser objeto de vigilancia extranjera o que sus comunicaciones podrían ser intervenidas en jurisdicciones extranjeras. El Relator Especial considera que los Estados están obligados jurídicamente a proporcionar igual protección a ciudadanos y extranjeros, y a quienes se encuentren dentro y fuera de su jurisdicción.

62. El Relator Especial está de acuerdo con la Alta Comisionada para los Derechos Humanos en que cuando los Estados penetran la infraestructura que se encuentra fuera de su jurisdicción territorial, siguen estando sujetos a las obligaciones que les incumben en virtud del Pacto. Además, el artículo 26 del Pacto prohíbe la discriminación por motivos de nacionalidad y ciudadanía, entre otros. Por lo tanto, el Relator Especial considera que los Estados están obligados jurídicamente a proporcionar igual protección de la privacidad a ciudadanos y extranjeros, y a quienes se encuentren dentro y fuera de su jurisdicción. Los regímenes de protección asimétrica de la privacidad constituyen una violación flagrante de los requisitos del Pacto.[56]

54 CCPR/C/USA/CO/4, párr. 22.

55 “El Comité de Derechos Humanos también destacó la importancia de que se adopten “medidas para que toda interferencia en el derecho a la intimidad se ajuste a los principios de legalidad, proporcionalidad y necesidad, con independencia de la nacionalidad o el emplazamiento de las personas cuyas comunicaciones estén bajo vigilancia directa”, CCPR/C/USA/CO/4, párr. 22 a). Ben Emerson. *Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*.

56 Ben Emerson, *Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*.

3. Anonimato[57]

3.1. Concepto

El anonimato se puede definir como el actuar o comunicarse con otra persona sin usar o presentar el nombre o identidad propia. También puede ser definido como actuar o comunicarse de una manera que se proteja el nombre o identidad propia, usando un nombre asumido o inventado que no puede necesariamente asociarse con la identidad legal o habitual de uno.[58]

El anonimato puede ser concebido como un espectro de fuerte a débil. Es fuerte cuando existen protecciones técnicas y legales que hacen que sea muy difícil desenmascarar la identidad de una persona anónima. El anonimato es débil cuando una persona anónima puede ser desenmascarada mediante métodos sencillos, tales como solicitudes gubernamentales al proveedor de servicio o buscando el nombre asumido en una base de datos existente.

A lo largo de la historia, las personas se han comunicado anónimamente. En el siglo XVIII, James Madison, Alexander Hamilton y John Jay asumieron el seudónimo de Publio cuando publicaron los Documentos Federales (*The Federalist Papers*). En el siglo XIX en Inglaterra, las hermanas Brontë utilizaron seudónimos para publicar bajo los nombres de Currer, Ellis y Acton Bell, nombres de hombres que le permitía a ellas ser tomadas como escritores serios.[59] Actualmente, el anonimato de las comunicaciones es uno de los "adelantos más importantes facilitados por Internet, que permite a las personas expresarse libremente sin temor a represalias o condenas."[60]

3.2. Protección del anonimato

La libertad de expresión es reforzada cuando uno puede hacerlo anónimamente. Existen muchas circunstancias donde una persona no hablará por temor a represalias, por un desequilibrio de poder inherente, u otra razón, o una asociación de individuos no hablará a menos que esté segura de proteger la identidad de sus miembros.

---

57 Esta sección ha sido reproducida parcialmente del informe publicado por la autora, Katitza Rodríguez, *Anonimato y Cifrado: Comentarios enviados a la Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión.*

58 Algunas fuentes distinguen entre anonimato (no usar nombre alguno) y seudónimo (usar un nombre asumido), sin embargo, para el propósito de esta presentación no hacemos distinción alguna. En la práctica, los seudónimos digitales requieren de un anonimato fuerte o débil como parte del proceso de separar el nombre asumido de los detalles de la identidad de la persona.

59 Jillian York. *The Right to Anonymity is a Matter of Privacy*, (EFF, 2012), https://www.eff.org/deeplinks/2012/01/right-anonymity-matter-privacy (consultado: 16 noviembre, 2015)

60 Frank La Rue. *Informe anual de la Relatoría Especial de Naciones Unidas para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, A/HRC/23/40*, (2013), párr. 23, http://www.hiperderecho.org/wp-content/uploads/2015/09/carta_relator_cidh_ley_stalker.pdf

La capacidad de leer y acceder a información anónimamente es también crucial para el ejercicio de la libre expresión. El artículo 19 de la Declaración Universal de Derechos Humanos, que consagra el derecho a la libertad de opinión y de expresión, incluye el derecho a buscar, recibir e impartir información e ideas a través de cualquier medio.

Esta inclusión es necesaria porque no puede haber una protección significativa a la libertad de expresión de los ciudadanos si ellos carecen del derecho a leer y comunicarse anónimamente. La doctrina internacional explica que "la interdependencia cercana entre la recepción y expresión de información y entre la lectura y la libertad de pensamiento hacen del reconocimiento de ese derecho [el derecho a leer anónimamente] una buena política constitucional.[61]

La Relatoría Especial de Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) dejó claro que: "en todos los casos, los usuarios deben tener derecho a permanecer bajo anonimato y cualquier disputa sobre este punto debe ser resuelta exclusivamente en sede judicial".[62]

En ese sentido, leyes que prohíban o fomenten indirectamente prácticas prohibitivas de anonimato *a priori* se encuentran en contraposición con lo dispuesto por la Relatoría de la CIDH.

Por su parte, la Relatoría de Libertad de Opinión y Expresión de Naciones Unidas ha dicho que "la injerencia indebida en la intimidad de las personas puede limitar en forma tanto directa como indirecta el libre intercambio y evolución de ideas."[63]

La cuestión del anonimato en línea también incorpora necesariamente preocupaciones respecto a la expresión y la privacidad, y el cuidadoso análisis de la interacción entre ambos derechos. Como se indica en el Informe de 2011 de la Relatoría Especial de Naciones Unidas sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión, "El derecho a la privacidad es esencial para que las personas se expresen libremente".[64]

La Declaración de la Libertad para la Comunicación en Internet del Consejo de Europa ha dejado claro que "con el fin de garantizar la protección contra la vigilancia en línea y para mejorar la libre expresión de información e ideas, los Estados Miembros deben respetar la voluntad de los usuarios de Internet de no revelar su identidad".[65]

---

61 Julie Cohen, "A Right to Read Anonymously: A Closer Look at "Copyright Management". *In Cyberspace*, 1996, 28 CONN. L. REV. 981.

62 CIDH, I*nforme de la relatoría especial para la libertad de expresión. Capítulo IV. OEA /Serv.L/V/II.149,* (2013), párr. 109, http://www.oas.org/es/cidh/docs/anual/2013/informes/LE2013-esp.pdf (consultado: 16 noviembre, 2015)

63 Frank La Rue, *Informe de la Relatoría Especial de Naciones Unidas para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión*, párr. 49,.

64 Frank La Rue, *Informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión,* p. 15,

65 Consejo de Europa, Declaration on Freedom of Communication on the Internet, Principio 7, (Consejo de Europa, 2003), https://wcd.coe.int/ViewDoc.jsp?id=37031 (consultado: 16 noviembre, 2015)

En un reciente informe de la Relatoría de Libertad de Opinión y Expresión de Naciones Unidas, se explica la interrelación entre seguridad, privacidad y anonimato:

> El cifrado y el anonimato, actualmente las principales vías de seguridad en línea, ofrecen a las personas un medio para proteger su privacidad, al permitirles buscar, leer, elaborar y compartir opiniones e información sin injerencia y al permitir a periodistas, organizaciones de la sociedad civil, miembros de grupos étnicos o religiosos, personas perseguidas debido a su orientación sexual o su identidad de género, activistas, eruditos, artistas y otros ejercer los derechos a la libertad de opinión y de expresión.[66]

3.3. Restricciones al anonimato

El anonimato está protegido bajo el derecho a la libertad de expresión, este no puede restringirse *a priori* sino bajo responsabilidades ulteriores.

La divulgación forzada de la identidad de un usuario anónimo solo debe ocurrir una vez que se haya cometido un delito. Los derechos al debido proceso de un interlocutor deben ser respetados antes de identificar a esa persona en respuesta a una solicitud de datos que permite la identificación del usuario. En este sentido, los regímenes legales deben garantizar el debido proceso y la transparencia, y que la restricción sea necesaria, idónea, proporcional y cumpla con un objetivo legítimo antes de forzar la revelación de la identidad.

La Relatoría de Libertad de Opinión y Expresión de Naciones Unidas explica el efecto que producen las restricciones al anonimato:

> "[Las restricciones producen] un efecto disuasorio, desalentando la libre expresión de información e ideas."[67] También tienen un "efecto intimidatorio en las víctimas de todas las formas de violencia y abuso, que podrían se renuentes a denunciar [abusos] por temor a la doble victimización."[68]

La Relatoría continúa su análisis explicando que el revelar la identidad puede resultar en la exclusión de personas de diversos ámbitos sociales, socavando sus derechos, y así exacerbando las desigualdades sociales.[69]

66 David Kaye, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión que aborda la utilización del cifrado y el anonimato en las comunicaciones digitales, UN Doc. A/HRC/29/32 sobre el anonimatoy el cifrado*, (2015), https://eff.org/A-HRC-29-32 (consultado: 16 noviembre, 2015)

67 Frank La Rue. *Informe de la Relatoría Especial de Naciones Unidas para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión*, párr. 49.

68 Frank La Rue. *Relator Especial de Naciones Unidas para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión*, párr. 24.

69 Frank La Rue. *Relator Especial de Naciones Unidas para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión*, párr. 49.

En las legislaciones de algunos países se restringe el anonimato en línea. Por ejemplo, la Constitución de Brasil en su artículo 5 prohíbe el discurso anónimo, lo mismo sucede con la Constitución de la República Bolivariana de Venezuela en su artículo 57. Otra forma de restricción al anonimato es el registro de tarjetas móviles *SIM*; en alrededor de 50 países en África[70] se les requiere brindar datos personales para poder activar una *SIM card*. Mientras que en el Perú todas las tarjetas deben contar con un número de identificación nacional.

70 Kevin P. Donovan and Aaron K. Martin, *The rise of African SIM registration: The emerging dynamics of regulatory change*, (2014), http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820 (consultado: 22 de noviembre, 2015).

4. Cifrado

4.1. Concepto

El cifrado es la ciencia matemática de códigos, cifras, y mensajes secretos. A través de la historia, las personas ha utilizado métodos cada vez más sofisticados de cifrado para enviarse mensajes entre sí, para proteger el contenido de personas ajenas a la conversación. Los primeros métodos de cifrado eran operaciones simples que podían realizarse a mano, como el "cifrado César" de la antigua Roma.

Hoy, tenemos computadoras que son capaces de hacer el cifrado por nosotros. La tecnología digital de cifrado se ha expandido mas allá de los mensajes secretos; actualmente, el cifrado puede ser usado para propósitos más elaborados, por ejemplo para verificar el autor de mensajes o para navegar en la web anónimamente.

4.2. Protección del cifrado

La privacidad de las comunicaciones incluye el derecho de toda persona a utilizar la tecnología de cifrado. En ausencia del cifrado, las comunicaciones en línea pueden ser fácilmente interceptadas. Los intermediarios pueden leer todas las comunicaciones que pasan a través de sus redes.

En ese escenario, los proveedores de servicios deben ser capaces de diseñar sistemas para la privacidad de extremo a extremo, ni ellos deben bloquear la transmisión de cualquier comunicación cifrada. Tanto los individuos como las agencias gubernamentales necesitan un cifrado fuerte en sus actividades diarias. Los activistas de derechos humanos, los periodistas, los refugiados, los bloggers, y los denunciantes necesitan tecnologías fuertes de cifrado para proteger sus comunicaciones, los nombres y la ubicación de sus fuentes y / o testigos, etc.

En el entorno digital, la libertad de utilizar la tecnología de cifrado es a menudo un pre-requisito para el ejercicio de los derechos de privacidad y de expresión.[71] En la ausencia de cifrado, las comunicaciones pueden ser fácilmente interceptadas.[72] Debido a la forma en que internet se ha desarrollado, los

71 David Kaye, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión que aborda la utilización del cifrado y el anonimato en las comunicaciones digitales, UN Doc. A/HRC/29/32 sobre el anonimatoy el cifrado*, (2015), https://eff.org/A-HRC-29-32 (consultado: 22 noviembre, 2015)

72 Véase, por ejemplo Firesheep, disponible en: http://codebutler.com/firesheep
Véase también John P. Mello Jr. *Free Tool Offered To Combat Firesheep Hackers*, (PCWorld, s.f.), http://www.pcworld.com/article/211531/free_tool_offered_to_combat_firesheep_hackers (consultado: 16 noviembre, 2015)
Seth Schoen, Richard Esguerra, *The Message of Firesheep: "Baaaad Websites, Implement Sitewide HTTPS Now!* (EFF, 2010), http://www.eff.org/deeplinks/2010/10/message-firesheep-baaaad-websites-implement (consultado: 16 noviembre, 2015)
EFF, *Tool Offers New Protection Against 'Firesheep'*, (EFF, 2010), https://www.eff.org/press/archives/2010/11/23 (consultado: 16 noviembre, 2015)

intermediarios de este que almacenan y reenvían nuestras comunicaciones están a menudo en condiciones de poseer y leer todas las comunicaciones que pasan a través de sus redes. Con el fin de preservar la seguridad y la privacidad de sus usuarios, los proveedores de servicios deben ser capaces de diseñar sistemas que aseguren la privacidad de extremo a extremo, es decir, sistemas que aseguren que un mensaje puede ser leído por su destinatario y nadie más.

La libertad de expresión tiene varias intersecciones con el derecho a desarrollar y usar tecnología de cifrado. Esta protege directamente la expresión impidiendo que los sistemas técnicos automatizados de censura bloqueen el acceso a un contenido en particular (o incluso a palabras clave particulares). También protege la expresión indirectamente brindando confianza a los usuarios sobre la confidencialidad de sus comunicaciones polémicas o de sus decisiones controvertidas de lectura, ya que están protegidos por medios técnicos.

Los desarrollares de software de cifrado se dedican a su propia actividad expresiva cuando publican código de cifrado. Cualquier intento de prohibir el uso de cifrado también iría en contra de la libertad de expresión de los programadores. Muchos programas más robustos de cifrado "extremo a extremo" son software libre, su código es público y está disponible desde la red para que cualquier persona los descargue desde una amplia variedad de fuentes. Si un Estado intenta prohibir estos programas, tendría que controlar el acceso a esta información, prohibir la publicación, o instituir la infraestructura necesaria para detectar y penalizar su uso. Todos estos métodos serían considerados censura previa, y por ende violatorio de los estándares interamericanos en materia de libertad de expresión.

4.3. Restricciones al cifrado

En un reciente informe del Relator Especial para la Promoción y Protección de la Libertad de Expresión y Opinión, David Kaye reconoce que el cifrado y el anonimato son fundamentales a la libertad de expresión y el derecho a la privacidad. Señala que las restricciones al cifrado deben cumplir con la prueba tripartita desarrollada en el derecho internacional:

> 31. Las restricciones a el cifrado y anonimato, como facilitadores del derecho a la libertad de expresión, deben cumplir con la prueba de los tres pasos bien conocida por todos: toda limitación sobre la expresión debe ser establecida por la ley; sólo podrá ser impuesta por motivos legítimos (como se establece en el artículo 19 (3) del Pacto); y debe ajustarse a las estrictas pruebas de necesidad y proporcionalidad.[73]

73 David Kaye, *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión que aborda la utilización del cifrado y el anonimato en las comunicaciones digitales, UN Doc. A/HRC/29/32 sobre el anonimatoy el cifrado*, (2015), https://eff.org/A-HRC-29-32 (consultado: 16 noviembre, 2015)

Algunos Estados han tratado de controlar el uso del cifrado. Entre los mecanismos de control se encuentran la obligación de requerir licencias para la exportación de las herramientas de cifrado.[74] Cuando establecen las últimas dos medidas los gobiernos pueden controlar e influir en la complejidad del cifrado.

En algunos países se han atribuido presunciones legales a quienes usan o enseñan el uso del cifrado. Por ejemplo, a los *blogueros* Zona 9 de Etiopía se les procesó penalmente por la intención de realizar capacitaciones en temas de seguridad de la información y uso del cifrado.[75] Los Estados erosionan los derechos de privacidad y expresión cuando penalizan a aquellos que brindan herramientas para permitir el acceso y ofrecer protección en línea a activistas.[76]

74 Ben Emerson, *Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*, párra. 46.

75 Sarah Myers West, *Ethiopian Arrests for Internet Security Training Undermine Right to Privacy,* (EFF, 2015), https://www.eff.org/es/deeplinks/2015/07/ethiopian-arrests-internet-security-training-undermine-right-privacy (consultado: 16 noviembre, 2015)

76 Ben Emerson, I*nforme del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*, parr. 46.

5. Conclusiones

Los 13 Principios proporcionan un marco básico para garantizar el Estado de derecho, la supervisión publica y las salvaguardas de las libertades fundamentales frente a la vigilancia del Estado. También dejan clara la necesidad de la rendición de cuentas, con sanciones por el acceso ilegal y protecciones fuertes y eficaces para los denunciantes. Es necesario revisar la legislación en cada país y asegurarnos que las fuertes protecciones legales del derecho internacional de los derechos humanos en el contexto de la vigilancia estén presentes en ella. Por ello es necesario interpretar y aplicar los estándares internacionales en materia de derechos humanos a la luz de los nuevos avances tecnológicos y cambios en los patrones de comunicación, y hacerlo con la intención de proteger los derechos humanos. Como siempre, tenemos que poner en práctica estas protecciones en la legislación interna de cada país para garantizar que el derecho a la vida privada se encuentre también garantizado en la era digital.

Pero mientras que los Principios están dirigidos a los Estados, la acción del gobierno no es la única manera de combatir la extralimitación de la vigilancia.

Todas las empresas de comunicación, internet y telecomunicaciones por igual, pueden ayudar a asegurar sus redes y limitar la información que recogen. Los proveedores de servicios en línea debe recolectar la cantidad mínima de información durante el tiempo mínimo que se necesita para llevar a cabo sus operaciones, y luego ofuscar efectivamente, agregar y eliminar la información que no sea necesaria. Después de todo, si hay menos datos recolectados por la empresas, hay menos que entregar al Estado. El Estado también debe asegurarse de garantizar la protección de datos de todas las personas, adoptando normas de protección de datos comprensivas que efectivamente protejan la privacidad de los usuarios.

Anexo I

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones

VERSIÓN FINAL 10 DE MAYO DE 2014

A medida que avanzan las tecnologías que facilitan la vigilancia estatal de las comunicaciones, los Estados están fallando en garantizar que las leyes, normas, actividades, poderes y autoridades relacionadas con la Vigilancia de las Comunicaciones se adhieran a las normas y estándares internacionales de derechos humanos. Este documento intenta clarificar cómo se aplica el derecho internacional de los derechos humanos en el actual entorno digital, en particular a la luz del aumento y de los cambios que están teniendo las tecnologías y técnicas de Vigilancia de las Comunicaciones. Estos principios pueden proporcionar a los grupos de la sociedad civil, a la industria y a los Estados un marco para evaluar si las leyes y prácticas de vigilancia, actuales o propuestas, están en línea con los derechos humanos.

Estos principios son el resultado de una consulta global con grupos de la sociedad civil, con la industria y expertos internacionales en legislación sobre Vigilancia de las Comunicaciones, políticas públicas y tecnología.

PREÁMBULO

La intimidad es un derecho humano fundamental y es cardinal para el mantenimiento de sociedades democráticas. Es esencial a la dignidad humana y refuerza otros derechos, tales como la libertad de expresión y de información, y la libertad de asociación. Además, es reconocida por el derecho internacional de los derechos humanos.[1]

La Vigilancia de las Comunicaciones interfiere con el derecho a la intimidad entre varios otros derechos humanos. Como resultado, solo puede estar justificada cuando es prescrita por ley, es necesaria para lograr un objetivo legítimo, y es proporcional al objetivo perseguido.[2]

Antes de la adopción pública de internet, principios jurídicos bien definidos y cargas logísticas inherentes al monitoreo de las comunicaciones crearon límites a la Vigilancia de las Comunicaciones por el Estado. En décadas recientes, esas barreras logísticas a la vigilancia han disminuido y ha perdido claridad la aplicación de principios jurídicos en los nuevos contextos tecnológicos. La explosión del contenido digital en las comunicaciones y de la información acerca de ellas - e información sobre las comunicaciones o el uso de dispositivos electrónicos de una persona-, el costo cada vez menor de almacenamiento y la minería de grandes cantidades de datos, y el suministro de contenido personal a

través de proveedores de servicios externos, hacen posible llevar la Vigilancia de las Comunicaciones estatal a una escala sin precedentes.[3]

Mientras tanto, las conceptualizaciones de la legislación vigente en materia de derechos humanos no ha seguido el ritmo de las modernas y cambiantes tecnologías y técnicas estatales de Vigilancia de Comunicaciones, la habilidad del Estado para combinar y organizar la información obtenida mediante distintas técnicas y tecnologías de vigilancia, o la creciente susceptibilidad de la información a la que se puede acceder.

La frecuencia con la que los Estados procuran acceder tanto al contenido de las comunicaciones como a los metadatos de las comunicaciones aumenta drásticamente, sin controles adecuados.[4]

Los metadatos de las comunicaciones pueden crear un perfil de la vida de un individuo, incluyendo condiciones médicas, puntos de vista políticos y religiosos, asociaciones, interacciones e intereses, revelando tan o, incluso, más detalladamente de lo que sería posible desde el contenido de las comunicaciones[5] A pesar del gran potencial para la intromisión en vida del individuo y el efecto negativo sobre las asociaciones políticas y otras, las leyes, normas, poderes o autoridades a menudo ofrecen a los metadatos de las comunicaciones un menor nivel de protección y no ponen restricciones suficientes sobre cómo pueden ser posteriormente utilizado por los Estados.

ÁMBITO DE APLICACIÓN

Los Principios y el Preámbulo son holísticos y autorreferenciales; cada principio y el preámbulo deberán leerse e interpretarse como parte de un marco más amplio que, en conjunto, logran una única meta: garantizar que las leyes, políticas y prácticas relacionadas con las Vigilancia de las Comunicaciones se adhieren a las leyes y estándares internacionales de derechos humanos y protegen adecuadamente los derechos humanos individuales como la privacidad y la libertad de expresión. Así, con el fin de que los Estados cumplan efectivamente sus obligaciones dimanantes de la legislación internacional sobre derechos humanos en lo relativo con la Vigilancia de las Comunicaciones, deben cumplir con los principios que se presentan a continuación.

Estos se aplican a la vigilancia llevada a cabo dentro de las fronteras de un Estado o extraterritorialmente. Los principios también se ponen en práctica con independencia de la finalidad de la vigilancia, incluyendo la aplicación de la ley, la protección de la seguridad nacional, la recopilación de inteligencia, u otra función gubernamental. También se emplean en relación con la obligación del Estado de respetar y garantizar los derechos individuales, así como al deber de proteger los derechos de las personas ante abusos por parte de actores no estatales, incluida la empresas comerciales.[6]

Las empresas comerciales tienen la responsabilidad de respetar la privacidad individual y otros derechos humanos, en particular dado el papel fundamental que desempeñan en el diseño,

desarrollo y difusión de tecnologías, permitir y proporcionar comunicaciones, y en la facilitación de determinadas actividades de vigilancia del Estado.[7] Sin embargo, estos principios articulan los deberes y obligaciones de los Estados cuando se involucran en la Vigilancia de Comunicaciones.

CAMBIO DE TECNOLOGÍA Y DEFINICIONES

«Vigilancia de las Comunicaciones» en el entorno moderno comprende monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas.

«Comunicaciones» abarca las actividades, interacciones y transacciones transmitidas por medios electrónicos, tales como el contenido, la identidad de las partes, información de rastreo de ubicación incluyendo direcciones IP, momento y duración de las comunicaciones, e identificadores de los equipos utilizados.

"Información Protegida" es toda información que incluye, refleja, surge de, o se refiere a las comunicaciones de una persona y que no está fácilmente disponible y accesible para el público en general.

Tradicionalmente, el carácter invasivo de la Vigilancia de las Comunicaciones ha sido evaluado sobre la base de categorías artificiales y formalistas. Los marcos legales existentes distinguen entre "contenido" o "no contenido", "información del suscriptor" o "metadatos", datos almacenados o datos en tránsito, datos que se tienen en el hogar o en la posesión de un tercero proveedor de servicios.[7]

Sin embargo, estas distinciones ya no son apropiadas para medir el grado de intromisión que la Vigilancia de las Comunicaciones realiza en la vida privada y las relaciones de las personas. Aunque desde hace tiempo se ha acordado que el contenido de la comunicación merece una protección significativa en la ley debido a su capacidad de revelar información sensible, ahora está claro que existe otra información que surge de las comunicaciones y datos que no son contenido, que puede revelar incluso más acerca de una persona que el contenido en sí, y por lo tanto merece una protección equivalente.

Hoy en día, cada uno de estos tipos de información, por sí sola o analizada colectivamente, puede revelar la identidad de una persona, su comportamiento, sus asociaciones, sus condiciones físicas o estado de salud, su raza, color, orientación sexual, origen nacional o puntos de vista, o puede permitir el mapeo de la ubicación de la persona, sus movimientos e interacciones en el tiempo[8], o puede hacer esto respecto de todas las personas en una ubicación determinada, incluyendo una manifestación pública u otro acontecimiento político.

Como resultado, toda la información protegida debe recibir la máxima protección de la ley.

Al evaluar el carácter invasivo de la Vigilancia de las Comunicaciones por el Estado, es necesario considerar la potencialidad de la vigilancia de revelar información protegida, así como la finalidad para la que el Estado procura la información. Cualquier Vigilancia de las Comunicaciones que posiblemente dé lugar a revelar información protegida que pueda poner a una persona en riesgo de ser investigada, de sufrir discriminación o de violación de sus derechos humanos, constituirá una infracción grave a su derecho a la privacidad, y también afectará negativamente el disfrute de otros derechos fundamentales, incluyendo las libertades de expresión, de asociación y de participación política. Ello es así porque estos derechos requieren que las personas sean capaces de comunicarse libres del efecto amedrentador de la vigilancia gubernamental. Será pues necesario en cada caso específico determinar tanto el carácter como los posibles usos de la información que se procura.

Al adoptar una nueva técnica de Vigilancia de las Comunicaciones o ampliar el alcance de una existente, el Estado debe determinar, antes de buscarla, si la información que podría ser adquirida cae en el ámbito de la "información protegida", y debería someterse a escrutinio judicial u otro mecanismo de control democrático. La forma de la vigilancia, así como su alcance y duración, son factores relevantes para determinar si la información obtenida a través de la Vigilancia de las Comunicaciones alcanza el nivel de "información protegida". Puesto que el monitoreo generalizado o sistemático tiene la capacidad de revelar información privada que excede en mucho la suma de valor informativo de los elementos individuales recogidos, puede elevar la vigilancia de información no protegida a un nivel invasivo que exija una mayor protección.[9]

Determinar si el Estado puede llevar a cabo vigilancia de comunicaciones que interfiera con Información Protegida debe ser compatible con los siguientes principios:

LOS PRINCIPIOS

LEGALIDAD: Cualquier limitación a los derechos humanos debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación. Dado el ritmo de los cambios tecnológicos, las leyes que limitan el derecho a la privacidad deben ser objeto de revisión periódica por medio de un proceso legislativo o reglamentario de carácter participativo.

OBJETIVO LEGÍTIMO: Las leyes solo deberían permitir la Vigilancia de las Comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

NECESIDAD: Leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La Vigilancia de las Comunicaciones solo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado.

IDONEIDAD: Cualquier caso de Vigilancia de las Comunicaciones autorizado mediante ley debe ser apropiado para cumplir el objetivo legítimo específico identificado.

PROPORCIONALIDAD: La Vigilancia de las Comunicaciones debería ser considerada como un acto altamente invasivo que interfiere con los derechos humanos, amenazando los cimientos de una sociedad democrática. Las decisiones sobre la Vigilancia de las Comunicaciones deben considerar la sensibilidad de la información accesible y la gravedad de la infracción sobre los derechos humanos y otros intereses en competencia.

Esto requiere que un Estado, como mínimo, deba demostrar lo siguiente -a una autoridad judicial competente- antes de la realización de la Vigilancia de las Comunicaciones para los fines de hacer cumplir la ley, la protección de la seguridad nacional, o la recolección de inteligencia:

1. Existe un alto grado de probabilidad de que un delito grave o una amenaza específica para un fin legítimo ha sido o será llevado a cabo,
2. Existe un alto grado de probabilidad de que las evidencias pertinentes y materiales de un delito tan grave o amenaza específica para un fin legítimo se conseguirían mediante el acceso solicitado a la la Información Protegida,
3. Otras técnicas de investigación que son menos invasivas ya han sido agotadas o serían inútiles, de modo que la técnica usada sería la menos invasiva en la práctica,
4. La información a la que se accederá estará limitada a lo relevante y material para el serio crimen o la amenaza especifica al fin legitimo alegado,
5. Cualquier información excedente no será retenida, siendo en su lugar destruida o devuelta con prontitud,
6. La información será accesada solo por la autoridad especifica y usada solamente para los propósitos y durante los lapsos para los cuales se otorgó autorización, y
7. Que las actividades de vigilancia solicitadas y técnicas propuestas no menoscaben la esencia del derecho a la privacidad o de las libertades fundamentales.

AUTORIDAD JUDICIAL COMPETENTE: Las decisiones relacionadas con la Vigilancia de las Comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente. La autoridad debe:

1. Estar separada e independiente de las autoridades encargadas de la Vigilancia de las Comunicaciones.

2. Estar capacitada en materias relacionadas y competente para tomar decisiones judiciales sobre la legalidad de la Vigilancia de las Comunicaciones, las tecnologías utilizadas y los derechos humanos, y

3. Tener los recursos adecuados en el ejercicio de las funciones que se le asignen.

DEBIDO PROCESO: El debido proceso exige que los Estados respeten y garanticen los derechos humanos de las personas asegurando que los procedimientos legales que rigen cualquier interferencia con los derechos humanos estén enumerados apropiadamente en la ley, sean practicados consistentemente y estén disponibles para el público general. Específicamente, al decidir sobre sus derechos, toda persona tiene derecho a una audiencia pública y justa dentro de un plazo razonable por un tribunal independiente, competente e imparcial establecido por ley,[10] salvo en casos de emergencia donde exista un riesgo inminente de peligro para la vida humana. En tales casos, debe buscarse una autorización con efecto retroactivo dentro de un plazo razonable y factible. El mero riesgo de fuga o de destrucción de pruebas no se considerará suficiente para justificar la autorización con efecto retroactivo.

NOTIFICACIÓN DEL USUARIO: Aquellos cuyas comunicaciones están siendo vigiladas deben ser notificados de la decisión de autorizar la Vigilancia de Comunicaciones con el tiempo y la información suficiente para que puedan impugnar la decisión o buscar otras soluciones y deben tener acceso a los materiales presentados en apoyo de la solicitud de autorización. El retraso en la notificación solo se justifica en las siguientes circunstancias:

1. La notificación pondría en serio peligro la finalidad para la que se autoriza la vigilancia, o existe un riesgo inminente de peligro para la vida humana,

2. La autorización para retrasar la notificación es otorgada por la autoridad judicial competente en el momento en que se concede la autorización para la vigilancia, y

3. El usuario afectado se notifica tan pronto como el riesgo desaparece según lo determinado por la autoridad judicial competente.

La obligación de notificar recae en el Estado, pero los proveedores de servicios de comunicaciones deben tener la libertad de notificar a las personas de la Vigilancia de las Comunicaciones, de forma voluntaria o bajo petición.

TRANSPARENCIA: Los Estados deben ser transparentes sobre el uso y alcance de las leyes de Vigilancia de las Comunicaciones, reglamentos, actividades, poderes o autoridades. Deben publicar, como mínimo, información global sobre el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo y

propósito, y el número específico de personas afectadas por cada una y según el tipo de investigación y sus propósitos. Los Estados deben proporcionar a las personas la información suficiente para que puedan comprender plenamente el alcance, naturaleza y aplicación de las leyes que permiten la Vigilancia de las Comunicaciones. Los Estados no deberían interferir con los proveedores de servicios en sus esfuerzos para publicar los procedimientos que aplican en la evaluación y el cumplimiento de solicitudes de los Estados para la Vigilancia de Comunicaciones, se adhieran a esos procedimientos, y publicar los registros de las solicitudes de los Estados para la Vigilancia de las Comunicaciones.

SUPERVISIÓN PÚBLICA: Los Estados deberían establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la Vigilancia de las Comunicaciones[11]

Los mecanismos de supervisión deben tener la autoridad para acceder a toda la información potencialmente relevante acerca de las actuaciones del Estado, incluyendo, según proceda, al acceso a información secreta o clasificada para valorar si el Estado está haciendo un uso legítimo de sus funciones legales, para evaluar si el Estado ha publicado de forma transparente y precisa información sobre el uso y alcance de las técnicas y poderes de la Vigilancia de las Comunicaciones; y para formular determinaciones públicas en cuanto a la legalidad de dichas acciones, incluyendo la medida en que cumplan con estos principios. Mecanismos de supervisión independientes deben establecerse, además de cualquier supervisión ya proporcionada a través de otra rama del gobierno.

INTEGRIDAD DE LAS COMUNICACIONES Y SISTEMAS: A fin de garantizar la integridad, seguridad y privacidad de los sistemas de comunicaciones, y en reconocimiento del hecho de que poner en peligro la seguridad con fines estatales casi siempre afecta la seguridad en términos generales, los Estados no deben obligar a los proveedores de servicios o proveedores de "hardware" o "software" a desarrollar la capacidad de vigilancia o de control en sus sistemas, ni a recoger o retener determinada información exclusivamente para fines de Vigilancia de las Comunicaciones del Estado. La retención o la recopilación de datos *a priori* nunca debe ser exigida a los proveedores de servicios. Las personas tienen el derecho a expresarse anónimamente, por lo que los Estados deben abstenerse de obligar a la identificación de los usuarios.[12]

GARANTÍAS PARA LA COOPERACIÓN INTERNACIONAL: En respuesta a los cambios en los flujos de información y en las tecnologías y servicios de comunicaciones, los Estados pueden necesitar procurar la asistencia de un proveedor de servicios extranjero y otros Estados. En consecuencia, los tratados de asistencia judicial recíproca (MLAT, por sus siglas en inglés) y otros acuerdos celebrados por los Estados deben garantizar que, cuando la legislación de más de un Estado pueda aplicarse a la Vigilancia de las Comunicaciones, se adopte la estándar disponible con el mayor nivel de protección para las personas. El principio de la doble incriminación debe ser aplicado en el momento en que

los Estados procuren asistencia para efectos de hacer cumplir su legislación interna. Los Estados no pueden utilizar los procesos de asistencia judicial recíproca y las solicitudes extranjeras de Información Protegida para burlar las restricciones del derecho interno relativas a la Vigilancia de las Comunicaciones. Los procesos de asistencia judicial recíproca y otros acuerdos deben estar claramente documentados, a disposición del público y sujetos a las garantías de equidad procesal.

GARANTÍAS CONTRA EL ACCESO ILEGÍTIMO Y DERECHO A RECURSO EFECTIVO: Los Estados deben promulgar leyes que penalicen la Vigilancia de las Comunicaciones ilegal por parte de actores públicos o privados. La ley debe proveer sanciones penales y civiles suficientes y adecuadas, protección a los "*whistleblowers*" y medios de reparación a las personas afectadas. Las leyes deben estipular que cualquier información obtenida de una manera que sea inconsistente con estos principios es inadmisible como prueba en cualquier procedimiento, al igual que cualquier prueba derivada de dicha información. Los Estados también deben promulgar leyes que establezcan que, después de que el material obtenido a través de la Vigilancia de las Comunicaciones ha sido utilizado con la finalidad por el que fue obtenida la información, el material no debe ser retenido, en su lugar debe ser destruido o devuelto a los afectados.

* El proceso de elaboración de estos Principios se inició en octubre de 2012 en una reunión de más de 40 expertos de seguridad y privacidad en Bruselas. Después de una amplia consulta inicial, que incluyó una segunda reunión en Río de Janeiro en diciembre de 2012, Access, EFFy Privacy International condujeron un proceso de redacción colaborativa inspirada en la pericia sobre derechos humanos y derechos digitales de expertos de todo el mundo. La primera versión de los Principios se finalizó el 10 de julio de 2013, y fue lanzada oficialmente en el Consejo de Derechos Humanos de la ONU en Ginebra en Septiembre de 2013.

El éxito rotundo y la adopción global de los Principios por más de 400 organizaciones en todo el mundo hizo necesaria una serie de cambios concretos en el lenguaje del texto, fundamentalmente superficiales, a fin de asegurar su interpretación uniforme y la aplicación en todas las jurisdicciones.

De marzo a mayo de 2013, otra consulta se llevó a cabo para determinar y corregir esos problemas textuales y actualización de los Principios en consecuencia. El efecto y la intención de los Principios no se alteró por estos cambios. Esta versión es el producto final de estos procesos y es la versión autorizada de los Principios.

NOTAS AL FIN

1 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.

2 Declaración Universal de Derechos Humanos, artículo 29; Comentarios Generales No. 27, Adoptado por el Comité de Derechos Humanos bajo el artículo 40, parágrafo 4 del Pacto Internacional de Derechos Civiles y Políticos, CCPR/C/21/Rev.1/Add.9, Noviembre 2, 1999; Ver también Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/ HRC/17/34, Ver también Frank La Rue; "Informe del Relator Especial del Consejo de Derechos Humanos sobre las implicaciones de la Vigilancia de las Comunicaciones de los Estados en el ejercicio de los derechos humanos a la intimidad y a la libertad de opinión y de expresión", 2013, A.HRC. 23.40 ES.

3 Los metadatos de las comunicaciones pueden incluir información acerca de nuestras identidades (información del abonado, información del dispositivo), las interacciones (origen y destino de las comunicaciones, especialmente las que muestran los sitios web visitados, los libros y otros materiales de lectura, las personas interactuaron con los amigos, familia, conocidos, búsquedas realizadas, los recursos utilizados) y ubicación (lugares y tiempos, proximidades a otros), en suma, los metadatos proporciona una ventana a casi todas las acciones en la vida moderna, nuestros estados mentales, los intereses, las intenciones y los pensamientos más íntimos.

4 Por ejemplo, solamente en el Reino Unido existe aproximadamente 500.000 solicitudes de acceso a los metadatos de las comunicaciones todos los años, actualmente bajo un régimen de auto-autorización, los servicios policiales puedan autorizar la solicitud de acceso a la información en poder de los proveedores de servicios. Mientras tanto, los datos proporcionados por los informes de transparencia de Google muestran que las solicitudes de datos de los usuarios de los EE.UU. aumentaron solamente de 8.888 en 2010 a 12.271 en 2011. En Corea, cada año había alrededor de 6 millones de solicitudes de abonados de información y alrededor de 30 millones de solicitudes de otras formas de metadatos de comunicaciones en el período 2011-2012, casi de todo lo cual se entregó y se ejecuta. Los datos del año 2012 están disponibles en http://www.kcc.go.kr/user.do?mode=view&page=A02060400&-dc=K02060400&boardId=1030&cp=1&boardSeq=35586

5 Ver la revisión del trabajo de Sandy Petland, 'Reality Mining', en MIT's Technology Review, disponible en http://www2.technologyreview.com/article/409598/tr10-reality-mining/ y ver también Alberto Escudero-Pascual y Gus Hosein, "'Questioning lawful access to traffic data", *Communications of the ACM*, 47 (3), marzo 2004, 77 - 82.

6 Frank La Rue, *Reporte del Relator de Naciones Unidas sobre la Promoción y Protección de la Libertad de Opinión y Expresión*, (2011), UN Doc A/HRC/17/27 http://ap.ohchr.org/documents/dpage_s.aspx?m=85

7 "Las personas revelan los números de teléfono que marcan para llamar o enviar mensajes de texto a sus proveedores de celulares, las direcciones URL que visitan y las direcciones de correo electrónico con las que se comunican a sus proveedores de servicios de Internet y los libros, alimentos y medicamentos que compran a los minoristas en línea. . . No imagino que toda la información voluntariamente revelada a algún miembro del público para un propósito limitado carece, por esa única razón, de la protección de la Cuarta Enmienda. "Los Estados Unidos contra Jones, 565 EE.UU. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurrente)."

8 "El seguimiento a corto plazo de los movimientos de una persona en la vía pública concuerda con las expectativas de privacidad", pero "el uso del monitoreo de GPS a largo plazo en las investigaciones de la mayoría de los delitos afecta a las expectativas de la vida privada." Los Estados Unidos contra Jones, 565 EE.UU., 132 S. Ct. 945, 964 (2012) (Alito, J. concurrente).

9 "La vigilancia prolongada revela tipos de información no reveladas por la vigilancia a corto plazo, como que hace una persona repetidamente, lo que no hace, y lo que hace en conjunto. Este tipo de información puede revelar más sobre una persona que lo que revelaría cualquier viaje individual considerado aisladamente. Visitas repetidas a una iglesia, un gimnasio, un bar, o un corredor de apuestas cuentan una historia no revelada en una sola visita, al igual que una ausencia a cualquiera de estos lugares a lo largo de un mes. La secuencia de los movimientos de una persona puede revelar aún más; un solo viaje a la oficina de un ginecólogo dice poco acerca de una mujer, pero ese viaje seguido, unas semanas después, de una visita a una tienda de artículos para bebé cuenta una historia diferente. * Una persona que sabe todo de los viajes de otros puede deducir si es un visitante semanal a la iglesia, un bebedor recurrente, un habitual en el gimnaso, un marido infiel, un paciente ambulatorio que recibe tratamiento médico, un asociado de individuos o grupos políticos particulares .. y no solo un hecho determinado acerca de una persona, si no todos esos hechos "EE. UU. v Maynard, 615 F. 3d 544 (EE.UU., DC Circ, CA) p 562; EE.UU. v Jones, 565 EE.UU. (2012), Alito, J., concurriendo. Por otra parte, la información pública puede entrar en el ámbito de la vida privada cuando se recoge y se almacena en archivos en poder de las autoridades de manera sistemática. Todo esto es aún más cierto cuando esa información se refiere al pasado lejano de una persona ... En opinión de la Corte, tal información, cuando se recoge de manera sistemática y se almacena en un archivo en poder de agentes del Estado , está comprendida en el ámbito de la «vida privada» en el sentido del artículo 8 (1) de la Convención. (Rotaru contra Rumania, [2000] CEDH 28341/95, párrs. 43-44.

10 El término “debido proceso” puede utilizarse de manera intercambiable con “justicia procesal” y “justicia natural” y está bien articulado en el Convenio Europeo de Derechos Humanos del artículo 6(1) y el artículo 8 de la Convención Americana sobre Derechos Humanos.

11 El Comisionado de Interceptación de Comunicaciones del Reino Unido es un ejemplo de un mecanismo de supervisión independiente de ese tipo. El ICO publica un informe que incluye algunos datos agregados pero no proporciona datos suficientes para examinar los tipos de solicitudes, la extensión de cada petición de acceso, el propósito de las solicitudes, y el escrutinio que se aplica a ellos. Ver http://www.iocco-uk.info/sections.asp?sectionID=2&type=top

12 Frank La Rue, *Informe del Relator Especial de Naciones Unidas sobre la protección y promoción del derecho a la libertad de opinión y expresión*, párr. 84.

El Salvador

Marlon Hernández Anzora

1. Antecedentes

1.1. Estado de la discusión nacional

Las principales reflexiones sobre el impacto de internet y las tecnologías de la información en El Salvador comienzan a darse a principios de la primera década del siglo XXI, principalmente en las Facultades de Jurisprudencia del país. Las discusiones iniciales fueron generadas, en buena parte, por los primeros casos sobre protección de datos que fueron judicializados.

Las tesis de grado para la Licenciatura en Ciencias Jurídicas de varias universidades, sobretodo enfocadas en las materias penal y mercantil, son los principales aportes académicos. En menor cantidad se identifican algunos blogs personales o institucionales que se dedican a discutir sobre las tecnologías de la información y comunicación y sus implicaciones en la realidad nacional, y -en menor proporción- se identifican informes, documentos institucionales, artículos académicos o libros.

Las primeras tesis y monografías de Licenciatura en Ciencias Jurídicas sobre comercio electrónico, *habeas data* y delitos informáticos se registran entre 2002 y 2003. A continuación se listan algunas de ellas:

Tabla I
Producción de tesis nacionales

Nombre	Año	Universidad	Autores
El Habeas Data en la Constitución	2002	Francisco Gavidia	Castro, Jorge et al.
Análisis jurídico del comercio electrónico	2003	Francisco Gavidia	Alcántara, Milton.
Las intervenciones telefónicas	2003	de El Salvador	Morán, Carolina et al.
Aspectos generales del delito informático	2004	Francisco Gavidia	Gómez, Luis.
El Habeas Data como garantía de protección de la persona frente al tratamiento de sus datos personales	2004	de El Salvador	Alvarado, Karla et al.
Penalización de los delitos informáticos en El Salvador	2005	de El Salvador	Benavides, Leo et al.
Habeas Data como mecanismo de protección de derechos relacionados con la autodeterminación informativa ante el tratamiento automatizado de datos personales	2006	de El Salvador	Hernández, María et al.
La Firma Electrónica, tecnología del siglo XXI en la legislación salvadoreña	2007	de El Salvador	López Flores, Sarbelio Enrique
La seguridad jurídica de los contratos en el comercio electrónico de El Salvador	2009	de El Salvador	Amaya, José et. al..
El derecho a la intimidad, su limitabilidad y protección en el marco normativo de la ley especial para la intervención de las telecomunicaciones	2010	de El Salvador	Olivares, Erick
Aplicación legal práctica para la realización de actividades económicas en el comercio electrónico	2011	Dr. José Matías Delgado	Álvarez, Katia et al
El ejercicio notarial frente a los avances tecnológicos, tales como la firma digital y la seguridad jurídica en el tráfico de bienes y servicios	2011	de El Salvador	Chámul, Flor et al.
La necesidad de crear una ley que regule el Habeas Data como mecanismo de protección de datos personales en El Salvador	2011	de El Salvador	Gavidia, María Magdalena et al.
El derecho a la intimidad, su limitabilidad y protección en el marco normativo de la ley especial para la intervención de las telecomunicaciones	2011	de El Salvador	Miranda, Verónica et al.
Respeto al derecho de intimidad en la estructura de la Ley Especial de Intervención de Telecomunicaciones	2012	de El Salvador	Amaya, Tomás et al.

Fuente: Elaboración propia, con datos de las universidades mencionadas.

Los temas que aparecen con más frecuencia en la discusión académica en El Salvador son la protección de datos, los delitos informáticos, el comercio electrónico y la gobernanza de internet. Temas como vigilancia electrónica, censura en internet, software libre, cifrado o anonimato, entre otros, aparecen en menor proporción o simplemente no se identifica producción y discusión académica al respecto.

1.1.1. Delitos informáticos

En cuanto a la penalización de los delitos informáticos, las tesis mencionadas en el cuadro anterior[1] se concentran principalmente en las definiciones de delito informático, así como los tipos penales surgidos del derecho comparado, las penas aplicadas a los delitos informáticos en el derecho comparado y los países que actualmente cuentan con legislación sobre delitos informáticos.

Las tesis producidas ponen énfasis en hechos históricos (jurídicos y tecnológicos) y perspectivas de futuro que justifican la necesidad de su tipificación en la legislación salvadoreña, sugiriendo incluso en la tesis de Benavides et al. (2005) algunas propuestas de tipos penales a adoptarse en el derecho penal salvadoreño.

En el ámbito político, en los primeros meses de 2015 se inició una discusión legislativa y mediática sobre un anteproyecto de ley denominado como Ley Especial sobre Delitos Informáticos y Conexos, sin embargo, ha existido poca divulgación del contenido de la iniciativa y la discusión se centró en la posibilidad de que, a través de dicha iniciativa de ley, se criminalice a los opositores políticos y activistas que hacen sus denuncias y críticas a través de las redes sociales. El anteproyecto resultó tan problemático que los legisladores decidieron no seguir el trámite de formación de ley, por lo que actualmente se encuentra detenido.

1.1.2. Protección de datos

Una de las primeras obras, muy completa, sobre protección de datos en El Salvador es la de Ayala, José María et al (2005), en donde puede verse claramente la predominancia de juristas españoles. Cuatro de los cinco autores son de ese país, mientras que solo Henry Campos, un reconocido jurista salvadoreño escribe en ella. Sin embargo, dicha obra contiene una importante reflexión sobre la situación del país, dejando clara la poca deliberación académica y producción jurídica en el tema.

Vale mencionar que de casi 40 fuentes bibliográficas utilizadas en esta investigación, ninguna es de origen salvadoreña. Para 2005, en El Salvador, sobre protección de datos las únicas fuentes que encontraron estos investigadores fueron una sentencia de amparo y algunos artículos dispersos en

1 Nos referimos a las tesis de Luis Alfredo Gómez Molina, "Aspectos generales del delito informático" (monografía de Licenciatura, Universidad Francisco Gavidia, 2004), y Leo Benavides et al., "Penalización de los delitos informáticos en El Salvador" (tesis de Licenciatura, Facultad de Jurisprudencia y Ciencias Sociales, Universidad de El Salvador, 2005).

distintos cuerpos legales nacionales o convenios internacionales.

Debe destacarse que la protección de datos es muy probablemente el tema que más se ha profundizado desde la academia. Para el caso de las tesis mencionadas en el cuadro anterior, profundizan en los elementos doctrinarios sobre el derecho a la intimidad, así como en el derecho a la autodeterminación informativa y la protección de datos personales. La figura del *habeas data* es ampliamente desarrollada y vista desde el derecho comparado, haciendo énfasis en la necesidad de una legislación de *habeas data* para proteger de manera más integral los datos de las personas en El Salvador.

1.1.3. Comercio electrónico

Uno de los aspectos que se ha desarrollado bastante en la producción académica salvadoreña, a menos a nivel de tesis, es la de comercio electrónico. Actualmente, se reconocen dos formas de promoción de los negocios por medio de las nuevas tecnologías: el negocio electrónico y el comercio electrónico, los cuales se encuentran relacionados pero no significan lo mismo.

Negocio electrónico es un intercambio de información ya sea con el público externo, interno o con ambos públicos de una compañía; mientras que el comercio electrónico abarca los procesos de compra y venta apoyados por medios electrónicos, principalmente internet[2].

El comercio electrónico es un concepto que engloba cualquier forma de transacción comercial o de negocios que se transmite electrónicamente, utilizando las redes de la telecomunicación y empleando como moneda de cambio el dinero electrónico. La Organización Mundial del Comercio (OMC) define comercio electrónico como "la producción, publicidad, venta y distribución de productos a través de las redes de telecomunicaciones"[3].

En cuanto a comercio electrónico, la primera tesis producida en El Salvador data de 2003. Sin embargo, guarda mucha similitud con las últimas producidas, ya que fundamentalmente trata sobre la definición del término, las diferentes formas, y el derecho comparado[4]. A pesar de haber un período mayor a 10 años, la iniciativa de ley que se analiza en las últimas tesis es la misma elaborada por el abogado Ricardo Cevallos a solicitud del Gobierno, un anteproyecto de Ley de Comercio Electrónico[5].

Lo que sí cambió entre las primeras y las últimas tesis es la cantidad de comercio electrónico que

2 Gary Armstrong y Philip Kotler, Marketing: versión para Latinoamérica, (México D.F.: Pearson Educación, 2007), 18.
3 Milton Leónidas Alcántara Quintanilla, et al., "Análisis jurídico del comercio electrónico", (monografía de Licenciatura, Universidad Francisco Gavidia, 2003), 11-2.
4 Las tesis a que nos referimos son las de Milton Leónidas Alcántara, et al., "Análisis jurídico del comercio electrónico" (monografía de Licenciatura, Universidad Francisco Gavidia, 2003) y la de Katia Susana Álvarez Hernández, et al., "Aplicación legal práctica para la realización de actividades económicas en el comercio electrónico" (monografía de Licenciatura, Universidad Dr. José Matías Delgado, 2011).
5 Katia Susana Álvarez Hernández, et al., "Aplicación legal práctica para la realización de actividades económicas en el comercio electrónico"

surgió en ese lapso de tiempo. Para 2011, se identificaban en el país, por lo menos, diez empresas con un fuerte comercio electrónico o cuyo comercio era solamente electrónico[6]; nuevamente la realidad superó por mucho tiempo a los instrumentos jurídicos necesarios para proteger, en este caso, el derecho de los consumidores.

1.1.4. Gobierno de internet

Otra reflexión reciente, principalmente a nivel de blogs y medios de comunicación oficial, ha sido sobre el gobierno o gobernanza de internet, en buena manera estimulada por la realización del Foro *NetMundial* en julio de 2014, en el se que reunió a buena parte de la comunidad de internet de la región para establecer una hoja de ruta de la nueva gobernanza de internet.

En el marco de dicho evento, representantes de la sociedad civil, gobiernos, academia y organizaciones empresariales debatieron los pasos a seguir en temas controversiales y urgentes referentes a la gobernanza en internet, tales como la privacidad, el acceso a datos privados, la seguridad nacional e informática, la vigilancia digital, entre otros[7].

En el marco de *NetMundial*, la Viceministra de Ciencia y Tecnología Erlinda Hándal aseguró que estaba trabajando en una plataforma de gobierno electrónico y que esta discusión ayudaría a dimensionar mejor los temas de seguridad y privacidad de cara a la protección de la sociedad y la soberanía nacional:

> Cada individuo que visita y navega en la red, tiene derecho a su privacidad y a su seguridad, ahora que se intentará masificar el internet en las escuelas públicas, esto es mucho más importante […] todos los materiales relacionados con violencia deben ser regulados y controlados de forma consensuada entre distintos sectores de la sociedad para no vernos afectados desde la red por este problema[8].

En El Salvador aún no existe una política de gobierno que aborde el tema de la gobernanza de internet[9]. Sin embargo, sí existe alguna discusión alrededor de estos temas aunque el debate aún no es relevante ante la opinión pública salvadoreña.

6 Katia Susana Álvarez Hernández, "Aplicación legal práctica para la realización de actividades".
7 Foro de Gobernanza de Internet, "LACIGF: El Salvador en la hoja de ruta de la gobernanza de internet", http://prensa.lacnic.net/news/14junio_es/lacigf-el-salvador-en-la-hoja-de-ruta-de-la-gobernanza-de-internet (consultado: 25 marzo, 2015).
8 Foro de Gobernanza de Internet, "LACIGF: El Salvador en la hoja de ruta de la Gobernanza de Internet".
9 José Mejía, "¿Quién gobierna internet en El Salvador?", http://www.transparenciaactiva.gob.sv/quien-gobierna-internet-en-el-salvador/ (consultado: 25 marzo, 2015).

1.1.5. Documentos e informes

Entre algunos informes y documentos reconocidos que trataron temas relacionados con las nuevas tecnologías y protección de datos, se identificaron los siguientes:

Tabla 2
Producción de documentos e informes nacionales

Nombre	Año	Organismo	Autores
El SABER MAS III: Informe Regional sobre Acceso a la Información Pública y la Protección de Datos Personales.	s.f.	La Alianza Regional por la Libre Expresión e Información	Asociación de Periodistas de El Salvador *et Al*.
Informe de coyuntura legal e institucional	2014	Fundación Salvadoreña para el Desarrollo Económico y Social (FUSADES)	Departamento de Estudios Legales

Fuente: Elaboración propia.

La Alianza Regional por la Libre Expresión e Información realizó un informe regional en el cual la Asociación de Periodistas de El Salvador (APES) y la Fundación Salvadoreña para El Desarrollo Económico y Social (FUSADES)[10] dieron sus valoraciones sobre la situación de la protección de datos y el acceso a la información en el país.

Por otra parte, un Informe de coyuntura presentado por el Departamento de Estudios Legales de FUSADES destacó y analizó la sentencia de amparo 142- 2012, emitida por la Sala de lo Constitucional en octubre de 2014 que estableció la violación al derecho a la autodeterminación informativa por parte de una sociedad privada, evidenciando la necesidad de aprobar en el país una ley de protección de datos personales. El informe subraya que en dicha sentencia se reiteró el asidero constitucional del derecho a la autodeterminación informativa y el derecho a ser protegido en su goce[11].

1.1.6. Blogs

En El Salvador existen algunos blogs que se dedican principalmente al desarrollo del tema de protección de datos personales y las TIC, los principales se encuentran en la siguiente tabla:

10 Alianza Regional por la Libre Expresión e Información, El SABER MAS III Informe Regional sobre Acceso a la Información Pública y la Protección de Datos Personales, (s.l., s.f), 66-7.
11 Fundación Salvadoreña para el Desarrollo Económico y Social, Informe de coyuntura legal e institucional (El Salvador: FUSADES, 2014), 95-6.

Tabla 3
Blogs y webs especializadas

Nombre del blog	Año	URL	Autor
El Economista	2005	http://blogs.eleconomista.net/author/ricardo-cevallos/	Ricardo Cevallos
Asociación Salvadoreña para la Protección de Datos e Internet (INDATA)	2011	http://indatasv.blogspot.com/	INDATA
Conversaciones en Línea con Lito Ibarra.	2011	http://blogs.laprensagrafica.com/litoibarra/	Rafael Ibarra

Fuente: Elaboración propia.

En el blog del abogado Ricardo Cevallos se analiza la jurisprudencia emitida por la Sala de lo Constitucional de la Corte Suprema de Justicia, específicamente sobre amparos sobre la figura del *habeas data*; asimismo, realiza un pequeño abordaje de los cuerpos normativos en donde la protección de datos personales ha tenido alguna regulación, como por ejemplo la Ley de Protección al Consumidor[12].

Por su parte, INDATA es una asociación sin fines de lucro, la cual muestra interés en temas como protección de datos, *habeas data*, autodeterminación informativa y derecho informático. En su blog se pueden encontrar diversos artículos relacionados a los temas citados. Uno de los aportes más significativos de INDATA fue la presentación de la demanda de inconstitucionalidad contra la empresa EQUIFAX-DICOM[13] por el procesamiento arbitrario e ilegal de datos personales de miles de personas, la cual fue resuelta a favor de INDATA[14].

En el blog de Rafael Antonio Ibarra se abordan temas sobre las tecnologías de la información y la comunicación e internet y protección de datos, entre otros temas relacionados. Todos los artículos son escritos por el ingeniero Ibarra, a quien se le reconoce como "el padre de internet" en El Salvador por haber sido la persona que lideró y concretó la conexión del país con internet en 1995[15].

En resumen, la discusión académica, legislativa y jurisprudencial sobre lo relacionado con las nuevas tecnologías y la denominada sociedad de control en El Salvador es aún mínima o prácticamente nula. A propósito de las revelaciones del caso Snowden, el gobierno de El Salvador expresó su preocupación ante la denuncia internacional sobre la existencia de espionaje cibernético sobre países latinoamericanos por parte del gobierno de los Estados Unidos, en los cuales estaba incluido El Salvador: "Nuestro

12 Ricardo Cevallos, "La protección de datos", http://blogs.eleconomista.net/marketing/2008/06/la-proteccion-de-datos/ (consultado: 25 marzo,2015).
13 Equifax ofrece a empresas y consumidores información de los consumidores, principalmente la relacionada con el récord crediticio en el sistema financiero de El Salvador. Dotamos a los consumidores individuales para gestionar su información de crédito personal, proteger su identidad y maximizar su bienestar financiero.
14 Asociación Salvadoreña para la Protección de Datos e Internet (INDATA), http://indatasv.blogspot.com/ (consultado: 25 marzo, 2015).
15 Rafael Ibarra, "Gobernanza de internet", http://blogs.laprensagrafica.com/litoibarra/?p=1205 (consultado: 10 marzo, 2015)

gobierno está dando seguimiento a esta situación para verificar la veracidad de la misma, pues riñe con el principio de soberanía y violenta los derechos a la privacidad de los salvadoreños y salvadoreñas[16]".

La sociedad salvadoreña, como la mayoría de sociedades en el mundo, parece haber abrazado los avances de las nuevas tecnologías de la información y la comunicación sin mayor conciencia ni discusión sobre los riesgos y efectos contraproducentes en la intimidad y la libertad que estos avances tecnológicos podrían afectar.

1.2. Brecha digital

El Salvador es un país de grandes contrastes sociales y económicos. Una parte de su sociedad tiene la capacidad de acceder a los servicios tecnológicos de primer mundo, mientras que otro importante porcentaje aún vive una realidad sin internet[17], de analfabetismo digital, siendo probablemente solo el acceso a la telefonía celular lo único que ambas realidades comparten.

Para el año 2007, el 65% de los hogares salvadoreños tenía al menos un teléfono móvil, el 9% tenía computadora y solo un 3% tenía acceso a internet[18]. Siete años después, en 2014, se calculaba que cerca del 30% de la población salvadoreña era usuaria de internet, según el Organismo Especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación, conocido por sus siglas en inglés como UIT[19].

En 2011 se estimaba que había cerca de 500 mil *smartphones* activos[20], cifra que para 2014 aumentó a 1.8 millones de un total de suscripciones de teléfonos móviles que rondaba los 9 millones (superando la población del país, que ronda los 6 millones de habitantes), según datos contrastados de la UIT[21] y del director país de la empresa Telefónica[22]. Los *smartphones* han posibilitado que, a pesar que la posesión de computadora y acceso al servicio de internet residencial sean aún bastante bajas, muchas personas en el país estén accediendo a internet desde sus dispositivos móviles[23].

16 "El Salvador expresa preocupación por posible espionaje de EEUU en América Latina", *Diario Digital Voces, 11 de julio, 2013,* http://voces.org.sv/2013/07/11/el-salvador-expresa-preocupacion-por-posible-espionaje-de-eeuu-en-america-latina/ (consultado: 25 marzo, 2015)

17 Para 2014 se estimaba que solo el 29.7% de la población salvadoreña era usuaria de internet, de acuerdo con el Organismo Especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación (UIT). Informe accesible en: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

18 Ana Marcela Lemus y César Villatoro Canales, "La brecha digital en El Salvador: causas y manifestaciones" (tesis de Licenciatura, Universidad Centroamericana José Simeón Cañas, 2009), 38-40.

19 Organismo Especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación (UIT), *Informe sobre estadísticas de individuos que usan Internet en El Salvador.* (Washington, D.C.: UIT, 2014), http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (consultado: 4 noviembre, 2015)

20 Luis Figueroa, "SmartPhones: una revolución en las comunicaciones", Realidad y Reflexión (septiembre-diciembre 2011): 33, 21-2.

21 Para 2014 se calculaba que había cerca de 9, 194,242 suscripciones a teléfonos celulares en El Salvador, según el Organismo Especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación (UIT). Informe accesible en: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

22 "Circulan 1.8 millones de smartphones en el país", *El Diario de Hoy*, 4 de noviembre, 2014, bajo "sección Negocios", http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=47861&idArt=9218924 (consultado: 8 abril, 2015).

23 En 14 años El Salvador pasó de tener solo un 1.8% de su población como usuaria de internet (en el año 2000) a cerca del 30% en 2014, según la UIT. Informe accesible en: http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

No obstante su histórico bajo crecimiento económico y sus graves problemas sociales, las tecnologías digitales de la comunicación como internet, los teléfonos inteligentes y los dispositivos con acceso a *Wi-Fi* ya forman parte de la vida cotidiana de buena parte de las personas e instituciones del país. Cada vez son más las personas cuya información se encuentra en los registros electrónicos del Centro Nacional de Registros (CNR) o del registro tributario del Ministerio de Hacienda, generando que estas modernas herramientas de comunicación incidan cada vez más en la vida diaria de la ciudadanía, del Estado y el mercado.

Las nuevas dinámicas generadas por las tecnologías de la información y las telecomunicaciones han provocado que derechos como acceso a la información, libertad de expresión, libertad de prensa, derecho a la protección de datos y la privacidad, entre otros, se vuelven cada vez más importantes de discutir y legislar. En el Salvador, en particular, urge la necesidad de poner en la agenda pública los temas derivados de la presencia cada vez más extensa de internet en la economía y política doméstica[24].

Dicha urgencia queda en evidencia cuando el escenario planteado hace diez años por José María Ayala en cuanto legislación sobre protección de datos, continúa siendo prácticamente el mismo:

> En El Salvador existen casos conflictivos, en donde las empresas manejan datos de cualquier persona sin su consentimiento e incluso con su desconocimiento sobre la existencia del mismo fichero. Ante esta situación, la incertidumbre gana terreno. La ciudadanía salvadoreña no sabe quién y para qué se están almacenando, gestionando o utilizando sus datos personales; ignora a quién tiene que dirigirse para solicitar la cancelación de informaciones erróneas o incluso desconoce si puede exigirlo jurídicamente, porque no existe, en el país, un marco jurídico que lo proteja contra el uso abusivo de sus datos personales[25].

Tantos años después en El Salvador, a pesar de la trascendencia de tales realidades, existe escasa discusión académica y política al respecto con una grave ausencia de normativas que regulen el inmenso mundo de internet y sus derivados[26]. En un país abatido por la violencia, la inseguridad y el alto costo de la vida, las preocupaciones por la seguridad de sus datos o la vigilancia que organismos públicos o privados puedan realizar a través de las nuevas tecnologías parece no solo no ser prioritario, sino estar poco presente en la agenda pública. Sin embargo, "no es admisible, al menos para juristas, políticos y tecnólogos, aducir sorpresa o desconocimiento de los eventuales peligros implícitos en el uso de las nuevas tecnologías"[27].

En la era digital, las tecnologías de la comunicación también han aumentado la capacidad de los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y

24 Rafael Ibarra, "Gobernanza de internet", La Prensa Gráfica, http://blogs.laprensagrafica.com/litoibarra/?p=1205 (consultado: 10 marzo, 2015)
25 José Ma. Ayala et al. *La protección de datos personales en El Salvador.* (El Salvador: UCA Editores, 2005), 21.
26 Rafael Ibarra, "Gobernanza de internet", http://blogs.laprensagrafica.com/litoibarra/?p=1205 (consultado: 10 marzo, 2015)
27 Antonio Enrique Pérez Luño, "Internet y los derechos humanos", Derecho y Conocimiento, (s.f.), 2:27.

recopilación de datos. El incremento de tecnología disponible, tanto para los delincuentes como las víctimas, combinado con el escaso conocimiento o información sobre cómo proteger sus datos personales y sus comunicaciones, así como de los posibles delitos que se pueden sufrir a través de las nuevas tecnologías, otorga a los delincuentes un campo fértil de potenciales víctimas[28].

1.3. Criminalización de defensoras y defensores de derechos humanos

A continuación un marco de la historia reciente y la situación actual de los derechos humanos de los y las defensores de derechos humanos en El Salvador. A su vez, también se realiza un acercamiento preliminar entre el marco jurídico nacional sobre nuevas tecnologías y telecomunicaciones y la posibilidad de que este pueda dejar espacios para la criminalización de las personas defensoras de derechos humanos.

1.3.1. Derechos humanos: durante y después de los militares

Los gobiernos militares (1931 a 1979) y el conflicto armado (1980 a 1991) que experimentó El Salvador en el siglo XX dejaron como saldo una amplia práctica institucional de persecución política, violaciones de derechos humanos y persecución de defensores y defensoras de derechos humanos. Dentro del largo y oscuro historial de leyes que fueron utilizadas para reprimir políticamente y que sirvieron para violar derechos humanos se encuentran, por ejemplo, el Código Penal de 1904 que ordenaba el internamiento –en hospital o cárcel- de los locos y dementes. En 1940 la ley represiva de vagos y maleantes se estableció como un medio de defensa social. Más adelante, en 1953, fue promulgada la ley del estado peligroso, la cual se mantuvo vigente hasta 1997[29].

También se crearon instituciones como ORDEN (Organización Democrática Nacionalista), que funcionó de 1961 a 1979 como el instrumento del ejército salvadoreño para recoger información para los servicios de inteligencia, siendo clave para la persecución y represión política. El Ejército y los cuerpos de seguridad como la Policía Nacional, la Guardia Nacional y la Policía de Hacienda, fueron instituciones estatales encargadas de reprimir y perseguir políticamente durante buena parte del siglo XX. A ellas les acompañaron organizaciones paramilitares como los Escuadrones de la Muerte, responsables de torturas y asesinatos, y también algunas células guerrilleras que cometieron secuestros y asesinatos en objetivos no militares[30].

28 Marcelo Gabriel Ignacio Temperini, "Delitos informáticos en Latinoamérica: un estudio de derecho comparado. 1ra. Parte", http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf (consultado: 9 marzo, 2015).
29 Juan Duarte Torres et al., "La efectividad de la función de prevención especial en la aplicación de las medidas de seguridad a los inimputables" (tesis de Licenciatura, Universidad de El Salvador, 2013).
30 Comisión de la Verdad para El Salvador y Organización de las Naciones Unidas, "Informe de la Comisión de la Verdad para El Salvador. De la locura a la esperanza: la guerra de 12 años en El Salvador", (San Salvador-Nueva York, 1992-1993).

De la época del conflicto armado sobresale como caso paradigmático el asesinato de Herbert Anaya Sanabria en 1987, quien fuera director de la Comisión Nacional de Derechos Humanos (CDHES), organización no gubernamental dedicada a la defensa de los derechos humanos. Un año antes de su asesinato, Herbert ya había sido apresado por la ahora extinta Policía de Hacienda, entre otras formas de hostigamiento de las cuales él y todas las personas defensoras de derechos humanos de la época eran víctimas. Y, en general, todo aquel que manifestara su oposición al régimen o emitiera posición política que fuera considerada como subversiva.

La defensa de los derechos humanos en El Salvador también estuvo muy ligada con los esfuerzos de una parte de la Iglesia católica, que se dedicó a documentar violaciones de derechos humanos, así como a judicializar algunos casos. En 1982, la Arquidiócesis de San Salvador como iniciativa de Monseñor Arturo Rivera Damas creó la oficina de Tutela Legal del Arzobispado, como instancia encargada de la promoción y defensa de los derechos humanos, nombrando para ello a la doctora María Julia Hernández como su directora, quien se convertiría en un referente importante por la defensa de los derechos humanos en el país. Tutela Legal surgió para "desarrollar una pastoral de derechos humanos según la doctrina social de la Iglesia, para promover y defender la dignidad de la persona como imagen de Dios, instaurando así una cultura de reconciliación, justicia y paz"[31].

1.3.2. Los Acuerdos de Paz

Los Acuerdos de Paz de 1992 son un parte aguas en la historia de represión y persecución política de El Salvador. Estos acuerdos buscaban conseguir cuatro grandes objetivos: terminar el conflicto armado por la vía política; impulsar la democratización del país; garantizar el irrestricto respeto a los derechos humanos y reunificar la sociedad salvadoreña. Desde la perspectiva de los derechos humanos, los Acuerdos de Paz significaron importantes avances entre los cuales se pueden mencionar la disolución de tres cuerpos de seguridad íntimamente ligados con la sistemática violación de derechos humanos (Policía de Hacienda, Policía Nacional y Guardia Nacional), sustituyéndolas por una nueva Policía Nacional Civil (PNC); la creación de la Procuraduría para la Defensa de los Derechos Humanos (PDDH) y la Academia Nacional de Seguridad Pública (ANSP); así como la reforma a la doctrina del Ejército y su exclusión de toda actividad política y de seguridad pública, limitándola a la defensa nacional.

Pero más allá de evaluar el cumplimiento o avance de los Acuerdos de Paz, es importante remarcar que la persecución y la violación de derechos humanos por motivos políticos fue bastante superada. Posterior a 1992 hubo mucha sensibilidad por proteger jurídica y políticamente la libertad de expresión, de organización y participación política. Esto en contraste con el pasado reciente significó un gran avance. Sin embargo, esto no implica que la realidad salvadoreña de pobreza, corrupción

31 Arzobispado de San Salvador, Tutela Legal Arzobispado de San Salvador, (San Salvador, El Arzobispado, 2012), http://www.arzobispadosansalvador.org/index.php/medios-de-comunicacion/radio-paz/11-nosotros/15-tutela-legal (consultad: 20 mayo, 2015).

e impunidad fuera superada totalmente. En 2013, el entonces Procurador para la Defensa de los Derechos Humanos lo resumía de la siguiente manera:

> […] Se terminó el conflicto armado, pero las causas estructurales que lo originaron no se han resuelto totalmente: como pobreza, impunidad, crisis económica, inseguridad, entre otras [...] En este sentido debe destacarse que no obstante se ha avanzado en un proceso democratizador del país, el impulso que se le ha dado ha sido lento, y en algunos momentos más que avanzar hacia una sólida democracia, parecería que retrocedemos, esto como resultado de medidas o acciones públicas de parte de los gobiernos anteriores; medidas como dolarización, privatización de servicios públicos, políticas neoliberales, permisividad de la impunidad, justicia tardía, corrupción, ausencia de políticas públicas a favor de la población, crisis política y financiera, entre otras[32].

Luego de los Acuerdos de Paz no se registran denuncias sobre persecución de defensores ni defensoras de derechos humanos en El Salvador, al menos no sistemáticamente y no bajo las mismas modalidades del pasado. Por el contrario, las organizaciones salvadoreñas de derechos humanos en la actualidad se han enfocado en la defensa de otros derechos fundamentales como el acceso al agua, el medio ambiente, el acceso a la información pública, derechos de la mujer y derechos de salud sexual reproductiva y diversidad. Incluso, han denunciado desde El Salvador la persecución que sufren sus colegas en la región: "Estamos acá frente a la embajada de Honduras en El Salvador, con el objetivo de hacer un acto de presencia, denunciando la represión, la persecución, la amenaza que están viviendo mujeres Defensoras de los Derechos en Honduras[33]".

1.3.3. La actualidad: la defensa de los derechos humanos en el auge de la violencia social y el crimen organizado

El marco jurídico que puede ser utilizado para el control, vigilancia o persecución de defensoras y defensores de derechos humanos debe ser examinado desde este nuevo contexto de violencia social, en el que el accionar de las maras y el crimen organizado está siendo utilizada como justificación para realizar una serie de reformas y crear legislaciones que restringen derechos humanos fundamentales, ya que buena parte de la opinión pública, los medios y las élites políticas etiquetan la leyes que establecen garantías y derechos fundamentales como "protectoras de delincuentes" o diseñadas "para Suiza".

En ese sentido, tanto el Estado como la sociedad salvadoreña, ante la desesperación por frenar el

32 Procuraduría para la Defensa de los Derechos Humanos, "Balance sobre la situación de los derechos humanos a 21 años de los Acuerdos de Paz", (San Salvador, La Procuraduría, 2013), http://www.pddh.gob.sv/menupress/menuprensa/457-pddh-brinda-balance-sobre-la-situacion-de-los-derechos-humanos-a-21-anos-de-los-acuerdos-de-paz (consultado: 20 mayo, 2015).

33 Omar Fernández, "Organizaciones de Derechos Humanos denuncian represión y persecución del Estado hondureño a la coordinadora de Las Chonas Gladys Lanza" *Diario Co Latino*, 6 de febrero de 2015, bajo *sección Nacionales*, http://www.diariocolatino.com/organizaciones-de-derechos-humanos-denuncian-represion-y-persecucion-del-estado-hondureno-a-la-coordinadora-de-las-chonas-gladys-lanza/ (consultado: 5 noviembre, 2015)

aumento de la delincuencia y la violencia, han propiciado un franco retroceso en la aprobación de legislaciones penales menos garantistas y fragmentadas, que probablemente ayudan a responder a las ansias de la coyuntura pero que cuya efectividad es francamente cuestionable. La actitud predominante es la de ceder o rebajar derechos fundamentales en pos de alcanzar mayor seguridad, sin detenerse a reflexionar en la efectividad y conveniencia a largo plazo. En palabras de Luigi Ferrajoli:

> Tal crisis se manifiesta en la inflación legislativa provocada por la presión de los intereses sectoriales y corporativos, la pérdida de generalidad y abstracción de las leyes, la creciente producción de leyes-acto, el proceso de descodificación y el desarrollo de una legislación fragmentaria, incluso en materia penal, habitualmente bajo el signo de la emergencia y la excepción [...] Precisamente, el deterioro de la forma de la ley, la falta de certeza generalizada a causa de la incoherencia y la inflación normativa y, sobre todo, la falta de elaboración de un sistema de garantías de los derechos sociales equiparable, por su capacidad de regulación y de control, al sistema de las garantías tradicionalmente predispuestas para la propiedad y la libertad, representan, en efecto, no sólo un factor de ineficacia de los derechos, sino el terreno más fecundo para la corrupción y el arbitrio[34].

Por otra parte, en este nuevo contexto político salvadoreño debe tenerse en consideración que la persecución a defensoras y defensores de derechos humanos probablemente ya no solo deba ser examinada desde el Estado, sino que deben agregarse otros actores no menos relevantes como pueden ser las organizaciones criminales, tal como ha sucedido ya en otros países donde las redes de narcotráfico han comenzado a silenciar a todas aquellas personas que han denunciado su accionar.

Un reciente caso paradigmático sobre la persecución de defensoras y defensores de derechos humanos en el actual contexto político salvadoreño fue el asesinato de tres ambientalistas que se oponían a la explotación minera de la empresa internacional *Pacific Rim* en Cabañas. Este caso despertó muchas sospechas y aún no ha sido debidamente investigado, ya que algunas organizaciones y lugareños ligan los asesinatos con la postura y acción de los ambientalistas en contra de los proyectos de la empresa internacional, incluso llegando a implicar de manera directa a quien en esos tiempos fuera su representante y vicepresidente en El Salvador[35].

La posibilidad de la utilización de las nuevas tecnologías de la información y la comunicación, y del derecho respectivo, para la persecución u hostigamiento de defensores y defensoras de derechos humanos es algo que debe ser investigado no solo desde el Estado como ente persecutor, sino también desde otras organizaciones con los intereses y recursos para llevar a cabo estas acciones.

34 Luigi Ferrajoli, Derechos y garantías: el derecho del más débil (Madrid: Editorial Trotta, 2004), 15-16.
35 Saúl Monge, "Piden investigar a ex vicepresidente de *Pacific Rim*, por muerte de ambientalistas", *Periódico Verdad Digital*, 22 de septiembre de 2014, bajo *sección Social*, http://verdaddigital.com/archivo/index.php/32-social/12831-piden-investigar-a-ex-vicepresidente-de-pacific-rim-en-el-salvador-por-muertes-de-ambientalistas (consultado: 5 noviembre, 2015)

1.4. Conclusiones preliminares

La discusión con respecto a internet, telecomunicaciones y nuevas tecnologías en El Salvador ha sido guiada, en importante proporción, por las necesidades e intereses del mercado antes que por un afán de proteger los derechos fundamentales de la ciudadanía.

A pesar de encontrar una importante producción académica en algunos temas relacionados, sobre todo a nivel de tesis universitarias, en El Salvador existe una fuerte desvinculación entre la academia y las élites políticas, e incluso con los medios de comunicación. En ese sentido, el impacto de dicha producción, aunque pueda ser académicamente significativo y relevante, tiene poco impacto en la discusión de las élites políticas y los medios de comunicación.

En un país abatido por la violencia, la inseguridad y el alto costo de la vida, las preocupaciones por la seguridad de sus datos o la vigilancia que organismos públicos o privados puedan realizar a través de las nuevas tecnologías, parece no solo no ser prioritario sino estar poco presente en la agenda pública.

La mayoría de los temas de esta investigación son sumamente novedosos para el país y, apenas cuentan con incipientes trabajos periodísticos y académicos. Aspectos que fueron legislados y discutidos hace bastante tiempo en América del Sur, Europa y Estados Unidos, en El Salvador se encuentran apenas en ciernes en la discusión mediática y legislativa. Además, muy pocas personas en el país han sido formadas y cuentan con experiencia, tanto desde lo tecnológico como desde las ciencias sociales y el derecho, en estos temas.

2. Marco legal nacional

El presente capítulo desarrolla las protecciones y las limitaciones constitucionales, jurisprudenciales y de legislación secundaria del derecho a la privacidad en los contextos de la vigilancia del Estado y del sector privado cuando actúa en colaboración con el Estado. Este marco jurídico es el que podría ser utilizado para la criminalización de defensores y defensoras de derechos humanos, pero también el que podría ser usado para la defensa de sus derechos.

Los conceptos privacidad e intimidad están íntimamente vinculados, ya que integran una zona de reserva personal que es propia de la autonomía del ser humano, en donde se limita la intromisión de terceras personas[36]. El Salvador reconoce y protege el derecho a la intimidad de las personas como un derecho fundamental mediante el cual se debe propiciar el libre desarrollo de la personalidad, así como la protección de datos personales, actividades personales, documentos y medios de comunicación.

El derecho a la intimidad guarda relación con el libre desarrollo a la personalidad, con la toma de decisiones personalísimas y con la autorrealización personal, pues supone una determinada calidad de relación con los demás[37]. Por otra parte, la protección de datos personales es una de las manifestaciones del derecho a la intimidad y, aunque en El Salvador no existe una ley especial dirigida a brindar protección a los datos personales, en el ordenamiento jurídico se encuentran normas y mecanismos que pueden utilizarse para hacer valer este derecho.

2.1. Tratados internacionales

Es importante iniciar aclarando la relación entre el derecho internacional y el derecho interno en el ordenamiento jurídico salvadoreño, debido a que los avances tecnológicos en materia de vigilancia han provocado que desde hace algunos años expertos y organismos internacionales se encuentren realizado esfuerzos para mostrar cómo el derecho internacional de los derechos humanos se aplica en el contexto de la vigilancia[38].

En ese sentido, según el orden constitucional salvadoreño ningún instrumento internacional estará sobre la Constitución de la República. En caso de darse un conflicto entre una disposición del derecho internacional y una constitucional, primará esta última. Sin embargo, los tratados internacionales

36 Germán, Bidart Campos, Manual de la Constitución Reformada, Tomo I, (Buenos Aires: Ediar, 1998).
37 Santiago Velásquez Velásquez, y María Isabel Nuques, El derecho a la intimidad y la competencia desleal, (Ecuador: Facultad de Derecho de la Universidad Católica de Guayaquil; s.f.), 9.
38 Ver: Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones: https://es.necessaryandproportionate.org/text

debidamente ratificados son considerados leyes de la República y en caso de entrar en contradicción con una legislación secundaria interna, prevalecerá el tratado internacional (Arts. 144-149 Cn).

2.2. Constitución de la República de El Salvador

2.2.1. Vigilancia

2.2.1.1. Salvaguardas constitucionales del derecho a la privacidad en el contexto de la vigilancia a las comunicaciones

Debe destacarse que la Constitución salvadoreña garantiza el derecho a la intimidad personal y familiar y a la propia imagen en su artículo 2, estableciendo la indemnización por daños de carácter moral. Posteriormente señala que solo podrá practicarse el registro o la pesquisa de una persona para prevenir o averiguar delitos o faltas, y que la morada es inviolable, pudiendo ingresarse a ella únicamente por consentimiento de la persona que la habita, por mandato judicial, por flagrante delito o peligro inminente de su perpetración, o por grave riesgo de las personas. (Arts. 19 y 20).

Además, el artículo 24 establece que la correspondencia de toda clase es inviolable, prohibiendo la interferencia y la intervención de las telecomunicaciones, salvo algunas excepciones, las cuales serán desarrolladas posteriormente.

A criterio de la Sala de lo Constitucional de la Corte Suprema de Justicia, el derecho a la intimidad es:

> Un derecho fundamental estatuido directamente en el artículo dos 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[39].
>
> Las formas a través de las cuales pueden realizarse intromisiones a la esfera protegida por el derecho de intimidad son muchas, así por ejemplo: la apertura de la correspondencia, intercepción de comunicaciones telefónicas y electrónicas, divulgación de información bancaria, divulgación de historias clínicas, allanamientos ilegítimos de domicilio, secuestro de computadoras, acceso a los datos en manos de terceros, etc. El Código Penal tipifica algunas conductas que atentan contra el derecho a la intimidad de las comunicaciones, las cuales se mencionarán y explicarán adelante

Según la Constitución, todas las personas son titulares de este derecho y gozan de protección en toda circunstancia; lo cual implica que tienen derecho a estar protegidas contra cualquier ataque innecesario y desproporcional, y solo en caso de extrema necesidad y cuando exista un legítimo

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

interés público -o para proteger y garantizar otros derechos fundamentales-, puede limitarse este derecho por disposición de ley. La Constitución sí establece las premisas para proteger y evitar toda clase de intromisión en la vida privada, reconociendo la protección a la intimidad personal en el artículo 2, la protección a la morada (domicilio) en el artículo 20; y la protección (inviolabilidad) a la correspondencia y telecomunicaciones en el artículo 24[40].

Para proteger este derecho, la jurisprudencia constitucional ha constituido al recurso de amparo como la garantía para la protección de los derechos fundamentales en general, y por lo tanto, del derecho a la intimidad. En algunos casos, la Sala de lo Constitucional también ha utilizado como garantía el *habeas corpus*, por medio del cual han surgido importantes líneas y criterios jurisprudenciales para proteger el derecho a la intimidad de las personas. A continuación algunos ejemplos:

Sentencia 255-2000[41], en la que el peticionario fundaba su petición en grabaciones telefónicas obtenidas contrariando lo dispuesto en el artículo 24 de la Constitución. Sentencia 249-2002[42], en la que el peticionario fundamentó su pretensión constitucional en la vulneración a su derecho a la inviolabilidad del domicilio, por no haberse motivado la orden que autorizó el registro y allanamiento.

Sentencia 35–2005/32–2007[43], en la que el peticionario fundamentó su pretensión constitucional en la violación a su correspondencia, por lo cual no debió ser valorada en juicio para configurar la culpabilidad del imputado.

La protección de los datos es un derecho de reciente consagración y se refiere al "derecho de los individuos, grupos e instituciones para determinar por sí mismos cuándo, cómo y con qué extensión la información acerca de ellos es comunicada a otros"[44]. En ese orden de ideas, el derecho a la protección de datos se entiende como la suma de principios, derechos y garantías establecidos a favor de las personas que pudieran verse perjudicadas por el tratamiento de los datos personales.

La autodeterminación informativa, por su parte, es el derecho que tiene por objeto garantizar la facultad de las personas para conocer y acceder a las informaciones archivadas en bancos de datos que les conciernen, así como controlar su calidad, lo cual implica la posibilidad de corregir o cancelar los

40 Se establece que por ningún motivo se puede violentar la privacidad en la correspondencia de todo tipo; asimismo, prohíbe la interferencia e intervención de las telecomunicaciones, salvo excepciones, que puede provenir de una investigación o proceso judicial; punto desde el cual se garantiza el secreto a la correspondencia y de las telecomunicaciones.
41 Sala de lo Constitucional. Sentencia de Habeas Corpus 255-2000 del 14 de septiembre de 2000, http://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2000-2009/2000/09/11B4.PDF (consultado: 5 noviembre, 2015)
42 Sala de lo Constitucional. Corte Suprema de Justicia, Sentencia de Habeas Corpus 249- 2002 del 24 de febrero de 2003, http://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2000-2009/2003/02/1D94.PDF (consultado: 5 noviembre, 2015)
43 Sala de lo Constitucional. Corte Suprema de Justicia, Sentencia de Amparo 135 – 2005/32 – 2007 del 16 de mayo de 2008, http://www.jurisprudencia.gob.sv/DocumentosBoveda/D/1/2000-2009/2008/05/30F7.PDF (consultado: 5 noviembre, 2015)
44 María Elena Hernández León, et al., "Habeas Data como mecanismo de protección de derechos relacionados con la autodeterminación informativa ante el tratamiento automatizado de datos personales" (tesis de Licenciatura, Facultad de Jurisprudencia, Universidad de El Salvador, 2006), 95-6.

datos inexactos o indebidamente procesados, y disponer sobre su transmisión[45]. La autodeterminación informativa es entonces un aspecto del derecho a la protección de datos, mientras que el *habeas data* es una garantía -un instrumento procesal-, que no alcanzaría como medio a tutelar todo el derecho a la protección de datos, pues este incluye aspectos que exceden a las posibilidades del accionar judicial por la vía sumarísima y contradictoria del *habeas data*[46]. Por otra parte, la libertad informática se entiende como "la facultad de la persona para controlar la información personal que le concierne, la cual está contenida en registros públicos o privados"[47].

En El Salvador el derecho a la autodeterminación informativa no está regulado expresamente ni en la Constitución ni en la legislación secundaria. Para ejercer tal derecho debe recurrirse de manera supletoria al derecho a la intimidad regulado en el artículo 2 de la Constitución, ya que se considera a la autodeterminación informativa como una manifestación del derecho de intimidad. A la fecha, el desarrollo jurídico de la autodeterminación informativa se ha dado a través de criterios jurisprudenciales, emitidos por la Sala de lo Constitucional de la Corte Suprema de Justicia en sentencias provenientes de recursos de amparo.

La jurisprudencia constitucional salvadoreña ha establecido que el derecho a la autodeterminación informativa es la aplicación de la intimidad al ámbito informático y que tal derecho implica la protección de todo individuo frente a la posibilidad de acceso a la información personal que se encuentre contenida en bancos informatizados[48]. La jurisprudencia sostiene que el derecho a la autodeterminación informativa posee dos facetas: "(i) una material —preventiva—, relacionada con la libertad y la autonomía del individuo con relación a sus datos personales; y (ii) otra instrumental —de protección y reparación—, referida al control que la resguarda y restablece ante restricciones arbitrarias"[49].

La Sala de lo Constitucional ha establecido que la dimensión material del derecho a la autodeterminación informativa pretende "satisfacer la necesidad de las personas de preservar su identidad ante la revelación y el uso de los datos que les conciernen y los protege frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos"[50]. En esta faceta se destacan los siguientes derechos: "i) La facultad de conocer, en el momento específico de la recolección de los datos, el tipo de información personal que se va a almacenar; ii) la potestad de conocer la existencia de bancos de datos automatizados; iii) la libertad de acceso a la información; iv) la facultad de rectificación, integración o cancelación de los datos para asegurar su calidad y el acceso a ellos; y, v) la potestad de conocer la transmisión de los datos personales hacia terceros"[51].

45 Oscar Puccinelli, El Hábeas Data *(*Santa Fe de Bogotá, Colombia: Temis, S.A, 1999*)*, 66.
46 María Elena Hernández León et al.,"Habeas Data como mecanismo de protección s", 99.
47 Ayala, J.M. et al. *La protección de datos personales en El Salvador*. (El Salvador: UCA Editores, s.f.), 53.
48 Sala de lo Constitucional. Corte Suprema de Justicia, Sentencia de Amparo 934-2007 del 4 de marzo de 2011, parte III, 1 A.
49 Sala de lo Constitucional. Corte Suprema de Justicia, Sentencia de Amparo 142-2012 del 20 de octubre de 2014.
50 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 142-2012.
51 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 142-2012.

Respecto a la dimensión instrumental, la Sala de lo Constitucional sostiene que

> la autodeterminación informativa constituye un derecho al control de la información personal sistematizada o contenida en bancos de datos informáticos o ficheros. De ahí que, ante esa necesidad de vigilancia, este derecho posea un contenido múltiple e incluya algunas facultades relacionadas con esa finalidad controladora, las cuales se manifiestan, básicamente, en aquellas medidas estatales de tipo organizativo y procedimental indispensables para la protección del ámbito material del derecho asegurado constitucionalmente[52].

En Sentencia de Inconstitucionalidad con referencia 58-2007, se reafirmó que el ámbito de protección del derecho a la autodeterminación informativa implica diferentes facultades a favor de la persona, las cuales se reconocen para controlar

> el uso de la información personal que le atañe, tanto en su recolección como en su tratamiento, conservación y transmisión. Sin embargo, esa protección no es ilimitada, pues las personas carecen de derechos constitucionales absolutos sobre sus datos. De ahí que la persona haya de tolerar ciertos límites a su derecho de autodeterminación informativa, por razón de un interés general[53].

2.2.1.2. Limitaciones constitucionales al derecho a la privacidad en el contexto de la vigilancia

El derecho a la intimidad no es un derecho absoluto, tiene alcances y límites como la protección de la seguridad nacional y del orden público, y la protección de derechos y libertades de las demás personas. La Constitución establece que el Estado puede restringir este derecho, siempre y cuando se encuentre en peligro el goce de derechos fundamentales de terceros, o se esté en el marco de una investigación judicial de ciertos ilícitos penales.

La Constitución de la República no regula expresamente cuáles son los criterios legítimos que el legislador tiene para restringir o limitar los derechos fundamentales. Al respecto la Sala de lo Constitucional ha establecido que:

> […] Él puede tomar en cuenta el sustrato ético-ideológico que le da unidad y sentido al ordenamiento jurídico (los valores constitucionales), pero no puede exigírsele que lo haga, ya que su margen de acción (en la elección de fines, medios y ponderaciones) le permite perseguir cualquier fin que no esté proscrito constitucionalmente o que no sea manifiestamente incongruente con su trasfondo axiológico[54].

En el artículo 24, la Constitución establece que solo de manera excepcional podrá autorizarse judicialmente, de forma escrita y motivada, la intervención temporal de cualquier tipo de

52 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 142-2012.
53 Sala de lo Constitucional. Corte Suprema de Justicia, Sentencia de Inconstitucional 58-2007 del fecha 8 de marzo de 2013.
54 Sala de lo Constitucional. Corte Suprema de Justicia, Sentencia de Inconstitucional 84-2006 del 20 de enero de 2009.

telecomunicaciones, preservándose en todo caso el secreto de lo privado que no guarde relación con el proceso. Según la Constitución, la información proveniente de una intervención ilegal carecerá de valor. Una ley secundaria regula lo establecido en dicha disposición constitucional, por lo que será analizada con mayor profundidad más adelante.

Por otra parte, a criterio de la Sala de lo Constitucional, el derecho a la autodeterminación informativa puede verse restringido

> por la finalidad que persigue la recolección y administración de los datos personales, la cual debe ser legítima (constitucional o legal), explícita y determinada. Para talefecto, el legislador debe tener en cuenta no sólo el principio de proporcionalidad, sino también el derecho general del ciudadano a la libertad frente al Estado, que sólo puede ser restringida por el poder público cuando sea indispensable para la protección del interés general[55].

En ese sentido, la necesidad de reconocer el derecho a la autodeterminación informativa, así como la necesidad de una legislación secundaria que regule el *habeas data* o su inclusión en alguna ya existente, como podría ser en la Ley de Procedimientos Constitucionales, es de fundamental importancia para no generar situaciones de indefensión.

2.2.1.3. Mecanismo de acceso a la justicia en el contexto de vigilancia

En virtud de la jurisprudencia emitida por la Sala de lo Constitucional, se distingue la naturaleza dual del derecho a la autodeterminación informativa. A partir de dicha dualidad la Sala establece que

> […] se desprende que su garantía no puede limitarse a la posibilidad del ejercicio de pretensiones por parte de los individuos, sino que ha de ser asumida por el Estado mediante la creación de un ámbito de protección mucho más operativo en las medidas legislativas que lo desarrollan. En efecto, es el legislador quien se encuentra obligado a llevar a cabo las delimitaciones de las esferas individuales requeridas por la faceta instrumental —de protección y reparación— y, de tal manera, configurar una parte sustancial del derecho a la autodeterminación informativa[56].

La Constitución de la República en el artículo 2 garantiza el derecho al honor, a la intimidad personal (derecho a la autodeterminación informativa), y a la propia imagen; asimismo, el artículo 247 reconoce el amparo como mecanismo de protección ante la violación de este derecho. En razón de ello, el amparo -de manera supletoria- se convierte en la garantía para proteger derechos como la autodeterminación informativa, entre otros.

En el ordenamiento jurídico salvadoreño, como ya se mencionó anteriormente, no es reconocida la garantía del *habeas data*, como instrumento diseñado para la protección específica del derecho

55 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 142-2012.
56 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 142-2012.

a la autodeterminación informativa. Sin embargo, ello no significa que este derecho se encuentre totalmente desprotegido. La Sala de lo Constitucional reconoció que el *habeas data* no tiene regulación especial en El Salvador, pero que la protección al derecho a la autodeterminación informativa es factible a través del proceso constitucional de amparo, sin importar la naturaleza del ente a quien se le atribuya su vulneración[57].

De lo anterior se debe entender que toda persona que estime violaciones a su derecho a la intimidad y al derecho a la autodeterminación informativa, por causa de su inclusión en una base de datos delictiva, crediticia u otra naturaleza, y especialmente por el uso no autorizado de su información personal, tiene derecho a interponer ante la Sala de lo Constitucional el recurso de amparo correspondiente.

2.2.2. Anonimato y cifrado

2.2.2.1. Salvaguardas constitucionales para la protección del cifrado y el anonimato

No se encontraron ni en la Constitución salvadoreña ni en la jurisprudencia constitucional regulaciones relacionadas directamente con las técnicas de cifrado ni con el anonimato digital. Sin embargo, el anonimato y el cifrado son necesarios para el efectivo ejercicio de los derechos a la intimidad y a la libertad de expresión reconocidos en la Constitución y desarrollados en la jurisprudencia constitucional.

a) Cifrado

Expertos internacionales sostienen que en el entorno digital actual, la posibilidad de utilizar la tecnología de cifrado puede ser considerada como un prerrequisito para el ejercicio de los derechos de privacidad y de expresión, ya que en ausencia de cifrado las comunicaciones pueden ser fácilmente interceptadas. Los intermediarios de internet a menudo están en condiciones de poseer y leer todas las comunicaciones que pasan a través de sus redes, relacionando el cifrado directamente con la protección de intimidad. Por otra parte, el cifrado protege la libertad de expresión directamente cuando impide que sistemas automatizados de censura bloqueen el acceso a un contenido en particular o, incluso, a palabras clave en específico. Además, la protege indirectamente al guardar la confidencialidad de las comunicaciones y fuentes de sus usuarios[58]. En ese sentido,el Relator para la Libertad de Expresión de las Naciones Unidas, David Kaye, ha sostenido que:

> Actualmente el cifrado y el anonimato son los principales vehículos para la seguridad en línea, proporcionando a los individuos con un medio para proteger su privacidad, dándoles el poder de navegar, leer, desarrollar y compartir opiniones e información sin interferencias y apoyando a los periodistas, organizaciones de la sociedad civil, miembros de las minorías étnicas o grupos

57 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 934-2007 del 4 de marzo de 2011, parte III 1. B. a.
58 Rodríguez, Katitza, *Anonimato y Cifrado: Comentarios enviados a la Relatoría Especial de la Comisión de Derechos Humanos.*

religiosos, a los perseguidos debido a sus orientación sexual o identidad de género, activistas, académicos, artistas y a otros los derechos a la libertad de expresión y opinión […] El Cifrado y el anonimato y los conceptos de seguridad detrás de ellos ofrecen la privacidad y la seguridad necesaria para el ejercicio del derecho a la libertad de opinión y de expresión en la era digital. Dicha garantía puede ser esencial para el ejercicio de otros derechos, incluidos los derechos económicos, la privacidad, el debido proceso la libertad de reunión y de asociación pacíficas, y el derecho a la vida y la integridad corporal[59].

El cifrado es el proceso matemático de utilizar códigos y claves para comunicarnos de forma privada. A lo largo de la historia, la gente ha utilizado métodos cada vez más sofisticados de cifrado para enviarse mensajes entre sí con el objetivo de que no puedan ser leídos por cualquier persona además de los destinatarios. Hoy en día, las computadoras son capaces de realizar un cifrado mucho más complejo y seguro.

Fuente: Rodríguez, Katitza, *Anonimato y Cifrado: Comentarios enviados a la Relatoría Especial de la Comisión de Derechos Humanos sobre la promoción y protección del derecho a la libertad de opinión y de expresión* (International: EFF, 2015), 37.

En El Salvador, el cifrado se encuentra protegido constitucionalmente a través de la libertad de expresión al ser un derecho fundamental reconocido y protegido en el artículo 6. Según la Constitución salvadoreña, comprende el derecho que tiene toda persona sin distinción alguna, a expresar y difundir libremente sus pensamientos. Esto significa que no se necesita ningún estudio o consideración de un hecho o asunto anticipado, ni un dictamen o juicio previo, ni debe rendirse garantía alguna para ejercer este derecho[60].Por otra parte, la libertad de expresión está íntimamente relacionada con la libertad de prensa y derecho a la información, por ser fundamentales para la formación de la opinión pública[61].

Por su parte, la Sala de lo Constitucional considera a través de su jurisprudencia que los derechos fundamentales son amplios en cuanto a su contenido y que la protección que debe dárseles por parte de las instituciones del Estado debe ser muy amplia[62]. En ese sentido, esta interpretación amplia sobre la protección de los derechos fundamentales podría servir de fundamento para la utilización de

59 Kaye, D. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression". Human Rights Council. Twenty-ninth session, http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc (consultado: 22 mayo, 2015)

60 El Salvador "Constitución de la República" Asamblea Legislativa (1983), artículo 6: Toda persona puede expresar y difundir libremente sus pensamientos siempre que no subvierta el orden público, ni lesione la moral, el honor, ni la vida privada de los demás. El ejercicio de este derecho no estará sujeto a previo examen, censura ni caución; pero los que haciendo uso de él, infrinjan las leyes, responderán por el delito que cometan.

61 Sergio García Ramírez, y Alejandra Gonza, *Libertad de Expresión en la jurisprudencia de la Corte Interamericana de Derechos Humanos*, (México DF.: Corte Interamericana de Derechos Humanos, Comisión de Derechos Humanos del Distrito Federal, 2007), 17.

62 Sala de lo Constitucional. Corte Suprema de Justicia, Sentencia de Inconstitucionalidad 91- 2007 del 24 de septiembre de 2010, http://www.csj.gob.sv/Comunicaciones/Boletin_informativo/2010/Septiembre_2010/Sentencia%2091-2007%20Art%20191%20con%20voto%20razonado.pdf (consultado: 5 noviembre, 2015) En relación a la colisión de derechos fundamentales, la Sala señala que para buscar el equilibrio entre estos debe haber una ponderación caso por caso, pues no existe en la Cn. una jerarquía, sino que todos los derechos tienen la misma fuerza y es ante una situación concreta que uno puede preponderar sobre otro.

técnicas de cifrado, en orden a proteger directamente su intimidad, pero también de manera indirecta su derecho a informarse y formarse una opinión, como etapa previa y necesaria para expresarse.

b) Anonimato

El anonimato puede ser necesario para quienes estén preocupados por retribuciones políticas o económicas, acoso, o incluso amenazas a sus vidas, lo cual dependerá de las situaciones socio-políticas en las que se encuentren y de la calidad que tengan o función que desempeñen. En ese sentido, el anonimato estará ligado con la necesidad de protección de la persona[63]. El informe del ex Relator para la Libertad de Expresión de Naciones Unidas, Frank La Rue, sostiene que:

> El anonimato de las comunicaciones es uno de los adelantos más importantes facilitados por Internet, que permite a las personas expresarse libremente sin temor a represalias o condenas [...] El derecho a la intimidad suele entenderse como un requisito esencial para la realización del derecho a la libertad de expresión. La injerencia indebida en la intimidad de las personas puede limitar en forma tanto directa como indirecta el libre intercambio y evolución de ideas. Las restricciones al anonimato de las comunicaciones, por ejemplo, tienen un efecto intimidatorio en las víctimas de todas las formas de violencia y abuso, que podrían ser renuentes a denunciarlas por temor a la doble victimización [...] Los Estados deben abstenerse de obligar a los usuarios a presentar sus documentos de identidad como condición previa para obtener acceso a las comunicaciones, incluidos los servicios en línea, los cibercafés o la telefonía móvil[64].

El anonimato se puede definir como actuar o comunicarse sin usar o presentar el nombre o identidad propios; o como actuar o comunicarse en una manera que protege la determinación del nombre o identidad propios, o usando un nombre asumido o inventado que no puede necesariamente asociarse con la identidad legal o habitual de uno.

Fuente: Rodríguez, Katitza, *Anonimato y Cifrado: Comentarios enviados a la Relatoría Especial de la Comisión de Derechos Humanos sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, 3.

La Constitución no contempla ninguna disposición que aborde de manera directa el derecho o la posibilidad de guardar el anonimato, como tampoco se identifican limitaciones directas. De manera general, el Estado salvadoreño tiene la obligación de brindar protección a las personas y asegurar el goce de los derechos humanos, por lo que debe proveer los mecanismos necesarios para que se cumplan y no sean vulnerados. Por lo que de seguirse el precepto constitucional que nadie está obligado a hacer lo que la ley no manda ni a privarse de lo que ella no prohíbe, tanto cifrado como anonimato pueden darse según nuestra Constitución (Art. 8). Más aún, como mencionamos anteriormente, la protección de los derechos por parte de las instituciones del Estado debe ser muy

63 Rodríguez, Katitza, *Anonimato y Cifrado: Comentarios enviados a la Relatoría Especial de la Comisión de Derechos Humanos*.
64 La Rue, F. "Informe del Relator para la Libertad de Expresión de Naciones Unidas", (Washington, D.C.: Asamblea General de las Naciones Unidas, 2013), http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/06/PDF/G1313306.pdf (consultado: 12 noviembre, 2015), párrafos 23, 24 y 88.

amplia[65]. En ese sentido, esta interpretación amplia sobre la protección de los derechos fundamentales podría servir de fundamento para el derecho que tiene toda persona a expresarse y formar una opinión anonimamente.

2.2.2.2. *Limitaciones constitucionales al cifrado y el anonimato*

No se encuentran normas específicas ni generales que puedan limitar el cifrado ni el anonimato en el texto constitucional.

2.2.2.3. *Mecanismos de acceso a la justicia en el contexto del cifrado y el anonimato a nivel constitucional*

A criterio de la Sala de lo Constitucional, todo derecho fundamental puede generar uno o varios tipos de obligación de parte del Estado, dentro de las cuales se destacan: i) de respetar – no violar los derechos por acción u omisión-; ii) de proteger – velar porque los particulares no violen los derechos-; iii) de garantizar – adoptar medidas en caso de que la persona sea incapaz de satisfacer el derecho por sí misma- ; y iv) de promover- adoptar medidas de largo alcance con el fin de fortalecer el derecho-[66].

La protección que otorga la Constitución de la República puede llevarse a la práctica por medio del recurso de amparo constitucional (cuando se trata de un particular o el Estado), o del proceso de inconstitucionalidad cuando una normativa vulnere derechos constitucionales relacionadas con la libertad de expresión, como el anonimato o el cifrado.

Si existe extralimitación en el ejercicio del derecho de libertad de expresión por parte de un tercero, y vulnera derechos como la intimidad, el honor, y buena imagen de otras personas, la consecuencia jurídica será el cometimiento de un delito, por lo que la persona que ha vulnerado tal derecho podrá ser procesada en un juicio penal, en el cual puede ser condenada a responder penal y civilmente.

2.3. Leyes, reglamentos y jurisprudencia

2.3.1. Vigilancia, cifrado y anonimato en leyes y reglamentos

A continuación se desarrolla la normativa secundaria y sus reglamentaciones en el contexto de la vigilancia de las comunicaciones por la autoridad pública, así como legislaciones que contemplen protección y/o limitaciones al cifrado y el anonimato.

65 Sala de lo Constitucional. Corte Suprema de Justicia, Sentencia de Inconstitucionalidad 91- 2007 del 24 de septiembre de 2010, http://www.csj.gob.sv/Comunicaciones/Boletin_informativo/2010/Septiembre_2010/Sentencia%2091-2007%20Art%20191%20con%20voto%20razonado.pdf (consultado: 5 noviembre, 2015) En relación a la colisión de derechos fundamentales, la Sala señala que para buscar el equilibrio entre estos debe haber una ponderación caso por caso, pues no existe en la Cn. una jerarquía, sino que todos los derechos tienen la misma fuerza y es ante una situación concreta que uno puede preponderar sobre otro.

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

2.3.1.1. Normas en materia penal

La legislación salvadoreña determina los límites al ejercicio absoluto del derecho a la intimidad y establece expresamente situaciones en las cuales el Estado tiene la potestad de intervenir. El Código Procesal Penal determina que cuando se requiera intervenir las telecomunicaciones de una persona que está siendo investigada o procesada, se deberá 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)[67]. Por su parte, el Código Penal tipifica algunas conductas que atentan contra el derecho a la intimidad e intercepción de las comunicaciones: violación de comunicaciones privadas (Art. 184); violación agravada de comunicaciones (Art. 185); captación de comunicaciones (Art. 186); revelación del secreto profesional (Art. 187), y utilización de la imagen o nombre de otro (Art. 190).

Debido a la grave situación de violencia imperante en el país, existe un programa estatal para la protección de víctimas y testigos, para los cuales el anonimato es fundamental. En consonancia con este programa, el Código Penal establece como delito la divulgación de la imagen o revelación de datos de personas protegidas. En su artículo 147 literal "f" dice que quien divulgare la imagen o revelare datos que permitan identificar a una persona beneficiaria del programa de protección de víctimas y testigos será sancionado con prisión de cuatro a ocho años. Dicha pena se agravará cuando ocurrieren lesiones o la muerte de la persona protegida o el hecho hubiere sido cometido por un funcionario o empleado público, autoridad pública o agente de autoridad.

Por otra parte, la Ley Especial para la Intervención de las Telecomunicaciones en su artículo 1[68] establece que de manera excepcional podrán intervenirse las comunicaciones mediante autorización judicial, cuando se tenga sospecha fundamentada de la comisión de ciertos delitos[69]. El artículo 5 de la referida ley regula de manera taxativa los delitos -16 en total- en los cuales se podrá hacer uso de la facultad de intervención[70]:

67 El Salvador "Código Procesal Penal" Asamblea Legislativa, (2009), artículo 176.
68 La Ley fue creada mediante Decreto Legislativo Nº 285 de fecha 18 de febrero de 2010, publicado en el Diario Oficial Nº51 , Tomo Nº386, de fecha 15 de marzo del año 2010.
69 El Salvador "Ley Especial para la Intervención de las Telecomunicaciones" Asamblea Legislativa (2010), artículo 1.
70 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.

Por otra parte, la Ley Especial contra el Delito de Extorsión[71] en su artículo 8, referido a las técnicas de investigación y aspectos probatorios, establece la grabación de llamadas telefónicas de uno de los interlocutores, así como cualquier otro medio tecnológico que les lleve al convencimiento de que la existencia del delito y la participación delictiva podrán ser utilizadas, de conformidad con al artículo 46 de la Ley Especial para la Intervención de las Telecomunicaciones. El artículo 10 regula que se podrá obtener o almacenar información electrónica contenida en algún dispositivo electrónico cuando se tenga sospecha que se está cometiendo un delito, previa autorización de un juez.

La Ley Orgánica de la Policía Nacional Civil en su artículo 25, numeral 7, establece que –en general- no se podrán intervenir las comunicaciones telefónicas, tal como lo establece la Constitución en el artículo 24 de la Constitución[72], salvo en los casos previamente establecidos y bajo el procedimiento estipulado para su autorización.

En lo que respecta a cifrado, en la legislación secundaria sí aparece la figura de manera expresa. La Ley para la Intervención de las Telecomunicaciones en su artículo 4, literal "D" reconoce y define la encriptación o cifrado, utilizándolas como sinónimos, como aquel sistema mediante el cual, con la ayuda de técnicas diversas o programas informáticos, se cifra o codifica determinada información con la finalidad de volverla inaccesible o ininteligible a quienes no se encuentran autorizados para tener acceso a ella.

Asimismo, en su artículo 21 establece que si el material grabado en el transcurso de una intervención legal no ha podido ser traducido o interpretado, total o parcialmente, por encriptación, protección por contraseñas u otra razón similar, el Centro de Intervención de las Telecomunicaciones conservará el material hasta su traducción o interpretación. El fiscal a cargo deberá indicar en detalle tal circunstancia al juez autorizante, entregándole la grabación íntegra de dicho material. Una vez revelado el material, el fiscal deberá remitir una copia de este al juez autorizante.

Por otra parte, la Ley de Telecomunicaciones en su artículo 6 define la encriptación como el sistema mediante el cual, con la ayuda de técnicas o programas informáticos, se cifra o codifica determinada información con la finalidad de volverla inaccesible o ininteligible para alguien no autorizado a acceder a ella.

En el artículo 42 literal D se establece que los operadores de redes comerciales de telecomunicaciones deberán desencriptar o asegurar que las autoridades puedan desencriptar cualquier comunicación de un suscriptor o cliente en los casos en que la encriptación haya sido proveída por el operador de servicio, todo ello con el propósito de obtener la información de personas que se encuentren bajo investigación judicial.

71 El Salvador "Ley Especial contra el Delito de Extorsión" Asamblea Legislativa (2015), artículos 8,10, y 12.
72 El Salvador "Ley Orgánica de la Policía Nacional Civil" Asamblea Legislativa (2001), artículo 27 No. 7.

Sin embargo, ninguna de estas legislaciones prohíben ni limitan la utilización de la encriptación, por lo que en aplicación de la disposición constitucional que establece, en su artículo 8, que nadie está obligado a hacer lo que la ley no manda ni a privarse de lo que ella no prohíbe, podemos inferir que el cifrado no está prohibido ni restringido en El Salvador.

2.3.1.2. Normas sobre inteligencia y contrainteligencia

El artículo 6 de la Ley del Organismo de Inteligencia del Estado habla sobre la facultad de esta entidad para hacer acopio de información, pero no establece el tiempo para mantener esa información en sus manos. Esta ley obliga a las instituciones y oficinas públicas a brindar la información que le sea requerida.

Al mismo tiempo, la Inteligencia del Estado está facultada para la realización de las actividades de inteligencia que conlleven a mantener la seguridad nacional, debiendo actuar con pleno respeto de los derechos y garantías constitucionales según la ley. Sin embargo, no establece formas ni límites para la realización del acopio de información ni para el ejercicio de inteligencia, con lo cual deja bastante abierta la posibilidad de cualquier tipo de vigilancia ilegal sobre opositores políticos y de personas defensoras de derechos humanos.

Según el artículo 8 todos los asuntos, actividades, documentación sobre los cuales conozca y produzca el Organismo de Inteligencia del Estado, serán considerados clasificados, cuyo manejo corresponderá al Presidente de la República. Por otra parte, la información sobre su estructura y funciones se clasifica como reservada.

2.3.1.3. Normas en el sector de telecomunicaciones

Según la Ley de Telecomunicaciones en su artículo 29, el usuario tiene derecho a acceder al servicio público de telefonía y mantener comunicaciones sin interferencias ni intervenciones; así como al secreto de sus comunicaciones y a la confidencialidad de sus datos personales[73].

Sin embargo, esta misma ley establece en sus artículos 42B y 42C que los operadores de redes comerciales de telecomunicaciones deberán brindar información relativa al origen, dirección, destino o terminación de la marcación o recepción de llamadas telefónicas de los números de sus usuarios que se encuentren bajo investigación, que se hayan generado o recibido por medio de equipo, facilidades o servicios de telecomunicación del operador de telefonía. Los operadores de redes comerciales de telecomunicaciones deberán poner a disposición de las autoridades correspondientes las bases de datos que contengan la información mencionada en el artículo anterior.

73 El Salvador "Ley de Telecomunicaciones", artículo 29, literal a) y b). "Art. 29. Son derechos de los usuarios: a) A acceder al servicio público de telefonía y mantener comunicaciones sin interferencias ni intervenciones; b) Al secreto de sus comunicaciones y a la confidencialidad de sus datos personales no públicos, teniendo en cuenta lo mencionado en el Título V-Bis, Capítulo Único de la presente ley. […]"

Según el artículo 30-A de la Ley de Telecomunicaciones, es obligación de los operadores de servicios de acceso llevar un registro de todos los usuarios incluyendo los de pago previo, debiendo mantener dicha información a disposición de la Fiscalía General de la República. Además, el artículo 34 de la misma ley establece que las empresas operadoras cometerán una infracción muy grave cuando nieguen la información que les requiera la Superintendencia General de Electricidad y Telecomunicaciones (SIGET)[74], especialmente aquella relacionada con sus usuarios. Dicha infracción será sancionada con una multa de $45 mil a $57 mil dólares estadounidenses, además de una multa de $571 dólares estadounidenses por cada día en que la infracción continúe.

2.3.1.4. Otras normas

En cuanto a protección de datos, la Ley de Acceso a la Información Pública (LAIP) regula y desarrolla expresamente lo relativo a protección de datos personales en manos de entidades públicas o privadas que administran servicios públicos, en sus artículos del 31 al 39. Así también, la Ley de Protección al Consumidor en el artículo 21[75] reconoce el derecho a la protección de datos del consumidor[76], según el cual se requiere de autorización previa y por escrito por el titular para que sus datos crediticios sean utilizados.

Con respecto a vigilancia de las telecomunicaciones, el artículo 10 de la LAIP establece que se considera como información pública las estadísticas que generen todos los entes obligados, dentro de los cuales se encuentra la Fiscalía General de la República, institución pública responsable del Centro de Intervenciones a las Telecomunicaciones. En ese sentido, de acuerdo con la LAIP, se considera información pública el número de intervenciones a las telecomunicaciones que se hayan realizado en cierto período de tiempo, siempre y cuando no se revele otra información considerada como confidencial.

Esta disposición de la LAIP no riñe con el principio de reserva y confidencialidad de la Ley Especial para la Intervención de las Telecomunicaciones (Art. 2), que establece que el procedimiento de intervención de las telecomunicaciones será reservado y la información privada ajena a la investigación será estrictamente confidencial, pues de acuerdo con la LAIP lo único que deberá ser público son las estadísticas anuales, sin publicar las partes involucradas ni cualquier otro pormenor que ponga en riesgo la investigación.

Por otra parte, existen otras disposiciones dispersas en leyes secundarias, principalmente vinculadas a la posibilidad y validez de firma electrónica, que habilitan la necesidad de mecanismos tecnológicos

74 La Superintendencia General de Electricidad y Telecomunicaciones (SIGET), es la entidad responsable de aplicar y velar por el cumplimiento de las normas y regulaciones establecidas en la Ley de Telecomunicaciones.
75 El Salvador "Ley de Protección al Consumidor" Asamblea Legislativa (2005), artículo 21.
76 La protección de datos del consumir es consecuencia del derecho a la intimidad, así lo ha establecido la Sala de lo Constitucional a través de sentencia bajo referencia 118-2002 emitida el 2 de marzo de 2004.

para salvaguardar la privacidad, como puede ser el uso de cifrado. Es importante tener en cuenta que dichas disposiciones responden principalmente a las necesidades del comercio electrónico y no tanto a la protección de la privacidad de la ciudadanía. Sin embargo, puede ser utilizadas en favor del uso de cifrado.

La Ley de Simplificación Aduanera[77] en su artículo 6 contempla que la declaración para destinar aduaneramente las mercancías, puede efectuarse mediante transmisión electrónica de la información conforme los lineamientos y formatos físicos y electrónicos establecidos por la Dirección General de Impuestos del Ministerio de Hacienda, a través de un sistema conocido como teledespacho, el cual, para asegurar la integridad de los flujos de información, deberá estar estructurado por procedimientos que aseguren la autenticidad, confidencialidad, integridad y no repudiación de la información transmitida.

Además, en el literal "f" del artículo 8 de la misma ley se establece que deben tomarse las medidas técnicas y administrativas tendientes a evitar la falsificación de llaves públicas y certificados. Para efectos de esta ley, teledespacho se entiende como el conjunto sistematizado de elementos tecnológicos de carácter informático y de comunicaciones que permiten, dentro de un marco de mutuas responsabilidades, y mediante los procedimientos autorizados, el intercambio por vía electrónica de información de trascendencia tributaria entre la Dirección General y los usuarios y auxiliares del servicio aduanero, bancos y en general, los operadores e instituciones controladoras del comercio exterior.

Por otra parte, en el artículo 90 de la Ley General Marítimo Portuaria[78] se contempla el intercambio electrónico de datos, estableciendo que para la emisión de algunos documentos de interés podrá emplearse cualquier medio por el que quede constancia de la información que contenga. Cuando el usuario y el armador o transportador convengan en comunicarse electrónicamente, dichos documentos podrán ser sustituidos por un mensaje de intercambio electrónico de datos. Dicha disposición establece que la firma podrá ser manuscrita, o bien estampada mediante facsímil o autenticada por un código electrónico. Así también, en los considerandos de la Ley de Anotaciones Electrónica en cuenta de Valores[79] se reconoce la firma por medio de código electrónico, y la Ley de Bancos[80] también reconoce la posibilidad de sustitución de la firma autógrafa por códigos electrónicos para ciertos contratos y transacciones.

77 El Salvador "Ley de Simplificación Aduanera" Asamblea Legislativa (1999), http://www.mh.gob.sv/portal/page/portal/PCC/SO_Administracion_Aduanera/Leyes/36_Ley_de_Simplificacion_Aduanera.pdf (consultado: 5 noviembre, 2015)

78 Ver: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-general-maritima-portuaria

79 Ver: http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/ley-de-anotaciones-electronicas-de-valores-en-cuenta

80 Ver: https://www.ssf.gob.sv/descargas/Leyes/Leyes%20Financieras/Ley%20de%20Bancos.pdf

Ante la ausencia de una Ley de Firma Electrónica, estas disposiciones reconocen ciertos aspectos relativos a la firma electrónica debido a las necesidades del mercado, abriendo indirectamente la puerta para el reconocimiento de manera indirecta del uso de mecanismos de cifrado.

2.3.2. Sobre allanamientos y registros

El registro con orden judicial, establecido en el artículo 191 del Código Procesal Penal (CPP), se dará cuando la Fiscalía General de la República o la Policía Nacional Civil tengan motivo fundado para presumir que en un lugar público o privado existen objetos relacionados con la comisión del hecho punible que se investiga. Para ello necesitarán la expedición de una orden judicial de registro de ese lugar, la cual deberá ser librada por escrito, especificando el lugar en que la diligencia habrá de practicarse, el tiempo durante el cual la orden estará vigente y el objeto de la diligencia.

Esta disposición habilita a la Policía para que, si en la práctica de la diligencia encuentra efectos concernientes a acciones delictivas distintas a la que se investiga, los incaute, identifique y ponga a disposición de la Fiscalía junto con un informe pormenorizado de su actuación. Esto podría ser utilizado para la obtención de computadoras y otros dispositivos con información personal y de trabajo.

Por otra parte, los allanamientos sin orden judicial se encuentran contemplados en el artículo 195 del CPP, el cual establece que la Policía podrá proceder al allanamiento sin orden judicial únicamente en los casos siguientes: 1) En persecución actual de un delincuente; 2) Cuando se tenga conocimiento que dentro de una casa o local se está cometiendo un delito o cuando en su interior se oigan voces que anuncien que se está cometiendo o cuando se pida auxilio o por grave riesgo de la vida de las personas, y 3) En los casos de incendio, explosión, inundación u otro estrago con amenaza de la vida o de la propiedad.

La requisa personal, contemplada en el artículo 196 y 197 del CPP, se dará cuando la Policía tuviere motivos suficientes para presumir que una persona oculta entre sus ropas, pertenencias, o lleva adheridos a su cuerpo, objetos relacionados con el delito. De todo lo acontecido se levantará un acta que deberá ser firmada por el policía que practicó la requisa y por la persona requisada. Si este rehusara firmar, el policía dejará constancia de ello en el acta. Para realizar el registro de vehículos, muebles y compartimientos cerrados, serán aplicables las reglas de la requisa personal.

En caso de encontrar información electrónica contenida en computadoras u otro tipo de dispositivos electrónicos como resultado de una requisa policial, se deberá aplicar el artículo 201 del CPP, el cual establece que solo los fiscales podrán solicitar la autorización judicial para la obtención, resguardo o almacenamiento de la información, pudiendo incluso ordenar su secuestro. En ese sentido, la Policía no podrá quedarse con dispositivos provenientes de una requisa personal, sino solo cuando se encuentre actuado bajo la dirección de la Fiscalía y/o cuenten con la debida autorización judicial.

En el artículo 198 del mismo código se establece que no podrán ser utilizados en la investigación o el proceso los documentos y objetos encontrados en el registro que se refieran a: 1) Las comunicaciones entre el imputado y sus defensores; 2) Las comunicaciones escritas entre el imputado y las personas que están facultadas para abstenerse de declarar, y 3) Los archivos de las personas indicadas en los numerales precedentes que contengan información confidencial relativa al imputado. Este apartado comprende también los documentos digitales, videos, grabaciones, ilustraciones y cualquier otra imagen que sea relevante a los fines de la restricción. Esta exclusión no tendrá lugar cuando se obtenga autorización expresa de su titular o cuando se trate de personas vinculadas como partícipes o coautoras del delito investigado o de uno conexo.

En el artículo 201 del CPP se establece que la obtención y resguardo de información electrónica solo será procedente bajo autorización judicial, cuando la Fiscalía tenga razones fundadas para inferir que una persona posee información constitutiva de delito o útil para la investigación, almacenada en equipos o instrumentos tecnológicos de su propiedad o posesión. La Fiscalía deberá adoptar las medidas que garanticen la obtención, resguardo o almacenamiento de la información, pudiendo solicitar al juez el secuestro previo respectivo. Dicha disposición deberá seguir las formalidades establecidas en el artículo 191 donde se regula el registro con orden judicial.

2.3.3. Supervisión pública

La entidad que realiza las intervenciones legales de las telecomunicaciones es el Centro de Intervención de las Telecomunicaciones, el cual depende de la Fiscalía General de la República (FGR). Las intervenciones se harán en colaboración con la Policía Nacional Civil, previa autorización y control de un Juez de Instrucción, el cual deberá garantizar que la intervención se desarrolla de conformidad con las condiciones establecidas en su resolución.

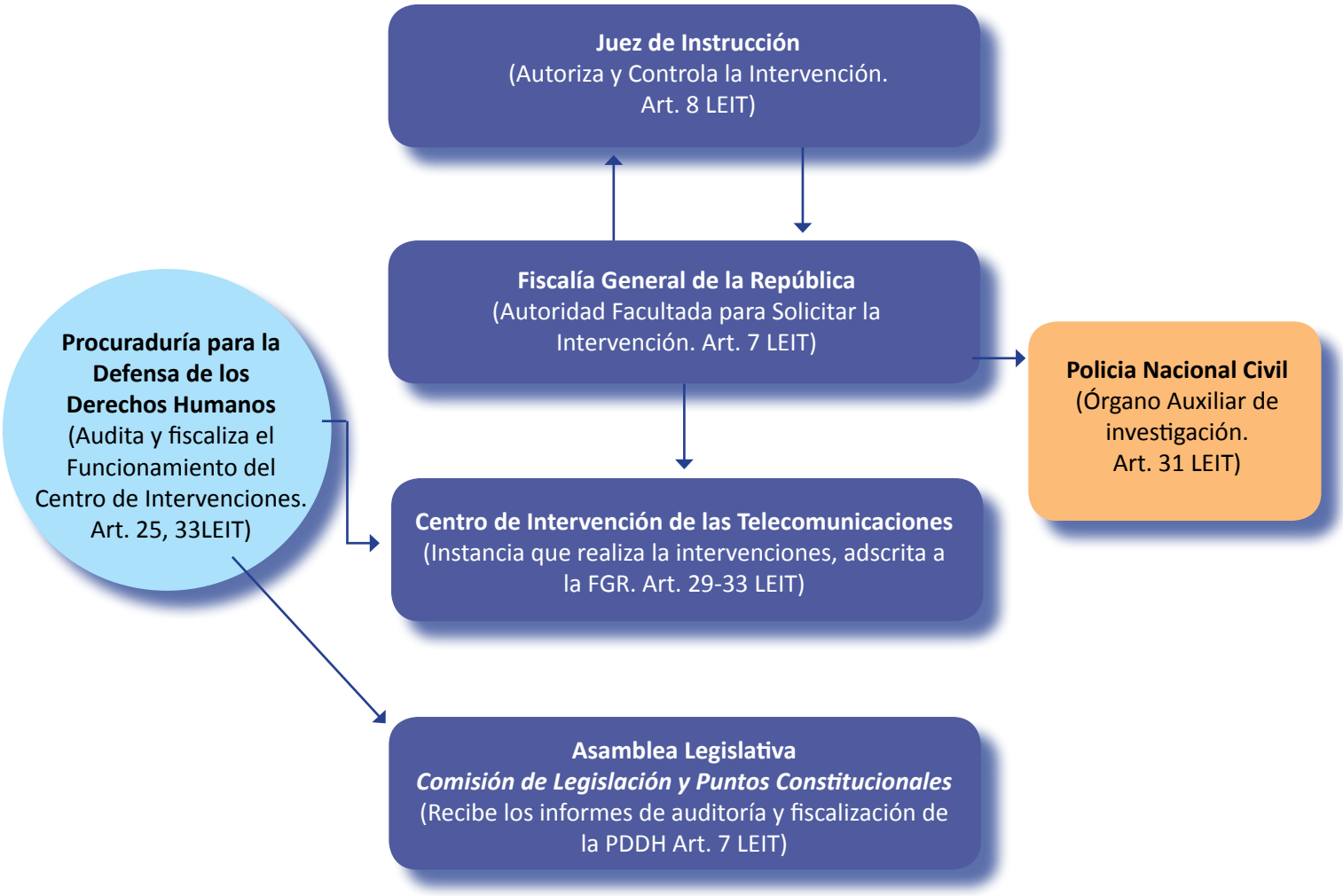
Por su parte, el Procurador para la Defensa de los Derechos Humanos (PDDH), en conjunto con el Fiscal General de la República, se encuentra facultado legalmente para elaborar el Protocolo de Funcionamiento del Centro de Intervención en cuanto a la fiscalización periódica y auditoría del mismo, según lo establece la Ley Especial para la Intervención de Telecomunicaciones. El Procurador también tiene la facultad de practicar anualmente una auditoría a las actividades del Centro y remitir el informe respectivo a la Comisión de Legislación y Puntos Constitucionales de la Asamblea Legislativa. La ley también lo faculta para realizar las auditorías específicas que estime convenientes sobre la violación del derecho a la intimidad o secreto de las telecomunicaciones. Dichas auditorías específicas se anexarán al informe general que se enviará a la Comisión Legislativa (Arts. 26, 33).

La PDDH será el principal órgano de supervisión en el proceso de intervención de las telecomunicaciones. Es importante señalar que la PDDH es una institución independiente, que surge como resultado de los Acuerdos de Paz, en 1992. El Procurador para la Defensa de los Derechos Humanos es un funcionario

de elección secundaria a través de la Asamblea Legislativa, que tiene el mismo nivel político de la Fiscalía General de la República, siendo ambas instituciones parte de lo que la Constitución reconoce como Ministerio Público. Sin embargo, y a pesar del rol protagónico de la PDDH desde su creación, sus resoluciones carecen de fuerza vinculante, siendo más bien un órgano de control político.

Sin embargo, merece especial atención el artículo 31 de la Ley Especial, ya que en él se establece que tanto el funcionamiento y seguridad del Centro de Intervenciones, como la selección y fiscalización permanente tanto del director, funcionarios, personal y miembros de la Policía Nacional Civil que elabore en el mismo, estará normado en un reglamento que para tal efecto deberá elaborar el Fiscal General de la República. En ese sentido, al no ser un ente diferente quien cree y regule el cumplimiento de dicho reglamento se abre la posibilidad de vulnerar derechos fundamentales, pues la Fiscalía es la parte acusadora en el proceso penal, por lo que tiene un interés particular en el mismo[81].

A continuación un flujograma de cómo se realiza la intervención de las telecomunicaciones y de quiénes ejercen la supervisión:



81 Verónica Beatriz Miranda Chicas et al., "El derecho a la intimidad, su limitabilidad y protección en el marco normativo de la ley especial para la intervención de las telecomunicaciones" (tesis de Licenciatura, Universidad de El Salvador, 2010).

2.4. Conclusiones preliminares

Los Acuerdos de Paz de 1992 fueron un parte aguas en la historia de represión y persecución política de El Salvador, provocando una serie de reformas jurídico-políticas para proteger la libertad de expresión, así como de organización y participación política. En ese sentido, luego de los Acuerdos de Paz el registro de denuncias sobre persecución de Defensores y Defensoras de Derechos Humanos en El Salvador de parte del Estado ha sido menos sistemático y no bajo las mismas modalidades del pasado.

Del marco jurídico examinado es importante remarcar que mayoritariamente tiende a brindar importantes garantías y protección a los derechos de intimidad, libertad de expresión y acceso a la información pública, al menos en lo que a su literalidad respecta, siendo una de las grandes deudas legislativas lo atinente a la protección de datos personales y la autodeterminación informativa. Sin embargo, en estas última áreas hay importante y reciente jurisprudencia constitucional emanada de recursos de amparo y *habeas corpus* que han servido para proteger estos derechos, incluso llegando a establecer al recurso de amparo como un recurso supletorio ante la ausencia de una regulación o legislación sobre *habeas data.*

Por otra parte, existe una importante deuda legislativa sobre nuevas tecnologías de la información y la comunicación, existiendo importantes vacíos en aspectos como firma electrónica[82], protección de datos personales, entre otros temas, lo cual coloca en indefensión a las personas que se encuentren expuestas a estas nuevas realidades.

Debe señalarse que la existencia de algún tipo de institucionalidad, como el Centro de Intervención de las Telecomunicaciones, creado por la Ley especial para la Intervención de las Telecomunicaciones, es a la vez un riesgo y una garantía. La posibilidad de que su funcionamiento se realice enmarcado en la ley y respetando los derechos fundamentales dependerá de la fortaleza e independencia con que funcione el resto de la institucionalidad de justicia y seguridad del país: Órgano Judicial, Policía Nacional Civil, Fiscalía General de la República, etc., así como también dependerá del juego gobierno-oposición que se genere entre los partidos políticos mayoritarios, los cuales deben tener la suficiente fuerza e institucionalización para poder contrarrestar las posibilidades de utilización de este tipo de instituciones y legislaciones con fines político-partidistas.

En ese sentido, la posibilidad de que el marco jurídico actual sea propicio o esté siendo utilizado para el control, vigilancia o persecución de defensores y defensoras de derechos humanos debe ser

82 Un decreto legislativo sobre Firma Electrónica fue aprobado en la Asamblea Legislativa (06/10/15) posteriormente a la elaboración de este capítulo. Por el momento, el decreto legislativo se encuentra en manos del presidente de la República, para su sanción y aprobación, o su veto por inconsitucionalidad o inconveniencia.

examinado desde el nuevo contexto político social, marcado por la violencia y criminalidad, que está abriendo camino a una serie de reformas, legislaciones y prácticas policiales que restringen derechos humanos fundamentales, y que podrían convertirse en un franco retroceso jurídico y político con respecto a lo avanzado luego de 1992.

Marco legal nacional y su adecuación a los estándares internacionales

El Estado y la sociedad salvadoreña, como muchas sociedades en el mundo, han adoptado las nuevas tecnologías de la comunicación con muchísima mayor velocidad que la construcción de marcos legales que garanticen que las nuevas realidades que estas construyen no terminen minando ni conculcando derechos fundamentales como la privacidad y la libertad de expresión. En ese sentido, en el presente capítulo evaluaremos si la normativa interna relacionada con la vigilancia de las comunicaciones se adhieren a los estándares internacionales de derechos humanos[83]. Para ello, utilizaremos los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones,[84] en adelante los 13 Principios, como guía para evaluar si la normativa de vigilancia en El Salvador se realiza en el marco de respeto de los derechos humanos[85].

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. Estos están firmemente enraizados en el derecho internacional de los derechos humanos y la jurisprudencia comparada. Estos Principios han sido citados en el informe del Grupo de Revisión del Presidente sobre Inteligencia y Tecnologías de las Comunicaciones de los Estados Unidos[86], el informe de la Comisión Interamericana de Derechos Humanos[87], el reporte sobre anonimato y cifrado del Relator de Libertad de Expresión de Naciones Unidas[88], el reporte de privacidad en la era digital del Alto Comisionado de Derechos Humanos de Naciones Unidas[89], entre otros. Al ser ello así, tanto los tratados y decisiones judiciales que interpretan los 13 Principios son aplicables a El Salvador, y los 13 Principios constituyen una fuente de doctrina relevante para analizar las prácticas de vigilancia a nivel nacional.

A continuación examinaremos los estándares frente a la normativa interna de El Salvador:

83 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Accesibles en: https://es.necessaryandproportionate.org/text

84 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Accesibles en: https://es.necessaryandproportionate.org/text

85 Para una descripción de cada uno de los principios y su fundamento como instrumento del derecho internacional de derechos humanos, ver pág XX

86 Sobre el Grupo de Revisión sobre Inteligencia y Tecnologías de Comunicación, puede accederse a más información en: http://www.cnnexpansion.com/economia/2013/08/12/eu-crea-supervisor-de-espionaje

87 Puede acceder al Informe de la Comisión Interamericana de Derechos Humanos en: http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf

88 Puede acceder al Reporte sobre Anonimato y Cifrado del Relator de Libertad de Expresión de Naciones Unidas en: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

89 Puede acceder al reporte sobre privacidad en la era digital del Alto Comisionado de Derechos Humanos de Naciones Unidas en: http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

3.1. Legalidad

Legalidad: Cualquier limitación a los derechos humanos debe ser prescrita por ley. El Estado no debe adoptar o implementar una medida que interfiera con los derechos a la privacidad en ausencia de una ley públicamente disponible, que cumpla con un estándar de claridad y precisión suficientes para asegurar que las personas la conozcan por adelantado y puedan prever su aplicación.

El artículo 24 de la Constitución de la República, que establece que la correspondencia de toda clase es inviolable, se reformó en 2010 a fin de permitir excepcionalmente la intervención temporal de las telecomunicaciones, previa autorización judicial motivada para la investigación de los delitos que una ley especial determine. La mencionada reforma constitucional obliga a adoptar una ley especial que desarrolle sus contenidos, con regulaciones que equilibren el respeto del derecho al secreto de las comunicaciones con eficacia en la investigación del delito. La reforma constitucional estableció que dicha ley especial, además, debía ser aprobada por una mayoría calificada de los diputados (56 votos), lo cual es inusual ya que ordinariamente las leyes se aprueban con mayoría simple (43 votos) [90].

Dicha reforma al artículo 24 de la Constitución establece que una ley especial determinará los delitos en cuya investigación podrá concederse la autorización para la intervención de las telecomunicaciones. Asimismo, establece que dicha ley deberá señalar los controles, los informes periódicos a la Asamblea Legislativa, y las responsabilidades y sanciones administrativas, civiles y penales en que incurrirán los funcionarios que apliquen ilegalmente esta medida excepcional[91].

La Constitución establece que el Estado solo puede restringir este derecho cuando se encuentre en peligro el goce de derechos fundamentales de terceros o se esté en el marco de una investigación judicial debido al posible cometimiento de ciertos delitos. La intervención en las telecomunicaciones, según la Constitución, solo es potestad del Estado, excepcionalmente y previa autorización judicial. Ello puede hacerse siempre que exista la sospecha fundada del cometimiento de uno de los delitos expresamente regulados en la que ahora se denomina Ley Especial para la Intervención de las Telecomunicaciones (LEIT)[92].

La LEIT establece que solo podrán intervenirse las comunicaciones mediante autorización judicial, aunque de manera excepcional, cuando se tenga sospecha fundamentada de la comisión de ciertos delitos[93]. El artículo 5 de la referida ley regula de manera taxativa los 16 delitos en los cuales se podrá hacer uso de la facultad de intervención:

90 El Salvador "Constitución de la República": Asamblea Legislativa (1983), artículo 24.
91 El Salvador "Constitución de la República", artículo 24.
92 La Ley fue creada mediante Decreto Legislativo Nº 285 de fecha 18 de febrero de 2010, publicado en el Diario Oficial Nº51, Tomo Nº386 , de fecha 15 de marzo del año 2010.
93 El Salvador "Ley Especial para la Intervención de las Telecomunicaciones" Asamblea Legislativa (2010), artículo 1.

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.

A pesar que los delitos que pueden ser investigados a través de la intervención de las telecomunicaciones se encuentran taxativamente contemplados en la LEIT, también es cierto que la misma abre la posibilidad de ampliarlos cuando se decrete un régimen de excepción[94] que suspenda la garantía del artículo 24 de la Constitución de la República. El decreto legislativo que declare el estado de excepción podría ampliar los delitos a los cuales se podrá aplicar la intervención de las telecomunicaciones, aunque se continuaría respetando la garantía de autorización judicial previa y el procedimiento establecido por la LEIT (Art. 49 LEIT).

Por otra parte, la Ley Especial contra el Delito de Extorsión[95] en su artículo 8, referido a las técnicas de investigación y aspectos probatorios, establece que solo se podrá utilizar la grabación de llamadas telefónicas de uno de los interlocutores, así como cualquier otro medio tecnológico que les lleve al convencimiento de la existencia del delito y la participación delictiva, de conformidad con al artículo 46 de LEIT. El artículo 10 regula que se podrá obtener o almacenar información electrónica contenida en algún dispositivo electrónico cuando se tenga sospecha que se está cometiendo un delito, previa autorización de un juez.

Además, la Ley Orgánica de la Policía Nacional Civil[96] en su artículo 25, numeral 7 establece que, en general, no se podrán intervenir las comunicaciones telefónicas, salvo en los casos previamente establecidos y bajo el procedimiento estipulado para su autorización conforme lo establece la Constitución en el artículo 24.

Por otra parte, según el criterio de la Sala de lo Constitucional, el derecho a la autodeterminación

94 El régimen de excepción se encuentra contemplado en la Constitución de la República del artículo 29 al 31, y establece que en casos de guerra, invasión del territorio, rebelión, sedición, catástrofe, epidemia u otra calamidad general, o de graves perturbaciones del orden público, podrán suspenderse las garantías establecidas en los artículos 5, 6 inciso primero, 7 inciso primero y 24 de esta Constitución (que establece la inviolabilidad de la comunicación y sus excepciones). Tal suspensión podrá afectar la totalidad o parte del territorio de la República, y se hará por medio de decreto del Órgano Legislativo o del Órgano Ejecutivo. El plazo de suspensión de las garantías constitucionales no excederá de 30 días. Transcurrido este plazo podrá prolongarse la suspensión, por igual período y mediante nuevo decreto, si continúan las circunstancias que la motivaron. Si no se emite tal decreto, quedarán establecidas de pleno derecho las garantías suspendidas. Cuando desaparezcan las circunstancias que motivaron la suspensión de las garantías constitucionales, la Asamblea Legislativa o el Consejo de Ministros, según el caso, deberá restablecer tales garantías.

95 El Salvador "Ley Especial contra el Delito de Extorsión" Asamblea Legislativa (2015), artículos 8,10, y 12.

96 El Salvador "Ley Orgánica de la Policía Nacional Civil" Asamblea Legislativa (2001), artículo 27 No. 7.

informativa splo puede verse restringido "por la finalidad que persigue la recolección y administración de los datos personales, la cual debe ser legítima (constitucional o legal), explícita y determinada"[97].

Así también, según el artículo 6 de la Constitución, la libertad de expresión solo podrá verse limitada por razones de subversión del orden público, lesión a la moral y a la vida privada de las personas. Todos ellos conceptos muy amplios, por lo que su definición puede llegar a generar cierto margen a la arbitrariedad en su aplicación. El artículo 29 de la Constitución regula el régimen de excepción, contexto en el que establece la posibilidad de suspender el derecho a la libertad de expresión. Los artículos 82 y 97 establecen restricciones para los agentes de la Policía Nacional Civil, los miembros de la Fuerza Armada y los Ministros de cultos religiosos, a quienes les está prohibida la propaganda política.

Finalmente, el principio de legalidad implica la publicidad de toda norma legal. En tal sentido, tanto la normativa interna como los estándares internacionales de derechos humanos establecen que las leyes, reglamentos, decretos y demás disposiciones de carácter general solo tendrán fuerza obligatoria en virtud de su promulgación y publicación. Sin embargo, a pesar que el artículo 31 de la LEIT establece que esta contará con un reglamento que deberá elaborar el Fiscal General de la República, este reglamento no es público, pues la FGR ha clasificado esta normativa como información reservada. Los motivos y contradicciones legales de la no publicidad de este reglamento será más ampliamente desarrollado en el Principio de Transparencia, sin embargo es preciso acotar que contradice el Principio de Legalidad y Transparencia conforme lo establece los estándares internacionales de derechos humanos.

3.2. Objetivo legítimo

Este principio establece que las leyes únicamente deberían permitir la vigilancia de las comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática[98].

En ese sentido, la exposición de motivos de la LEIT considera que la intervención de las telecomunicaciones planteada en dicha

> Las leyes solo deberían permitir la vigilancia de las comunicaciones por parte de autoridades estatales específicas para alcanzar un objetivo legítimo que corresponda a un interés jurídico preponderante e importante y que sea necesario en una sociedad democrática. Cualquier medida no debe aplicarse de manera que discrimine con base en raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

97 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 142-2012.
98 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Accesible en: https://es.necessaryandproportionate.org/text

normativa es un instrumento o herramienta de persecución penal que busca mejorar la eficacia en la lucha contra la delincuencia grave, organizada y transnacional. Asimismo, sostiene que la posibilidad de intervenir las telecomunicaciones debe considerarse como limitación legítima, que por tanto debe cumplir con los criterios de necesidad, proporcionalidad y razonabilidad del derecho constitucional al secreto de las comunicaciones, en el marco del derecho fundamental a la intimidad.

Según los legisladores, la intervención de las telecomunicaciones constituye un instrumento útil en la persecución del delito, en particular la criminalidad organizada, pero su utilización debe estar resguardada por garantías que eviten abusos contra la intimidad de las personas[99].

3.3. Necesidad

Según este principio, las leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo[100]. En ese sentido, de acuerdo al principio de proporcionalidad establecido en la LEIT (Art. 2), solo deberá recurrirse a la intervención de las telecomunicaciones cuando se justifique suficientemente la necesidad de la medida, siempre que no existan otras formas menos gravosas a las cuales recurrir para la averiguación de los delitos previstos en la ley.

El juez autorizante fijará las condiciones y plazo en que debe realizarse la intervención, indicando las personas afectadas, los datos del servicio de telecomunicación a ser intervenido y su fecha de finalización, así como los períodos en los cuales será informado por el fiscal del desarrollo de la investigación. Solo podrán autorizarse nuevos plazos para la intervención si se presenta una nueva solicitud del fiscal con todos los requisitos previstos para la primera petición y con justificación suficiente de la necesidad de la prórroga.

Leyes de vigilancia, reglamentos, actividades, poderes o autoridades deben limitarse a lo que es estricta y evidentemente necesario para alcanzar un objetivo legítimo. La vigilancia de las comunicaciones solo debe llevarse a cabo cuando es el único medio para alcanzar un objetivo legítimo, o bien cuando habiendo varios medios sea el menos propenso a vulnerar los derechos humanos. La carga de establecer esta justificación, tanto en los procesos judiciales como en los legislativos, recae en el Estado.

99 El Salvador "Ley Especial para la Intervención de las Telecomunicaciones" Asamblea Legislativa (2010).
100 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Accesible en: https://es.necessaryandproportionate.org/text

3.4. Idoneidad

En consonancia con el Principio de Idoneidad, la LEIT establece que en caso de duda sobre el sentido de dicha normativa, sus disposiciones deben ser interpretadas en el sentido más favorable a la protección de los derechos a la vida privada, la intimidad personal y el secreto de las telecomunicaciones. Por lo que las disposiciones legales que limiten estos derechos serán interpretadas restrictivamente (Art. 3).

Cualquier medida de vigilancia de las comunicaciones autorizado mediante ley debe ser apropiado para cumplir el objetivo legítimo específico identificado.

3.5. Proporcionalidad

La intervención de las telecomunicaciones tendrá carácter excepcional y únicamente podrá recurrirse a ella cuando resulte útil para una investigación penal y se justifique suficientemente la necesidad de la medida, siempre que no existan otras formas menos gravosas a las cuales recurrir para la averiguación de los delitos previstos en la ey Especial para la Intervención de las Telecomunicaciones[101].

Las medidas de vigilancia solo deben autorizarse por una autoridad judicial independiente cuando exista un alto grado de probabilidad de que un delito grave o una amenaza específica, actual y comprobable a la seguridad nacional pueda materializarse.

Así también deberá cumplir con el principio de temporalidad, según el cual la intervención se mantendrá durante el tiempo autorizado por el juez. Además, la intervención debe recaer únicamente sobre las telecomunicaciones y medios de soporte de las personas presuntamente implicadas en el delito, ya sean sus titulares o usuarios habituales o eventuales, directa o indirectamente, incluidas las telecomunicaciones por interconexión. La ley especial también establece que la intervención podrá recaer sobre aparatos de telecomunicaciones y otros medios de soporte abiertos al público.

Con respecto a la recolección de datos e información personal, la Sala de lo Constitucional establece que esta solo será legítima cuando cumpla no solamente con el principio de proporcionalidad y legalidad, sino que también establece que el legislador debe tener en cuenta, al momento de legislar en este aspecto, el derecho general del ciudadano a la libertad frente al Estado, la cual únicamente puede ser restringida por el poder público cuando sea indispensable para la protección del interés general[102].

101 El Salvador "Ley Especial para la Intervención de las Telecomunicaciones", artículo 2.
102 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 142-2012.

3.6. Autoridad judicial competente

Entre los principios que la Ley Especial para la Intervención de las Telecomunicaciones establece para su aplicación se encuentra el de Jurisdiccionalidad, según el cual solo podrán intervenirse las telecomunicaciones previa autorización judicial, escrita y debidamente motivada. Según la misma ley, la intervención de las telecomunicaciones exclusivamente podrá ser autorizada por los jueces de instrucción con residencia en San Salvador[103].

Las medidas de vigilancia de comunicaciones deben ser autorizadas de manera previa, o inmediata con efecto retroactivo en casos de emergencia, por una autoridad judicial competente, independiente e imparcial.

Los delitos que pueden ser investigados a través de la intervención de las telecomunicaciones se encuentran taxativamente contemplados en la LEIT, sin embargo la misma ley deja abierta la posibilidad de ampliarlos cuando se decrete un régimen de excepción. Dicho régimen consiste en la suspensión de las garantías del artículo 24 de la Constitución de la República, por lo que el decreto legislativo que lo declare podrá ampliar los delitos a los que se podrá aplicar la intervención de las telecomunicaciones, pero deberá seguirse respetando la garantía de autorización judicial previa y el procedimiento establecido por la LEIT (Art. 49).

3.7. Debido proceso

La legislación salvadoreña determina los límites al ejercicio absoluto del derecho a la intimidad y establece expresamente situaciones en las cuales el Estado tiene la potestad de intervenir. De manera más específica, el Código Procesal Penal (CPP) establece que cuando se requiera intervenir las telecomunicaciones de una persona que está siendo investigada o procesada, deberán cumplirse las respectivas garantías constitucionales y legales del debido proceso para que esta información pueda ser incorporada en un proceso judicial y constituyan prueba (Art. 176)[104].

Las decisiones de autorización de medidas de vigilancia de comunicaciones deben garantizar el debido proceso. Lo anterior implica que, cuando para la consecución del objetivo legítimo, y en particular la protección de la vida de una persona, sea necesaria la secrecía de la medida o su aplicación inmediata, existan otras medidas que garanticen la protección de los intereses del afectado como la designación de una persona o institución que asuma representación general de sus intereses en la audiencia o que la autorización judicial se lleve a cabo con efecto retroactivo.

En complemento, según el artículo 1 de la LEIT, la información proveniente de una intervención ilegal que no cumpla con el debido proceso, carecerá de valor probatorio.

103 El Salvador "Ley Especial para la Intervención de las Telecomunicaciones", artículos 2 y 8.
104 El Salvador "Código Procesal Penal" Asamblea Legislativa (2009), artículo 176.

3.8. Notificación del usuario

Cuando se trata de una intervención en la comunicación de las personas ninguna disposición de la LEIT establece la posibilidad de notificar al usuario de la intervención mientras esta se encuentre realizando. Sin embargo, el artículo 25 de la misma ley contempla que una vez entregado el expediente de la intervención al juez competente, el mismo deberá ser público excepto que resulten aplicables las reglas generales de reserva del proceso penal. Esta disposición hace hincapié en que -en todo caso- las partes mantendrán estricto secreto sobre el contenido del material que no interesa a la investigación.

> Las personas afectadas por medidas de vigilancia de comunicaciones deben ser notificadas de ello y tener acceso a las materiales que pretendan ser o hayan sido obtenidos. La notificación podrá diferirse cuando la misma ponga en riesgo la consecución del objetivo legítimo o exista un riesgo inminente de peligro a la vida humana.

Por otra parte, una vez incorporado al proceso penal el expediente judicial de la intervención, la defensa tendrá acceso completo e irrestricto al mismo (Art. 26 LEIT).

3.9. Transparencia

El artículo 10 de la Ley de Acceso a la Información Pública (LAIP) establece que se considera como información pública las estadísticas que generen todos los entes obligados, dentro de los cuales se encuentra la Fiscalía General de la República (FGR), que es responsable del Centro de Intervención de las Telecomunicaciones. En ese sentido, de acuerdo con la LAIP, se considera información pública el número de intervenciones a las telecomunicaciones que se han realizado en cierto período de tiempo, siempre y cuando no se revele otra información considerada como confidencial.

> El Estado debe publicar de manera periódica información estadística sobre las medidas de vigilancia encubierta llevadas a cabo. Como mínimo debe publicar el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad, tipo y propósito.

Esta disposición de la LAIP no riñe con el principio de reserva y confidencialidad de la Ley Especial para la Intervención de las Telecomunicaciones (art. 2), que establece que el procedimiento de intervención de las telecomunicaciones será reservado y la información privada ajena a la investigación será estrictamente confidencial, pues de acuerdo con la LAIP lo único que deberá ser público son las estadísticas anuales, sin mencionar las partes involucradas ni cualquier otro pormenor que ponga en riesgo la investigación. Sin embargo, la Fiscalía aún no rinde anualmente el informe global sobre el número de solicitudes de intervención aprobadas y rechazadas, ni el número específico de personas intervenidas.

Por otra parte, según el artículo 31 de la LEIT, el funcionamiento y seguridad del Centro de Intervenciones a las Telecomunicación, así como la selección y fiscalización permanente tanto del director como funcionarios, personal y miembros de la Policía Nacional Civil que labore en el mismo, estará normado en un reglamento que para tal efecto deberá elaborar el Fiscal General. Sin embargo, este reglamento no es público, pues según el criterio de la Unidad de Acceso a la Información Pública (UAIP) de la Fiscalía esta normativa se encuentra clasificada como información reservada[105].

Este criterio de la FGR contradice directamente el principio de publicidad de la ley establecido en el artículo 6 del Código Civil, que establece que las leyes, reglamentos, decretos y demás disposiciones de carácter general solo tendrán fuerza obligatoria en virtud de su solemne promulgación y después de transcurrido el tiempo necesario para que se tenga noticia de ella[106]. Contradice también lo establecido en el artículo 10, numeral 1 de la LAIP, que establece como información oficiosa, es decir que debe ser pública siempre, la normativa aplicable a cada ente obligado. De igual manera, de acuerdo con los estándares internacionales, una norma secreta no califica como norma pues viola el principio de legalidad.

En ese sentido, la no publicidad de este reglamento no solo se convierte en una afrenta a los principios internacionales de transparencia y legalidad, sino que también coloca en una situación de indefensión a quienes hayan sido sometidos a una investigación en la que se autoriza la intervención de sus comunicaciones.

3.10. Supervisión pública

La entidad que realiza las intervenciones legales de las telecomunicaciones es el Centro de Intervención de las Telecomunicaciones, el cual depende de la Fiscalía General de la República (FGR). Las intervenciones se harán en colaboración con la Policía Nacional Civil, previa autorización y control de un juez de instrucción, el cual deberá garantizar que la intervención se desarrolla de conformidad con las condiciones establecidas en su resolución.

Deben establecerse mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones.

Por su parte, el Procurador para la Defensa de los Derechos Humanos (PDDH), en conjunto con el Fiscal General de la República, se encuentra facultado legalmente para elaborar el Protocolo de Funcionamiento del Centro de Intervención en cuanto a la fiscalización periódica y auditoría del mismo, según lo establece la Ley Especial para la Intervención de Telecomunicaciones. El Procurador

105 Resolución 128-UAIP-FGR-2015 a Solicitud de Acceso a la Información presentada por el investigador el 24 de julio de 2015.
106 Su publicación deberá hacerse en el periódico oficial.

también tiene la facultad de practicar anualmente una auditoría a las actividades del Centro y remitir el informe respectivo a la Comisión de Legislación y Puntos Constitucionales de la Asamblea Legislativa. La ley también lo faculta para realizar las auditorías específicas que estime convenientes sobre la violación del derecho a la intimidad o secreto de las telecomunicaciones. Dichas auditorías específicas se anexarán al informe general que se enviará a la Comisión Legislativa (Arts. 26, 33).

La PDDH será el principal órgano de supervisión en el proceso de intervención de las telecomunicaciones. Es importante señalar que la PDDH es una institución independiente que surge como resultado de los Acuerdos de Paz en 1992. El Procurador para la Defensa de los Derechos Humanos es un funcionario de elección secundaria, a través de la Asamblea Legislativa, que tiene el mismo nivel político de la Fiscalía General de la República, siendo ambas instituciones parte de lo que la Constitución reconoce como Ministerio Público. Sin embargo, y a pesar del rol protagónico de la PDDH desde su creación, sus resoluciones carecen de fuerza vinculante, siendo más bien un órgano de control político.

Sin embargo, merece especial atención el artículo 31 de la Ley Especial, ya que en él se establece que tanto el funcionamiento y seguridad del Centro de Intervenciones, como la selección y fiscalización permanente tanto del Director como funcionarios, personal y miembros de la Policía Nacional Civil que labore en el mismo, estará normado en un reglamento que para tal efecto deberá elaborar el Fiscal General de la República. En ese sentido, al no ser un ente diferente quien cree y regule el cumplimiento de dicho reglamento se abre la posibilidad de vulnerar derechos fundamentales, pues la Fiscalía es la parte acusadora en el proceso penal, por lo que tiene un interés particular en el mismo[107].

La Constitución en su artículo 24, establece que la Ley Especial para la Intervención de las Telecomunicaciones requerirá el voto favorable de por lo menos las dos terceras partes de los diputados electos para ser aprobada o reformada dando así un extra de seguridad política, pues la totalidad de leyes en el país solo necesitan la mayoría simple.

3.11. Integridad de las comunicaciones y sistemas

Según la Ley de Telecomunicaciones, en sus artículos 42B y 42C, los operadores de redes comerciales de telecomunicaciones deberán brindar información relativa al origen, dirección, destino o terminación de la marcación o recepción de llamadas telefónicas de los números de sus usuarios que se encuentren bajo investigación, que se hayan generado o recibido por medio de equipo, facilidades o servicios de telecomunicación del operador de telefonía. Los operadores de redes comerciales de telecomunicaciones deberán poner a disposición de las autoridades correspondientes las bases

107 Verónica Beatriz Miranda Chicas et al., "El derecho a la intimidad, su limitabilidad y protección en el marco normativo de la ley especial para la intervención de las telecomunicaciones" (tesis de Licenciatura, Universidad de El Salvador, 2010).

de datos que contengan la información antes mencionada.

> No debe obligarse a proveedores de servicios o desarrolladores de "hardware" o "software" a desarrollar capacidades de vigilancia que comprometan la seguridad de las comunicaciones y los dispositivos. No debe exigirse la retención indiscriminada y masiva de datos de las personas que usan dichos servicios ni debe comprometerse el derecho a la expresión anónima a través del establecimiento de obligaciones de identificación o prohibiciones respecto del uso de herramientas de cifrado y otras para proteger la identidad y la seguridad de las personas, sus comunicaciones y sus dispositivos.

Además, el artículo 30A de la misma ley establece que es obligación de los operadores de servicios de acceso llevar un registro de todos los usuarios -incluyendo los de pago previo-, debiendo mantener dicha información a disposición de la FGR, sin establecer el tiempo durante el cual deberá mantener dichos registros. Según el artículo 34 de la misma ley, las empresas operadoras cometerán una infracción muy grave[108] cuando nieguen la información que les requiera la Superintendencia General de Electricidad y Telecomunicaciones (SIGET)[109], especialmente aquella información relacionada con sus usuarios.

En ese sentido, las anteriores disposiciones entran en conflicto con lo establecido en este principio, sobre la no exigibilidad de retención o recopilación de datos a los proveedores de servicios o proveedores por parte del Estado.

3.12. Garantías contra el acceso ilegítimo y derecho a recurso efectivo

> La vigilancia ilegal de comunicaciones debe ser castigada mediante sanciones civiles y penales suficientes y adecuadas. Los *whistleblowers* de interés público deben ser protegidos por la ley de cualquier repercusión legal por el incumplimiento de su deber de secretividad.

El Código Penal tipifica algunas conductas que atentan contra el derecho a la intimidad e intercepción de las comunicaciones, constituyéndose estos delitos en cierto tipo de protección que pueda ser utilizada en caso de algún tipo de acceso ilegítimo. Entre estos tipos penales se encuentran la violación de comunicaciones privadas (Art. 184); violación agravada de comunicaciones (Art. 185); captación de comunicaciones (Art. 186); revelación del secreto profesional (Art. 187); y, utilización de la imagen o nombre de otro (Art. 190). El mismo código también establece responsabilidad penal cuando en el ejercicio de la libertad de expresión se cometen abusos. El Código

108 Dicha infracción será sancionada con una multa de 45 mil a 57 mil dólares estadounidenses, además de una multa de 561 dólares estadounidenses por cada día en que la infracción continúe.

109 La Superintendencia General de Electricidad y Telecomunicaciones (SIGET), es la entidad responsable de aplicar y velar por el cumplimiento de las normas y regulaciones establecidas en la Ley de Telecomunicaciones.

Penal tipifica los delitos de calumnia (Art. 177), difamación (Art. 178) e injuria (Art. 179), entre otros.

Por otra parte, la jurisprudencia constitucional ha constituido al recurso de Amparo como la garantía para la protección de los derechos fundamentales en general, y por lo tanto, del derecho a la intimidad[110], pues como se mencionó anteriormente, en el ordenamiento jurídico salvadoreño aún no es reconocida la garantía del *habeas data* como instrumento diseñado para la protección específica del derecho a la autodeterminación informativa.

Sin embargo, la Sala de lo Constitucional reconoció que la protección al derecho a la autodeterminación informativa es factible a través del proceso constitucional de amparo, sin importar la naturaleza del ente a quien se le atribuya su vulneración[111]. La Sala reafirmó que el ámbito de protección del derecho a la autodeterminación informativa implica diferentes facultades a favor de la persona, las cuales se reconocen para "controlar el uso de la información personal que le atañe, tanto en su recolección como en su tratamiento, conservación y transmisión"[112].

3.13. Conclusiones preliminares

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.

Por otra parte, como hemos señalado en capítulos anteriores, 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 LEIT, 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.

A pesar de contar con importantes leyes a favor de la transparencia como la 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

110 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 135 – 2005/32 – 2007 del 16 de mayo de 2008.
111 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 934-2007 del 4 de marzo de 2011, parte III 1. B. a.
112 Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Inconstitucional 58-2007 del 8 de marzo de 2013.

principios internacionales de legalidad y transparencia, sino también a las garantías constitucionales en la formación de ley según la Constitución de la República.

En resumen, más importante aún que la carencia o deficiencia del marco legal, sería la cultura de opacidad y arbitrariedad en las élites políticas del país que es acompañado con el respectivo elemento de debilidad institucional, que permite que algunos funcionarios de turno puedan utilizar, ya sea omitiendo la ley o retorciéndola, mecanismos para la vigilancia de opositores, personas defensoras de derechos humanos y cualquiera que pueda ser incómodo para su gestión. Ante ello, la ciudadanía si bien tiene armas legales para enfrentarlos, se enfrenta con una institucionalidad débil, con dificultad para hacer valer esas garantías.

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

El objetivo de este capítulo es presentar 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 El Salvador, que surgieron de entrevistas a profundidad y de un grupo focal realizado con personas comprometidas con la defensa de los derechos humanos.

El presente se subdivide de la siguiente manera: una reseña sobre los aspectos metodológicos utilizados para luego dar paso a las experiencias de defensores (as) y técnicos (as) relacionadas con vigilancia, anonimato, cifrado, allanamientos y requisas, entre otros. Finalmente, cierra con un sub-acápite que contiene las principales dudas manifestadas por las y los entrevistados sobre el marco legal existente en el país con respecto a anonimato, cifrado, allanamientos, requisas y cualquier otro tipo de legislación relacionada con vigilancia de las telecomunicaciones y/o que pudiera estar encaminado a criminalizar la labor de defensores y técnicos.

4.1. Reseña metodológica

La metodología utilizada fue de carácter cualitativo a través de herramientas como la entrevista a profundidad, de tipo semi-estructurado, y la realización de un grupo focal con expertos con el objetivo de obtener las percepciones, experiencias, dudas y observaciones sobre el marco legal de defensores y defensores de derechos humanos, así como de técnicos y técnicas involucrados en la defensa de derechos humanos o que trabajen para organizaciones y/o personas defensoras de derechos humanos en El Salvador.

En tal sentido, se realizaron cinco entrevistas a personas defensoras de derechos humanos (tres mujeres y dos hombres), vinculados a distintas áreas de defensa de los derechos humanos: víctimas de crímenes de lesa humanidad, derechos LGBTI, derechos de la mujer, y derechos de jóvenes en riesgo y en conflicto con la ley. Se realizaron tres entrevistas a técnicos, todos hombres, siendo importante mencionar que se tuvo cierto nivel de dificultad para encontrar el perfil adecuado de las y los técnicos, pues no solo se buscaba su conocimiento y capacidad técnica en las áreas de telecomunicaciones e internet, sino también su compromiso por la defensa de derechos humanos y/o trabajo con organizaciones defensoras de derechos humanos.

Se realizó además un grupo focal con técnicos, para el cual se logró acceder a nuevos técnicos que cumplían con el perfil antes mencionado, haciendo un total de 5 especialistas dentro de los cuales una era una abogada defensora de derechos humanos con previa formación en privacidad en las telecomunicaciones e internet. El resto eran técnicos en áreas de comunicación e internet, todos hombres.

Previo a las entrevistas a profundidad se realizaron otras de tipo exploratorio, con el objetivo de profundizar sobre el marco legislativo nacional de internet y telecomunicaciones, así como para conocer el panorama nacional en cuanto a desarrollo tecnológico y producción académica sobre privacidad en las telecomunicaciones e internet. En tal sentido, se entrevistó a un ex asesor legislativo que estuvo a cargo de desarrollar y analizar proyectos de ley sobre delitos informáticos y firma electrónica, entre otros. Así también, se entrevistó a dos técnicos, un ingeniero informático y un ingeniero experto en informática forense, los cuales se desempeñan en el sector de educación superior.

Es importante mencionar que las experiencias, opiniones y dudas a continuación presentadas surgen de personas que trabajan en la defensa de derechos humanos, lo cual los convierte en actores válidos para hablar sobre sus experiencias en cuanto a vigilancia y criminalización por medio del 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.

4.2 Experiencias (hallazgos y casos paradigmáticos)

4.2.1. Vigilancia

Tanto defensores y defensoras como técnicos que fueron entrevistados manifiestan que las intervenciones telefónicas hacia opositores políticos y defensores de derechos humanos vienen dándose desde el conflicto armado en el país. Las y los entrevistados mencionaron con bastante frecuencia algunos elementos que les llevan a sospechar que están siendo o han sido intervenidos telefónicamente, entre los cuales destacan: el eco que se escucha durante sus llamadas telefónicas, las llamadas son cortadas cuando se usan ciertas palabras o términos, se escuchan otras voces durante las llamadas, en los teléfonos móviles se da una especie de sobrecalentamiento del aparato, entre otros que mencionaron. Por otra parte, también manifiestan haber tenido experiencias como *hackeos* e intentos de *hackeo* de sus cuentas de correo y redes sociales, así como del *hackeo* y/o clonación de las páginas web institucionales a través del envío de solicitudes masivas.

Entre los entes que los y las entrevistadas identifican como las posibles entidades vigilantes se mencionan a la Presidencia de la República a través del Organismo de Inteligencia del Estado y de la Secretaría de Participación Ciudadana, Transparencia y Anticorrupción; la Fiscalía General de la República; las empresas telefónicas, así como ciertos equipos de personas ligadas a los partidos mayoritarios (ARENA y FMLN), y la Embajada de los Estados Unidos de América en San Salvador.

Es importante mencionar que según las y los técnicos que participaron en el grupo focal, existen suficientes indicios para sostener que muy probablemente existe vigilancia de parte del Estado y de entes paraestatales a defensores y defensoras de derechos humanos, y opositores políticos. A continuación, algunas de sus experiencias:

> En varias ocasiones y organizaciones detectamos software de escaneo a nuestros servidores […] Detectamos y prevenimos ataques de negación de servicios, de inyección XSL y SQL. Logramos en algunos casos rastrear las IP y conocer el lugar desde donde se realizaban. Encontramos también de dónde se originó una campaña de ataques y era desde una empresa del país. De todo lo anterior tengo pruebas. Técnico 3[113]

> He detectado malware [y] spyware pero siempre han sido de agentes externos […] Estos software al final son fácilmente eliminados […] he llegado a tener sospecha de infiltración en la red pero conectados a la red inalámbrica, pero como menciono sólo ha sido sospecha, los cuales pudieron ocupar técnicas de ingeniería social para obtener contraseña de redes wifi. Técnico 2[114]

> Mi celular y el de mi Directora estaban siendo intervenidos pues las llamadas se cortaban, escuchábamos ecos y hasta se apagaban los teléfonos. Tuvimos que cambiar línea y compañía [telefónica], y salir del país. Técnico 3[115]

> Tuve conocimiento de la existencia de áreas restringidas en la antigua Administración Nacional de Telecomunicaciones (ANTEL)[116], dónde sólo ingresaba personal especializado y personal militar. Técnico 1[117]

Las y los entrevistados manifiestan que la preocupación por la 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. A pesar de ello, en las y los entrevistados predomina aún más el temor y la preocupación por los ataques y atentados

113 Respuesta de Técnico 3 en Grupo Focal con Técnicos Informáticos que trabajan en el ámbito de la defensa de Derechos Humanos. San Salvador, El Salvador. 28 de agosto de 2015.
114 Respuesta de Técnico 2 en Grupo Focal con Técnicos Informáticos que trabajan en el ámbito de la defensa de Derechos Humanos. San Salvador, El Salvador. 28 de agosto de 2015.
115 Respuesta de Técnico 3 en Grupo Focal con Técnicos Informáticos que trabajan en el ámbito de la defensa de Derechos Humanos. San Salvador, El Salvador. 28 de agosto de 2015.
116 Institución estatal existente antes de la privatización de las telecomunicaciones en 1996.
117 Respuesta de Técnico 1 en Grupo Focal con Técnicos Informáticos que trabajan en el ámbito de la defensa de Derechos Humanos. San Salvador, El Salvador. 28 de agosto de 2015.

físicos que puedan sufrir debido a la situación de inseguridad que los ataques a la privacidad de sus telecomunicaciones.

4.2.2. Anonimato y cifrado

No hubo mayores hallazgos en cuanto anonimato y cifrado, más bien escasas dudas respecto a su posibilidad legal. En tal sentido, es importante mencionar que las y los entrevistados se encuentran en un momento en el que comienzan a tomar mayor conciencia de la importancia de su privacidad en las telecomunicaciones y de los riesgos que implica no estar preparados ni como individuos ni como organizaciones en este sentido. Muy probablemente esta sea una de las explicaciones sobre la poca información recibida cuando se les preguntó sobre anonimato y cifrado, ya que en la mayoría de los casos no son recursos utilizados –o muy poco utilizados- ni individualmente ni como organizaciones.

4.2.3. Allanamientos y requisas

Al menos dos de las organizaciones en las que trabajan las personas defensoras de derechos humanos entrevistadas han sufrido allanamientos ilegales por desconocidos durante el contexto de ciertos casos simbólicos y con cierta relevancia mediática que ellos llevaron. En dichos allanamientos se sustrajeron computadoras, con la particularidad de sustraer aquellas laptops o computadoras de escritorio que tenían la información precisamente de esos casos emblemáticos que se encontraban en curso.

También se mencionaron los casos de organizaciones que sufrieron allanamientos ilegales con la clara intención de desaparecer información. Uno de los casos incluso llegó a los medios de comunicación, sin embargo continúa con poca claridad cuál era el objetivo de sustraer y destruir la información, existiendo varias posibilidades que aún no han sido esclarecidas[118].

Por otra parte, es importante apuntar que las y los entrevistados no mencionaron ejemplos de requisas ni allanamientos dentro del curso de una investigación legal por parte de la Fiscalía General de la República o de la Policía Nacional Civil.

4.2.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones

Las y los entrevistados manifestaron que tenían conocimiento de casos en los que algunos opositores políticos y/o personas defensoras de derechos humanos eran chantajeados con la información

118 El Caso mencionado es de la Asociación de Niñas y Niños desaparecidos durante la guerra, PRO-BÚSQUEDA. En ese caso se conoce que unos "asaltantes robaron y destruyeron documentos y archivos relevantes de algunos procedimientos abiertos y otros ya archivados, así como ordenadores que contenían información clasificada. Seguidamente, rociaron con gasolina las oficinas allanadas y les prendieron fuego". Para más información del caso acceder al siguiente sitio: https://www.fidh.org/es/americas/El-Salvador/14281-el-salvador-allanamiento-robo-y-destruccion-de-documentos-en-las-oficinas

personal obtenida a través de intervenciones a sus telecomunicaciones, con el objetivo de que bajaran su perfil público y/o modificaran sus posturas críticas, sin embargo hubo dificultad para precisar sobre casos en específico.

Por otra parte, mencionaron que se utilizan mecanismos como blogs anónimos y cuentas de redes sociales identificadas como *troles* que utilizan la información personal de opositores y defensores y defensoras para hacer una especie de desprestigio y calumnia de aquellos que son considerados como incómodos. El caso más emblemático conocido fue el del director de una organización de la sociedad civil, la Fundación Nacional para el Desarrollo Económico (FUNDE), cuyo director sufrió una serie de ataques usando la información privada de uno de sus familiares.

La FUNDE, que es el capítulo nacional de Transparencia Internacional en El Salvador, ha mantenido una línea crítica hacia el gobierno en temas de transparencia y acceso a la información, a través de diversos medios de comunicación. El director de la organización manifestó ante los medios de comunicación que la información que habían utilizado contra él había sido trabajada en Casa Presidencial, guardada en una USB y luego había sido viralizada desde un cyber-café lejos de la presidencia.

> El director de la Fundación Nacional para el Desarrollo (FUNDE), Roberto Rubio, cuestionó ayer [*18/Mayo/2015*] al secretario de Transparencia de la Presidencia, Marcos Rodríguez, luego de haber recibido ataques por internet, en los que se compromete a una de sus familiares más cercanas […] Rubio aseguró que tiene información de que existen oficinas en Casa Presidencial que se dedican a hacer ataques por internet a personas que no comparten la ideología del gobierno del FMLN[119].

Debe mencionarse que en este caso, el mismo personero de gobierno señalado, Marcos Rodríguez, se desligó totalmente de estas prácticas y acudió a la Fiscalía General de la República para pedir que se investiguen los ataques contra Roberto Rubio, director de la FUNDE. Más allá de quién es el responsable de este acoso en específico, lo importante es que los y las entrevistados expresaron que quienes se encuentran en oposición a algunos funcionarios del Estado pueden ser víctimas de vigilancia y acoso a través de las nuevas tecnologías, a lo cual debe prestarse especial atención sin que esto signifique que pueda afirmarse contundentemente la existencia de un aparataje estatal designado para hacer este tipo de labores. Sin embargo, las dudas están allí y deben considerarse.

Otro caso importante que fue mencionado por varios de las y los entrevistados fue el del sacerdote español, padre Antonio Rodríguez, en las que sí hubo una investigación de parte de la Fiscalía General de la República en la que se solicitó la intervención y grabación de sus llamadas telefónicas debido a su relación y trabajo con pandilleros. Las y los entrevistados mencionaron que era probable que

119 Fernando Romero, "Roberto Rubio cuestiona a Marcos Rodríguez por ataques en internet", *La Prensa Gráfica*, (19 de mayo de 2015), bajo *sección Política*, http://www.laprensagrafica.com/2015/05/19/roberto-rubio-cuestiona-a-marcos-rodriguez-por-ataques-en-internet (consultado: 7 noviembre, 2015)

las conversaciones íntimas del padre Antonio pudieran haber sido utilizadas fuera de los parámetros establecidos por la Ley Especial para la Intervención de las Telecomunicaciones (LEIT) de parte de la FGR para lograr la condena del padre Antonio. Por otra parte, muchas de las conversaciones grabadas fueron filtradas a los medios, a pesar de que la LEIT establece que estas tienen carácter de reservadas para el proceso penal[120].

4.3. Inquietudes

4.3.1 Vigilancia

Una de las dudas que aparece de manera más constante tanto en técnicos como en defensores y defensoras es la de los criterios utilizados para intervenir las telecomunicaciones, es decir si existen criterios claros establecidos y dónde se encuentran plasmados, por medio de los cuales la Fiscalía justifica o fundamenta la solicitud de una intervención a las telecomunicaciones. En el razonamiento de las y los entrevistados, de no existir unos criterios establecidos por ley, esto quedaría al arbitrio del Fiscal General de la República o de los encargados del Centro de Intervención de las Telecomunicaciones (a cargo del Fiscal General), los cuales podrían utilizar casi cualquier tipo de justificación -o incluso crearla- para que el juez autorizara la intervención.

Por otra parte, algunos de los técnicos expresaron sus dudas con respecto a la claridad de la legislación salvadoreña para utilizar el espacio radioeléctrico, manifestando que perciben pocas o nulas garantías sobre el manejo de la información personal que hacen las empresas telefónicas. Entre las dudas más frecuentes que los técnicos manifestaron sobre los marcos legales para la protección de los datos personales e institucionales se encuentran: ¿Se quedan las empresas de telefonía con nuestra información? ¿Por cuánto tiempo? ¿Con qué tipo de información?

> La legislación es ambigua y es para beneficio de quienes en algún momento pueden vigilar. Por eso ellos podrían manipular la legislación vigente. Toda esa [posibilidad] está en la Ley de Telecomunicaciones. Técnico 5[121]

> Aún cuando se aprueben marcos legales que protejan el derecho a la privacidad de la ciudadanía, esto puede ser evadido por entidades o personas con intereses políticos particulares. Creo que la inmunidad de la que gozan los políticos debe ser revisada y cuestionada. Técnico 1[122]

120 Una nota del periódico digital El Faro sostiene que "durante la negociación para lograr que [el sacerdote] Antonio Rodríguez confesara haber cometido delitos en su labor de mediación con la pandilla 18, el Fiscal General hizo que lideres religiosos y diplomáticos españoles escucharan grabaciones de conversaciones íntimas del sacerdote, aparte de los audios que le incriminaban legalmente. Varios de los implicados afirman que al escuchar las grabaciones se sintieron implícitamente amenazados por el fiscal y que ello influyó en el desenlace judicial". Acceder a nota en el siguiente enlace: http://www.elfaro.net/es/201409/noticias/15912/Fiscal-us%C3%B3-conversaciones-%C3%ADntimas-del-padre-To%C3%B1o-para-conseguir-su-confesi%C3%B3n.htm

121 Respuesta de Técnico 5 en Grupo Focal con Técnicos Informáticos que trabajan en el ámbito de la defensa de Derechos Humanos. San Salvador, El Salvador. 28 de agosto de 2015.

122 Respuesta de Técnico 1 en Grupo Focal con Técnicos Informáticos que trabajan en el ámbito de la defensa de Derechos Humanos. San Salvador, El Salvador. 28 de agosto de 2015.

Finalmente, otra de las dudas que expresaban -principalmente los técnicos entrevistados- era qué se entendería por delito informático, debido a que durante la realización de las entrevistas se conoció de la discusión legislativa sobre un proyecto de ley sobre delitos informáticos. Los entrevistados no conocían de espacios o procesos de consulta para dicho proyecto ley, manifestaron que ellos como técnicos no habían sido invitados ni conocían a nadie que hubiese sido invitado para conocer y/o comentar en el anteproyecto de ley.

4.3.2. Anonimato y cifrado

Sobre anonimato y cifrado surgieron dudas generales sobre su prohibición o habilitación para utilizarlos, manifestándose más que una preocupación una especie de desconocimiento sobre la legalidad o no de usar cifrado o que la legislación salvadoreña contemple la posibilidad de anonimato digital. De manera muy clara llegaron a sostener que "existen muchos vacíos en cuanto a la protección de la información y de sus datos[123]".

4.3.3. Allanamientos y requisas

Las dudas sobre allanamientos y requisas estuvieron principalmente relacionadas con qué información pueden quitar o pedir las autoridades, y qué normas pueden utilizarse para que no les quiten información de manera arbitraria. También surgieron dudas sobre la utilización del término *flagrancia* en el derecho penal, el cual según alguno de los defensores de derechos humanos era demasiado amplio y que valiéndose de él se podía recabar información arbitrariamente con la excusa de estar aún en el tiempo de flagrancia en el cometimiento de un delito. En tal sentido la duda era ¿hasta dónde alcanza la flagrancia?

4.3.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones

Otra de las inquietudes estaba relacionada con los efectos de la aplicación de la Ley Especial contra Actos de Terrorismo (LEAT) y de la sentencia de la Sala de lo Constitucional que avaló el uso de

123 Respuesta de Técnico 3 en Grupo Focal con Técnicos Informáticos que trabajan en el ámbito de la defensa de Derechos Humanos. San Salvador, El Salvador. 28 de agosto de 2015.

dicha normativa[124]. La LEAT penaliza a los apologistas y colaboradores de las que son consideradas organizaciones terroristas, lo que ha despertado muchas dudas y aprehensiones en varias organizaciones de la sociedad civil y defensoras de derechos humanos que trabajan en comunidades controladas por las pandillas (las cuales son consideradas agrupaciones terroristas según la Sala de lo Constitucional) y con jóvenes pandilleros o ex pandilleros en programas de reinserción, pacificación e inclusión.

En el contexto de la LEAT, los y las entrevistadas manifestaron su desconfianza en las instituciones responsables de la investigación criminal (PNC y FGR), quienes estarían a cargo de la implementación de dicha ley expresando sus dudas con respecto a la posibilidad de que esta sea utilizada para criminalizar su ejercicio de defensa de derechos humanos.

4.4. Conclusiones preliminares

4.4.1. Sobre experiencias

En general, se manifiesta una amplia desconfianza por parte de defensores y defensoras de derechos humanos en las instituciones responsables de la investigación del delito (PNC y FGR), quienes estarían a cargo de la implementación de varias leyes que causan suspicacia respecto a la posibilidad de su utilización para vigilar y/o criminalizar su ejercicio de defensa de derechos humanos. El contexto de combate contra las pandillas y la criminalidad, en su modalidad *antiterrorista*, genera muchas más dudas y temores en defensoras y defensores de derechos humanos.

En consonancia con ello, hay una percepción generalizada sobre la práctica de vigilancia de las comunicaciones a defensores y defensoras de derechos humanos, tanto por parte del Estado como de entes paraestatales. Dicha noción y preocupación por la intervención en sus telecomunicaciones ha aumentado debido a la actual lógica *manodurista*, bajo la cual las invasiones a la privacidad podrían ser normalizadas o vistas como necesarias no solo por parte de los funcionarios públicos, sino también por una parte de la ciudadanía, desesperada por la agobiante situación de violencia e inseguridad.

124 En 2005, luego del asesinato de dos efectivos policiales por un joven francotirador -ligado al partido FMLN- durante una protesta frente a la Universidad de El Salvador (UES), el partido de gobierno de aquel entonces (ARENA) propuso la Ley Especial contra Actos de Terrorismo (LEAT), la cual fue duramente criticada por organizaciones de la sociedad civil (muchas de ellas defensoras de derechos humanos) y por el principal partido de oposición de ese entonces (FMLN), quienes sostenían que lo que realmente se buscaba era criminalizar la protesta social, por lo que presentaron sendos recursos de inconstitucionalidad contra la ley en 2007. La resolución de estos recursos de inconstitucionalidad (REF 22-2007/42-2007/89-2007/96-2007) fue postergada hasta agosto de 2015, dándose en un contexto de recrudecimiento del enfrentamiento entre policías y pandilleros. La Sala de lo Constitucional falló no ha lugar a los recursos de inconstitucionalidad y, además, afirmó en su sentencia que las pandillas MS13 y Barrio 18 era consideradas terroristas (algo que no fue solicitado ni mencionado en ninguno de los recursos), coincidiendo en ello con el gobierno de turno (FMLN) que desde inicios de 2015 inició una renovada política de *manodurismo* y ha insistido en denominar a las *maras* como organizaciones terroristas debido principalmente a que estas han asesinado sistemáticamente a muchos efectivos policiales desde finales de 2013 con el objetivo de presionar para volver a una negociación similar a la que se dio en el marco de la tregua entre pandillas de marzo de 2012.

Se identificaron varios casos de uso de blogs anónimos y cuentas de redes sociales -identificadas como *troles*- que utilizan la información personal de aquellos que son considerados como incómodos para atacar su credibilidad personal o su intimidad familiar. También muchos ataques verbales en redes sociales, sobre todo cuando se trata de defensa de derechos humanos de la comunidad LGBTI y discusiones sobre derecho al aborto.

A pesar de lo anteriormente expuesto, en las y los entrevistados predominó aún más el temor y la preocupación por los ataques y atentados físicos que puedan sufrir debido a la situación de violencia e inseguridad, que los ataques a la privacidad de sus telecomunicaciones. Además, varios señalaron que la situación de aguda violencia es un escenario adecuado para que se dé algún tipo de prácticas de intimidación o violencia por motivo de su trabajo, pero que es difícil diferenciar de otro tipo de violencia ante una situación tan profunda de inseguridad. Sobre todo cuando las instituciones para la investigación del delito son muy deficientes y causan poca confianza entre los y las entrevistadas.

Se identificaron también varios casos de allanamiento ilegal a oficinas de organizaciones defensoras de derechos humanos por desconocidos durante el contexto de ciertos casos simbólicos y con cierta relevancia mediática que ellos estaban llevando. Sin embargo, no se mencionaron ejemplos de requisas ni allanamientos dentro del curso de una investigación legal por parte de la Fiscalía General de la República o de la Policía Nacional Civil.

La utilización de información personal con otros fines, como las del mercado, probablemente sea más fácil de detectar y demostrar. Sin embargo, se vuelve sumamente difícil de determinar si las nuevas tecnologías de la comunicación e información están siendo utilizadas con fines de control político y/o criminalización hacia opositores en general, y defensores y defensoras de derechos humanos en particular.

4.4.2. Dudas sobre el marco legal

La discusión sobre recursos como anonimato y cifrado para proteger su privacidad genera aún pocas reacciones, pues las y los entrevistados han comenzado a tomar mayor conciencia muy recientemente de la importancia de su privacidad en las telecomunicaciones y de los riesgos que implica no estar preparados ni como individuos ni como organizaciones. Surgieron dudas generales sobre su prohibición o habilitación para utilizarlos, manifestándose más que una preocupación una especie de desconocimiento sobre la legalidad o no de usar cifrado o que la legislación salvadoreña contemple la posibilidad de anonimato digital.

Otra de las dudas sobre marco jurídico fue la de los criterios utilizados para intervenir las telecomunicaciones, es decir, si existen criterios claros y dónde se encuentran plasmados, por medio de los cuales la FGR justifica o fundamenta la solicitud de una intervención a las telecomunicaciones.

Por otra parte, surgieron dudas con respecto a la claridad de la legislación salvadoreña para utilizar el espacio radioeléctrico, manifestando que perciben pocas o nulas garantías sobre el manejo de la información personal que hacen las empresas telefónicas. Entre las dudas más frecuentes sobre la protección de datos personales e institucionales estaban: ¿Se quedan las empresas de telefonía con nuestra información? ¿Por cuánto tiempo? ¿Con qué tipo de información?

Las dudas sobre allanamientos y requisas estuvieron principalmente relacionadas con qué información pueden quitar o pedir las autoridades, y qué normas pueden utilizarse para que no les quiten información de manera arbitraria. También surgieron dudas sobre la utilización del término *flagrancia* en el derecho penal, el cual podría estar siendo utilizado para recabar información arbitrariamente con la excusa de estar aún en el tiempo de flagrancia en el cometimiento de un delito.

Otra de las inquietudes giró alrededor de los efectos de la aplicación de la Ley Especial contra Actos de Terrorismo (LEAT), a propósito de una reciente sentencia de la Sala de lo Constitucional que avaló el uso de dicha normativa. La aplicación de la LEAT despierta muchas dudas y aprehensiones en organizaciones defensoras de derechos humanos, principalmente aquellas que trabajan en comunidades controladas por las pandillas y con jóvenes pandilleros o ex pandilleros en programas de reinserción, pacificación e inclusión social.

5. Conclusiones nacionales

Si bien el marco legal y la jurisprudencia salvadoreña brindan importantes garantías generales para proteger el derecho a la privacidad digital, también es importante reconocer que algunas normas secundarias que han sido aprobadas recientemente -generalmente en el marco del combate a la violencia y el crimen-, podrían ser utilizadas para vigilar, obstaculizar y/o criminalizar la labor de personas defensoras de derechos humanos.

Sin embargo, el principal riesgo para el derecho a la privacidad digital de personas defensoras de derechos humanos más que en el marco legal se identifica en las prácticas institucionales, pues las instituciones públicas salvadoreñas (principalmente las encargadas y/o relacionadas con seguridad y justicia) gozan de baja credibilidad, así como de poca eficiencia e independencia. Las y los defensores de derechos humanos entrevistados pusieron especial énfasis en su desconfianza en las prácticas institucionales, antes que en el marco jurídico como tal.

Los principios internacionales de derechos humanos para la vigilancia de las telecomunicaciones aún son poco o nada conocidos, y la escasa discusión sobre los nuevos marcos jurídicos que El Salvador necesita en materia de telecomunicaciones e informática aún no los toma en cuenta. Generalmente, el impulso de las pocas legislaciones existentes (Ley de Firma Electrónica, Ley Especial para la Intervención de las Telecomunicaciones, etc.) viene dado por la dinámica del mercado o por las urgencias de seguridad pública, dejando del lado (o en un plano secundario) lo relacionado con la protección de la información, identidad y privacidad de las y los usuarios.

Aún no se detectan en El Salvador organizaciones con relevancia en la defensa del derecho a la privacidad en general ni en la privacidad digital en específico. La privacidad digital parece ser un derecho y un aspecto de la realidad que aún no es importante para la sociedad salvadoreña, en buena medida preocupada primordialmente por su seguridad física. Algo similar parece darse entre defensores y defensoras de derechos humanos, quienes si bien es cierto están más alerta a las posibles vulneraciones a su privacidad digital, aún están en una etapa inicial de toma de conciencia y de adopción de algunas medidas básicas de seguridad. Sin embargo, la privacidad digital aún no es una demanda fuerte desde las y los defensores de derechos humanos en el país.

En general, existe una arraigada noción entre los y las defensoras de derechos humanos de que en El Salvador la vigilancia de las telecomunicaciones es una práctica histórica, que no solo es y ha sido ejercida por entes estatales, sino también por entes privados, paraestatales e incluso extranjeros. En los últimos años se ha incrementado el número de casos de filtraciones de documentos privados a la prensa o las redes sociales, así como allanamientos ilegales para sustraer computadoras con información sensible sobre la labor de organizaciones de derechos humanos. A pesar de ello, la

privacidad digital aún no es un asunto importante en la agenda de defensa de derechos humanos del país.

Es importante también señalar que el cambio de partido de gobierno en 2009 marcó un parteaguas para el ejercicio de defensa de derechos humanos en el país, generando nuevos escenarios y relaciones que están modificando las prácticas y la visión de defensoras y defensores de derechos humanos. Aunado e esto, la profunda violencia social e inseguridad también han propiciado que el ejercicio de la defensa de derechos humanos deba replantearse en muchos sentidos. Por otra parte, la aut-concepción y auto-denominación como defensoras y defensores de derechos humanos, así como su identidad gremial o asociativa, es muy probablemente más débil que en otros países centroamericanos.

Bibliografía

Libros

Alianza Regional por la Libre Expresión e Información. *El SABER MAS III Informe Regional sobre Acceso a la Información Pública y la Protección de Datos Personales. (*Washington D. C, EUA., 2011.

Armstrong, Gary Armstrong, y Kotler, Philip. *Marketing: Versión para Latinoamérica.* México D.F.: Pearson Educación, 2007.

Ayala, José Ma. et al. *La protección de datos personales en El Salvador*. El Salvador: UCA Editores, 2005.

Bertoni, Eduardo. *Hacia un internet libre de censura: propuestas para América Latina*. Argentina: Universidad de Palermo, 2012.

Bidart Campos, Germán. *Manual de la Constitución Reformada*. Buenos Aires: Ediar, 1998.

Catucci, Silvina. *Libertad de Prensa. Calumnias e injurias*. Buenos Aires: Ediar, 1995.

Comisión de la Verdad para El Salvador. *Informe de la Comisión de la Verdad para El Salvador. De la locura a la esperanza: la guerra de 12 años en El Salvador.* San Salvador-Nueva York: Organización de las Naciones Unidas, 1992-1993.

De Slavin, Diana. *1 MERCOSUR: la protección de los datos personales*. Buenos Aires: Ediciones de Palma, 1999.

Ferrajoli, Luigi. *Derechos y garantías: el derecho del más débil*. Madrid: Editorial Trotta, 2004.

Fundación Salvadoreña para el Desarrollo Económico y Social. *Informe de coyuntura legal e institucional*. El Salvador: FUSADES, 2014.

García Ramírez, Sergio y Gonza, Alejandra. *Libertad de Expresión en la jurisprudencia de la Corte Interamericana de Derechos Humanos*. México DF: Comisión de Derechos Humanos del Distrito Federal, 2007.

González, Norberto. *El Deber del Respeto a la Intimidad.* España: Universidad de Navarra, Pamplona, 1990.

Instituto Nacional de Derechos Humanos. *Internet y Derechos Humanos. Cuadernillo Temas Emergentes Internet y Derechos Humanos*. Chile: Consejo del Instituto Nacional de Derechos Humanos, 2013.

Linares Quintana, Segundo. *Tratado de la Ciencia del Derecho Constitucional Argentino y Comparado*, T. IV. Buenos Aires: Plus Ultra, 1977.

Puccinelli, Oscar. *El Hábeas Data. Santa Fe de Bogotá.* Colombia: Temis, S.A., 1999.

Rodríguez, Katitza. *Anonimato y Cifrado: Comentarios enviados a la Relatoría Especial de la Comisión de Derechos Humanos sobre la promoción y protección del derecho a la libertad de opinión y de expresión*. San Francisco, EUA: Electronic Frotntier Foundation, 2015. https://www.eff.org/files/2015/03/18/anonimatoycifrado-eff-11.pdf (consultado: 5 noviembre, 2015)

Velásquez Velásquez, Santiago y Nuques, María Isabel. *El derecho a la intimidad y la competencia desleal*. Ecuador: Facultad de Derecho de la Universidad Católica de Guayaquil, s.f.

Revistas de difusión

Almeida, Mónica. "Estado, medios y censura soft: una comparación transnacional y transideológica". *Nueva Sociedad,* enero-febrero, 2013.

Álvarez Ugarte, Ramiro. "El caso Snowden y la democracia en disputa". *Nueva Sociedad*, septiembre-octubre, 2013, http://www.nuso.org/upload/articulos/3975_1.pdf (consultado: 25 marzo, 2015).

Figueroa, Luis. "SmartPhones: una revolución en las comunicaciones". *Realidad y Reflexión*, septiembre-diciembre, 2011.

Jaramillo, Paula y Lara, J. Carlos. "Derechos fundamentales en internet y su defensa ante el Sistema Interamericano de Derechos Humanos". *ONG Derechos Digitales*, (s.f.).

Revistas académicas

Velásquez Velásquez, Santiago y Nuques, María Isabel. "El Derecho a la Intimidad y la Competencia Desleal". Facultad de Derecho de la Universidad Católica de Guayaquil, s.f., http://www.revistajuridicaonline.com/index.php?option=com_content&task=view&id=65&Itemid=27 (consultado: 15 marzo, 2015)

Artículos y noticias de periódicos

"Circulan 1.8 millones de smartphones en el país". *El Diario de Hoy*, 4 de noviembre, 2014, bajo *sección Negocios*. http://www.elsalvador.com/mwedh/nota/nota_completa.asp?idCat=47861&idArt=9218924 (consultado: 8 abril, 2015)

"El Salvador expresa preocupación por posible espionaje de EEUU en América Latina". *Diario digital Voces*, 11 de julio, 2013. http://voces.org.sv/2013/07/11/el-salvador-expresa-preocupacion-por-posible-espionaje-de-eeuu-en-america-latina/ (consultado: 25 marzo, 2015)

Fernández, Omar. "Organizaciones de Derechos Humanos denuncian represión y persecución del Estado hondureño a la coordinadora de Las Chonas Gladys Lanza". *Diario Co Latino*, 6 de febrero, 2015, bajo *sección Nacionales*. http://www.diariocolatino.com/organizaciones-de-derechos-humanos-denuncian-represion-y-persecucion-del-estado-hondureno-a-la-coordinadora-de-las-chonas-gladys-lanza/ (consultado: 5 noviembre, 2015)

Monge, Saúl. "Piden investigar a ex vicepresidente de Pacific Rim, por muerte de ambientalistas". *Periódico Verdad Digital*, 22 de septiembre, 2014, bajo *sección Social*. http://verdaddigital.com/index.php/social-48/12831-piden-investigar-a-ex-vicepresidente-de-pacific-rim-en-el-salvador-por-muertes-de-ambientalistas (consultado: 5 noviembre, 2015)

Tesis

Torres, Juan Duarte et al. "La efectividad de la función de prevención especial en la aplicación de las medidas de seguridad a los inimputables." Tesis de Licenciatura, Universidad de El Salvador, 2013.

Alcántara Quintanilla, Milton Leónidas et al. "Análisis jurídico del comercio electrónico." Monografía de Licenciatura, Universidad Francisco Gavidia, 2003.

Álvarez Hernández, Katia Susana et al. "Aplicación legal práctica para la realización de actividades económicas en el comercio electrónico." Monografía de Licenciatura, Universidad Dr. José Matías Delgado, 2011.

Gómez Molina, Luis Alfredo. "Aspectos generales del delito informático." Monografía de Licenciatura, Universidad Francisco Gavidia, 2004.

Hernández León, María Elena et al. "Habeas Data como mecanismo de protección de derechos relacionados con la autodeterminación informativa ante el tratamiento automatizado de datos personales." Tesis de licenciatura, Universidad de El Salvador, 2006.

Lemus, Ana Marcela y Canales, César Villatoro. "La brecha digital en El Salvador: causas y manifestaciones." Tesis de Licenciatura, Universidad Centroamericana José Simeón Cañas, 2009.

López Flores, Sarbelio Enrique. "La Firma Electrónica, tecnología del siglo XXI en la legislación salvadoreña." Tesis de Licenciatura, Universidad de El Salvador, 2007.

Miranda Chicas, Verónica Beatriz et al. "El derecho a la intimidad, su limitabilidad y protección en el marco normativo de la ley especial para la intervención de las telecomunicaciones." Tesis de Licenciatura, Universidad de El Salvador, 2010.

Legislación nacional

El Salvador. "Constitución de la República de El Salvador". Asamblea Legislativa (1983).

El Salvador. "Código Penal". Asamblea Legislativa (1997).

El Salvador. "Código Procesal Penal". Asamblea Legislativa (2009).

El Salvador. "Ley de Acceso a la Información Pública". Asamblea Legislativa (2012).

El Salvador. "Ley de Anotaciones Electrónica en cuenta de Valores". Asamblea Legislativa (2002).

El Salvador. “Ley de Bancos”. Asamblea Legislativa (1999).

El Salvador. “Ley de Protección al Consumidor”. Asamblea Legislativa (2005).

El Salvador. “Ley de Simplificación Aduanera”. Asamblea Legislativa (1999).

El Salvador. “Ley del Organismo de Inteligencia del Estado”. Asamblea Legislativa (2001).

El Salvador. “Ley Especial contra el Delito de Extorsión”. Asamblea Legislativa (2015).

El Salvador. “Ley Especial para la Intervención de las Telecomunicaciones”. Asamblea Legislativa (2010).

El Salvador. “Ley General Marítimo Portuaria” Asamblea Legislativa (2002).

El Salvador. “Ley Orgánica de la Policía Nacional Civil”. Asamblea Legislativa (2001).

El Salvador. “Ley Reguladora del Uso de Medios de Vigilancia Electrónica en Materia Penal”. Asamblea Legislativa (2015).

Jurisprudencia

Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 142-2012 del 20 de octubre de 2014.

Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 934-2007 del 4 de marzo de 2011, parte III 1. B. a.

Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo 934-2007 del 4 de marzo de 2011, parte III, 1 A.

Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Habeas Corpus 135 – 2005/32 – 2007 (acumulado) del16 de mayo de 2008.

Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Habeas Corpus 249- 2002 del 24 de febrero de 2003.

Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Habeas Corpus 255- 2000 del 14 de septiembre de 2000.

Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Habeas Corpus 255- 2000 del14 de septiembre de 2000.

Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Inconstitucionalidad 118-2002 del 2 de marzo de 2004.

Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Inconstitucionalidad 58-2007 del 8 de marzo de 2013.

Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Inconstitucionalidad 84-2006 del 20 de enero de 2009.

Páginas web

Arzobispado de San Salvador. "Tutela Legal". Arzobispado de San Salvador, http://www.arzobispadosansalvador.org/index.php/medios-de-comunicacion/radio-paz/11-nosotros/15-tutela-legal (consultado: 20 mayo, 2015).

Procuraduría para la Defensa de los Derechos Humanos. "Balance sobre la situación de los derechos humanos a 21 años de los Acuerdos de Paz". La Procuraduría, http://www.pddh.gob.sv/menupress/menuprensa/457-pddh-brinda-balance-sobre-la-situacion-de-los-derechos-humanos-a-21-anos-de-los-acuerdos-de-paz (consultado: 20 mayo, 2015).

Organismo Especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación (UIT). "Informe sobre estadísticas de suscripciones de teléfonos móviles en El Salvador". UIT: 2014, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (consultado: 20 mayo, 2015).

Organismo Especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación (UIT). "Informe sobre estadísticas de individuos que usan Internet en El Salvador". UIT: 2014, http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (consultado: 20 mayo, 2015).

lqVRomqgghOAGr2Ov9VxK/Eb

r79b8K3hVurUKZnLI8ag

RXlyjpbQioxwxvU1jeZpj86Z/sIDhll vy5WvrrskJ4A1dbQioxwx

CPRXlyjpbQioxwxvU1jeZpj86Z/sIDhll vy5

oxwxvGuatemala/sl

sCPRXlyjpbQioxwxvU1jeZpj86Z/sIDhll vy5WvrrskJ4A1dbQiox

Jorge Jiménez Barillas
Hedme Sierra-Castro[1]

1. Antecedentes

1.1. Estado de la discusión nacional

Las nuevas formas de vigilancia adoptadas por algunos gobiernos son una amenaza al derecho a la privacidad, y nadie entiende mejor estos desafíos que quienes trabajan por la promoción y defensa de los derechos fundamentales de las personas. Aunque el acceso a las tecnologías aún resulta ser un reto en países en vía de desarrollo, el uso de medios electrónicos de almacenamiento de información y medios de comunicación y difusión de la información (internet, blogs, redes sociales, correo electrónico, etc.), se vuelve más común entre la amplia y diversa comunidad de activistas de derechos humanos, ya que las nuevas Tecnologías de la Información y la Comunicación (TIC) les permite, entre otras cosas, compartir información y hacer denuncias en tiempo real, así como socializar comunicados y acciones urgentes con un mayor número de personas y organizaciones a nivel internacional.

Pese a que las prácticas de intervención masiva a las comunicaciones se remontan a inicios del siglo anterior, cuando el espionaje militar tenía acceso a los telegramas enviados, recibidos y retransmitidos por Estados Unidos, no fue sino hasta 2013, con las revelaciones[2] de Edwards Snowden[3], que el mundo comenzó a tomar conciencia sobre los grandes alcances de la vigilancia digital, ejercida por los gobiernos en nombre de la seguridad nacional. Los diversos programas mediante los que se obtienen datos de las comunicaciones en forma masiva son utilizados violando los derechos a la privacidad de millones de personas que no son sospechosas de haber cometido un delito y mucho menos de tener conexión alguna con el crimen organizado.

Con ansias de indagar a profundidad sobre el contexto particular de Guatemala respecto al derecho a la privacidad y conocer también el nivel de la discusión del tema a nivel nacional, es decir, el momento en el que se encuentra este debate dentro de la agenda social-política guatemalteca, se consultaron diversas fuentes de información tales como: informes de situación producidos y publicados por organizaciones de sociedad civil defensoras de derechos humanos, informes de instituciones gubernamentales, informes y publicaciones de organismos internacionales respecto a Guatemala,

1 La Máster Hedme Sierra-Castro es la autora de los apartados “Antecedentes” y “Experiencias e inquietudes del sector técnico y de defensa de derechos humanos”. Por su parte, la autoría de los apartados “Marco legal nacional” y “Análisis del marco legal nacional desde los estándares internacionales” corresponde al Licenciado Jorge Jiménez Barillas, con la colaboración de la Máster Sierra-Castro. Finalmente, las conclusiones generales fueron elaboradas de forma conjunta.

2 Ewen Macaskill y Gabriel Dance, “NSA files: decoded”, *The Guardian* (2013), http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 (consultado: 5 noviembre, 2015)

3 Edward Snowden ex técnico de inteligencia, antiguo empleado de la Agencia Central de Inteligencia (CIA) y de la Agencia de Seguridad Nacional (NSA).

monitoreo de medios de comunicación digitales así como la producción académica de algunas de las universidades guatemaltecas.

Guatemala cuenta con diecisiete universidades tanto públicas y privadas. La producción académica encontrada y consultada corresponde a tesis de Licenciatura y tesis de Maestría de la Universidad de San Carlos y la Universidad Rafael Landívar respectivamente. Los principales hallazgos fueron sobre los antecedentes históricos del derecho a la privacidad en el derecho constitucional guatemalteco, el cual comenzó en 1824 con la primer Constitución guatemalteca[4]; la ilegalidad en el funcionamiento de empresas mercantiles que comercializan datos personales a entidades privadas o estatales vulnerando el derecho a la privacidad de las personas, poniendo en riesgo su seguridad y afectando su dignidad[5]; la intimidad en el ordenamiento jurídico guatemalteco referido a empresas que realizan operaciones profesionales relacionadas con servicios de investigación de personas individuales o jurídicas y comercializan datos personales[6]; el conflicto que existe entre la libertad de la información y la vida privada de las personas en la República de Guatemala[7]; el flujo correo electrónico comercial no solicitado (o SPAM) y el derecho a la confidencialidad de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna como garantía constitucional[8], y el rol indiferente del Estado ante tutela del derecho fundamental a la privacidad en el servicio de internet[9].

La legislación guatemalteca contiene una sólida protección a derechos inherentes y fundamentales de las personas, como el derecho a la inviolabilidad del domicilio, de la correspondencia y de las escuchas telefónicas, entre otros[10]; aunque no reconoce ni se menciona expresamente el derecho a la privacidad. Este derecho se observa únicamente de manera implícita en el artículo 44 cuando invoca los "derechos inherentes a la persona humana", y en los otros derechos mencionados anteriormente. De esta manera, en el actual contexto de desarrollo tecnológico que promueve la vigilancia, surge la necesidad que el derecho a la privacidad se proteja no de manera implícita sino más bien de manera

4 Sandra González Rivera, "La regulación del derecho a la intimidad en el derecho constitutional guatemalteco" (tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2007), 85, http://biblioteca.usac.edu.gt/tesis/04/04_6641.pdf (consultado 5 noviembre, 2015)

5 Lourdes Boj Saavedra, "Análisis sobre la ilegalidad en el funcionamiento del Sistema de Información en Red "INFORNET" y el respeto al derecho a la privacidad, seguridad y dignidad" (tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2012), 75-96, http://biblioteca.usac.edu.gt/tesis/04/04_9993.pdf (consultado 5 noviembre, 2015)

6 Julio Díaz Sontay, "Análisis del derecho a la intimidad en el ordenamiento jurídico guatemalteco referido a empresas mercantiles que comercializan datos personales", (tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2011) 85-99, http://biblioteca.usac.edu.gt/tesis/04/04_9520.pdf (consultado 5 noviembre, 2015)

7 William Portillo Menjivar, "El conflicto que existe entre la libertad de la información y la vida privada de las personas en la República de Guatemala", (tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2012), 19-30, http://biblioteca.usac.edu.gt/tesis/04/04_9899.pdf (consultado 5 noviembre, 2015)

8 Max Mazariegos de León, "El correo electrónico o SPAM y el derecho humano a la intimidad o privacidad; Visión desde el ámbito del derecho internacional de los Derechos Humanos", (tesis de Maestría, Facultad de Ciencias Jurídicas y Sociales, 2012), 55-58, 82, http://biblio3.url.edu.gt/Tesis/2012/07/07/Mazariegos-Max.pdf (consultado 5 noviembre, 2015)

9 Vilma Juarez del Cid, "El rol del Estado en la tutela del derecho fundamental de privacidad de los usuarios del servicio de Internet como producto de la tecnología moderna", (tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2014), 73, 80-81, http://biblio3.url.edu.gt/Tesario/2014/07/01/Juarez-Vilma.pdf (consultado 5 noviembre, 2015)

10Guatemala "Constitución Política de la República de Guatemala" Congreso Nacional de la República (1985), artículos 23, 24, 44.

concreta que dé como resultado una herramienta jurídica para poder defender este derecho[11]. La falta de protección al derecho a la privacidad genera un comprometedor vacío legal y deja, a su vez, la puerta abierta a la libre interpretación.

Por otro lado, en cuanto a la protección del Estado ante el derecho a la privacidad en internet, entendiendo el excepcional alcance global de internet y que es tarea del mismo Estado crear mecanismos de regulación que se adhieran a las normas y estándares internacionales de derechos humanos, el Estado guatemalteco tiene dentro de su ordenamiento jurídico una regulación poco precisa en relación a la protección del derecho a la privacidad en internet. En este caso, las Cortes del país pueden suplir la ambigüedad respecto a la protección de este derecho. La actual regulación se encuentra orientada especialmente a proteger a las personas usuarias de internet de la posible comisión de delitos en su contra a través de medios electrónicos de comunicación y a regular situaciones que podrían alterar el orden público, mas no de proteger el ámbito privado de su vida personal, el cual es vulnerado de muchas maneras a través de internet[12].

En 2012, Guatemala firmó junto con otros ochenta y ocho países el tratado sobre regulación de internet[13] promovido para respaldar las regulaciones que busquen controlar los contenidos de internet. Sin embargo, a lo interno no cuenta con una regulación que determine las responsabilidades de las empresas proveedoras de servicios y de los usuarios, y que establezca las competencias estatales en relación a la supervisión o regulación de internet.

1.2. Brecha digital

América Latina es la región más desigual y heterogénea del mundo[14], en la que si bien es cierto se ha logrado apreciar un significativo nivel de desarrollo económico en las últimas décadas, aún se observan altos niveles de pobreza, exclusión y desigualdad social. Tomando conciencia de lo anterior, resulta gratamente curioso que América Latina sea una de las regiones más proactivas del mundo en relación con la inclusión de la tecnología en sus sistemas educativos[15]. Sin embargo, la brecha digital resulta ser un problema aún no resuelto en la región, lo que es una pauta para estimar cuál es la población con acceso a internet y/o a las telecomunicaciones, y así estimar qué sector de la población

11 Sandra González Rivera, "La regulación del derecho a la intimidad en el derecho constitucional guatemalteco" (tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2007), 111, http://biblioteca.usac.edu.gt/tesis/04/04_6641.pdf (consultado 5 noviembre, 2015)

12 Vilma Juarez del Cid, "El rol del Estado en la tutela del derecho fundamental de privacidad de los usuarios del servicio de Internet como producto de la tecnología moderna", (tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2014), 105, http://biblio3.url.edu.gt/Tesario/2014/07/01/Juarez-Vilma.pdf (consultado 5 noviembre, 2015)

13 ITU, "Firmantes del Acta final", http://www.itu.int/osg/wcit-12/highlights/signatories.html (consultado 5 noviembre, 2015)

14 Leonardo Gasparini, Martín Cicowiez y Walter Sosa Escudero, *Pobreza y Desigualdad en America Latina: Conceptos, Herramientas y Aplicaciones.* (Argentina: Centro de Estudios Distributivos, Laborales y Sociales , UNLP, 2014), 3.

15 OCDE/CEPAL, *Perspectivas económicas de América Latina para 2012,* (OCDE, 2012), 98, http://www.agci.cl/attachments/article/693/2011-548_Leo2011_WEB.pdf (consultado 5 noviembre, 2015)

tiene este acceso vedado o, al menos, restringido, y de esta manera identificar la población cuyo derecho a la privacidad en el área digital puede ser violentado.

La brecha digital se entiende como la distancia en cuanto al acceso, uso y empoderamiento de las tecnologías entre la población, tanto urbana como rural, y se comprende dentro del nivel socio-económico y las dimensiones de género en articulación con otras desigualdades culturales. Todo lo anterior en consideración con la capacidad y calidad de la infraestructura tecnológica y el nivel de alfabetización en el uso de las tecnologías como parte de la adopción de políticas públicas que apunten a la democratización del conocimiento para reducir las dificultades en cuanto al acceso a los medios tecnológicos.

El acceso a los medios sociales en Guatemala sigue siendo un privilegio, y no se ha hecho mucho por empoderar a grupos históricamente excluidos de los medios de comunicación hegemónicos en las áreas rurales y entre las poblaciones indígenas. El uso de internet se concentra entre la clase media y la población juvenil urbana. Por otra parte, las organizaciones no gubernamentales han adoptado de manera tardía las plataformas digitales y, dado el limitado alcance de internet entre la población, el activismo de la sociedad civil tiende a emplear estrategias virtuales solo como un suplemento de campañas en los medios tradicionales[16].

Guatemala cuenta con una población estimada de 15.859.714 habitantes, que por cierto resulta ser la población más numerosa entre los países de la región centroamericana, de la cual solamente el 17.13% tiene acceso a internet a través del uso de computadoras y dispositivos móviles, y se concentra en la población urbana. Según el Banco Mundial, Guatemala tiene un índice de desarrollo de banda ancha (IDBA) de 3.71%.

El Departamento de Guatemala tiene una población estimada de 3.103.683 habitantes, lo que la convierte en el Departamento más poblado del país, y cuenta con un porcentaje aproximado del 29,75% de hogares que tienen servicio de internet. La ciudad capital detalla una penetración de internet del 28.75%; una penetración de computadoras de 52.3% y penetración de banda ancha de 4.59%.[17]

Por otro lado, el acceso a la telefonía en Guatemala se distribuye entre telefonía fija y móvil (terminales móviles analógicas y digitales, de crédito y prepago) así como teléfonos comunitarios y públicos. En base al último informe sobre la situación de la telefonía en Guatemala realizado por la Súper Intendencia de Telecomunicaciones (SIT) en 2013, se mostró un crecimiento significativo del 0.02% en el uso de telefonía fija entre 2004 y 2013. Por otro lado, el uso de telefonía móvil se multiplicó un

16Renata Ávila y Alejandra Gutiérrez, “Los Medios Digitales: Guatemala” (Guatemala: Open Society Foundation, 2013), 6-10.
17 BID/DIGILAC, “Penetración Internet en Guatemala” (Banco Interamericano de Desarrollo, http://kp.iadb.org/DigiLAC/es/Paginas/Indice-de-Desarrollo-de-Banda-Ancha.aspx (consultado 5 noviembre, 2015)

95% entre 2012 y 2013 con un total de 20.787.080 de terminales móviles digitales en operación con sistema de crédito y postpago en 2012, y un total de 21.716.357 en 2013[18].

Para 2014, según un boletín estadístico de la SIT, se aprecia un crecimiento del 79.42% en el total de líneas de telefonía fija con 1,718,298 unidades, cuya mayor cantidad se concentra en la ciudad capital con un total de 1,364,776 unidades. Mientras que el acceso a terminales móviles sobrepasa por mucho a las líneas fijas con un total de 16,911,811 unidades, de las cuales el 3.80% cuentan con plan de crédito y el 96.20% restante corresponde a unidades con plan prepago.[19] Llama la atención el crecimiento de más del 50% de las líneas de telefonía fija; resta suponer que la población se conecta a internet a través de líneas de telefonía fijas.

Lo anterior significa que la mayoría de la población cuenta con más de un teléfono celular y el porcentaje de uso de teléfono móvil con plan pospago es del 3.80%, mientras que el uso de plan prepago es de un 96.20%. El acceso a internet con el sistema prepago cuenta con precios que van, por ejemplo, desde 1.25 dólares hasta 9 dólares para tener acceso a internet y servicio de mensajería, mensajes de texto y llamadas nacionales o internacionales. Resulta importante destacar que las empresas de telefonía móvil proveen servicios de 3G y a partir del segundo semestre de 2015 se cuenta también servicios de conexión a internet 4G, que actualmente solamente tiene cobertura en el área metropolitana del Departamento de Guatemala.

Guatemala aún no cuenta con un plan nacional de banda ancha para aumentar el acceso a la tecnología y minimizar la brecha digital. Sin embargo, se encuentra mejor evaluada que Nicaragua y Honduras en el índice de desarrollo de la banda ancha (IDBA).[20] En cuanto a la aplicación de las nuevas tecnologías de la información y la comunicación (TIC), en 2013 Guatemala bajó 4 posiciones y se encuentra en el puesto 107[21]. En base a esto, se puede afirmar que no existen normas claras para manejo de la red, y que la calidad de servicio de internet móvil y de banda ancha resulta un tanto precaria.

Guatemala no tiene una política orientada a la capacitación en habilidades referidas a medios de comunicación, la efectividad de tales iniciativas es ciertamente limitada[22]. En 2007, la Superintendencia de Telecomunicaciones de Guatemala publicó un informe titulado “Penetración y adopción de la Internet

18 SIT, “Situación de la Telefonía en Guatemala” (Guatemala, Superintendencia de Telecomunicaciones, 2013), 33, http://www.sit.gob.gt/index.php/2014-05-28-20-40-11/situacion-de-la-telefonia-en-guatemala (consultado 5 noviembre, 2015)

19 SIT, Boletín Estadístico 9, 20 y 45.

20 Unión Internacional de Telecomunicaciones, “Visión General de Banda Ancha en América” (ITU, 2014), 17-18, 82, http://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/PBLCTNS/2014_Sp_PostCAS.pdf (consultado 5 noviembre, 2015)

21 Networked Readiness Index,.. “The Global Information Technology Report Report 2013” (2013), http://www3.weforum.org/docs/GITR/2013/GITR_OverallRankings_2013.pdf (consultado 5 noviembre, 2015)

22 Avila y Gutiérrez, “Los Medios Digitales”, 10.

y de las tecnologías de la información y comunicaciones en Guatemala"[23], el cual expresa que las personas usuarias de internet en el país se habían duplicado en los últimos años, es decir, a partir de 2002. Por otro lado, el informe de la Superintendencia de Telecomunicaciones asegura que Guatemala cuenta con una infraestructura adecuada para el desarrollo de la industria de las TIC, pues tiene una industria de TIC en el sector de software que durante el año 2006 exportó $100 millones con un crecimiento superior al 30% con respecto al 2005 y el crecimiento de la industria del hardware y servicios.

De esta manera, en consonancia con los estándares internacionales, en 2011 la Asamblea General de las Naciones Unidas, en su "Informe para la promoción, protección y disfrute de los derechos humanos en internet"[24], declaró el acceso a internet como derecho humano fundamental altamente protegido. De acuerdo al artículo 46 de la Constitución Guatemalteca, en materia de derechos humanos, los tratados aceptados y ratificados por el país tienen preeminencia sobre el derecho interno. En consonancia con lo anterior, el artículo 44 de la Constitución Guatemalteca establece que "los derechos y garantías que otorga la Constitución no excluyen otros que, no figuren expresamente en ella, son inherentes a la persona humana [...]" por lo que, aunque Guatemala no ha ratificado ningún tratado que considere expresamente el acceso a internet como un derecho humano, el mismo podría ser considerado como un derecho inherente.

1.3. Criminalización de defensoras y defensores de derechos humanos

El derecho a defender derechos humanos es una garantía contenida en los convenios y tratados internacionales suscritos y ratificados por Guatemala, los cuales por mandato constitucional son parte del derecho interno. De manera que al defender los derechos humanos se actúa en el marco de la ley, y quien ejerce, defiende o promueve algún derecho humano es por naturaleza un defensor o defensora de derechos humanos.

Durante los años de guerra civil en Guatemala, el Estado estigmatizó a víctimas y organizaciones sociales, convirtiéndoles en objetivos legítimos de represión. Este adoctrinamiento sistemático ha dejado huellas profundas en el subconsciente de la sociedad guatemalteca. El miedo, el silencio, la apatía y la falta de interés en la esfera de participación política son algunas de las secuelas más relevantes que resultaron de la represión de muchos personas, y supone un obstáculo para la

23 Superintendencia de Telecomunicaciones, "Penetración y adopción de la Internet y de las tecnologías de la información y comunicaciones en Guatemala" (Guatemala, Superintendencia de Telecomunicaciones, 2007), http://www.sit.gob.gt/sit/docs/GUATE_CSM_FINAL.pdf (consultado 5 noviembre, 2015)

24 Relatoría Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, "Promoción, protección y disfrute de los derechos humanos en Internet", http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf (consultado 5 noviembre, 2015)

intervención activa de toda la ciudadanía en la construcción de la democracia.[25]

Dado que la criminalización impide poder abordar el origen y naturaleza del conflicto, pues en lugar de enfrentar los problemas sociales con soluciones políticas, se emprende persecución y sanción penal al convertir toda acción de oposición en un delito. Es decir, se convierte el conflicto social en un asunto exclusivamente de legalidad. La firma de los Acuerdos de Paz en 1996 en su momento representó para Guatemala la oportunidad de construir una sociedad basada en principios de equidad y de justicia, lamentablemente el gobierno de Álvaro Arzú desarrolló una agenda neoliberal en la que introdujo herramientas legales que, hasta la fecha, han permitido la criminalización de los movimientos sociales.[26] Asimismo, entre 2005 y 2009 llegaron al poder Álvaro Colóm y Óscar Berger quienes impulsaron leyes como la Ley Contra la Delincuencia Organizada[27] y Ley de la Dirección General de Inteligencia civil[28], que propician la criminalización hacia activistas de derechos humanos.

En 2005, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) firmó un acuerdo con el Gobierno de Guatemala para el establecimiento de una oficina en el país, cuya función principal es observar la situación de los derechos humanos y proveer asistencia técnica a las instituciones del Estado y a la sociedad civil[29]. En su informe anual sobre las actividades de su oficina en Guatemala de 2013, la ACNUDH sigue reportando agresiones hacia la sociedad civil organizada.

Siendo Guatemala una democracia relativamente joven, caracterizada por altos niveles de corrupción e impunidad, actualmente se aprecia una creciente dinámica de privatización de la seguridad, mediante empresas privadas y comerciales. Paralelo al aparato de vigilancia montado por el binomio Estado-empresa privada, se encuentra la sistematización de las tecnologías. Es decir, el desarrollo de capacidades tecnológicas para manipular y monitorear la información aumentando las restricciones en las (tele)comunicaciones, potenciando la vigilancia e invadiendo la privacidad de las personas. La *nueva* vigilancia social se define como el control mediante la utilización de medios tecnológicos para extraer datos personales[30]. Específicamente hablando, la *cibervigilancia* se define como el

25 Comisión para el Esclarecimiento Histórico, G*uatemala Memoria del Silencio* (Guatemala: Programa de Naciones Unidas para el Desarrollo, 1999), 33.

26 UDEFEGUA, "Criminalización en contra de Defensores y Defensoras de Derechos Humanos" (Guatemala, 2009), 7.

27 Ver: http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2009/pdfs/decretos/D023-2009.pdf

28 Ver: http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2005/pdfs/decretos/D071-2005.pdf

29 Naciones Unidas Guatemala, "Mandato OACNUDH", (Guatemala: Naciones Unidas, 2005), http://www.onu.org.gt/contenido.php?ctg=1404-1399-1338-oacnudh (consultado 5 noviembre, 2015)

30 Gary T. Marx. "Encyclopedia of Social Theory". (S.l.: Surveillance and Society, 2005), http://web.mit.edu/gtmarx/www/surandsoc.html (consultado 5 noviembre, 2015)

monitoreo, intercepción, recolección y retención de datos (y metadatos[31]) de la información que ha sido comunicada, transmitida o generada a través de las redes de comunicación[32].

El gobierno de Otto Pérez Molina, líder militar durante la guerra civil, ex director de inteligencia vinculado a los crímenes de lesa humanidad de la década de 1980 y signatario de los acuerdos de paz, sorprendió a la ciudadanía auto convocada cuando durante una manifestación pacífica en la ciudad capital que exigía la renuncia de la vice presidenta Roxana Baldetti, procesada por estar involucrada en una red de corrupción aduanera[33], utilizó cámaras de alta definición y *Drones* para la identificación de rostros[34]. El uso de todo ese equipo de vigilancia de alta calidad es un llamado de alerta y queda confirmado que el gobierno guatemalteco cuenta con la tecnología necesaria para realizar prácticas que pueden vulnerar el derecho a la privacidad, criminalizando los esfuerzos de la ciudadanía que busca construir democracia. La criminalización evade abordar el origen y naturaleza del conflicto al convertir toda acción política en un delito.

Bajo este escenario, es importante resaltar que las movilizaciones pacíficas contra diversos casos de corrupción que han tenido lugar durante 2015, que contó con la participación de casi todos los sectores de la sociedad y que logró la salida del presidente Otto Pérez Molina, deja entrever que el pueblo guatemalteco está rompiendo, sin duda, el miedo y el silencio colectivo. Durante este levantamiento popular, denominado por muchos medios de comunicación internacionales como la primavera guatemalteca, se incrementaron los casos de criminalización hacia activistas de derechos humanos: operativos policiales, persecución, vigilancia, etc.[35]

31 Los metadatos son los datos de los datos. Por ejemplo, es toda aquella información referida a la identificación del número, la fecha, el tiempo de conversación o la localización de la llamada.

32 Privacy International, "What is the communications surveillance?", (Londres, Privacy International, s.f.), https://www.privacyinternational.org/?q=node/10 (consultado 5 noviembre, 2015)

33 "El escándalo aduanero que forzó la renuncia de la vicepresidenta de Guatemala, Roxana Baldetti", *BBC*, 2015, http://www.bbc.co.uk/mundo/noticias/2015/05/150507_guatemala_corrupcion_escandalo_vicepresidenta_baldetti_jp (consultado 5 noviembre, 2015)

34 Centro de Medio Independientes. "Las fotografías de una marcha histórica", (Guatemala, CMI, 2015), http://cmiguate.org/las-fotografias-de-una-marcha-historica-renunciaya/ (consultado 5 noviembre, 2015)

35 Marisol Garcés. "Criminalización de comunidades indígenas Kaqchikeles de San Juan Sacatepéquez", (Guatemala, Guatemala Comunitaria, 2015), http://guatemalacomunitaria.periodismohumano.com/2015/06/15/criminalizacion-de-comunidades-indigenas-kaqchikeles-de-san-juan-sacatepequez/ (consultado 5 noviembre, 2015)

2. Marco legal nacional

2.1. Tratados internacionales

2.1.1. Fuerza normativa de los tratados internacionales en materia de derechos humanos que pueden ser afectados por la vigilancia de las comunicaciones

Los tratados internacionales aceptados y ratificados por Guatemala en materia de derechos humanos tienen preeminencia sobre el derecho interno, de acuerdo al artículo 46[36] de la Constitución Política de la República de Guatemala[37]. De esta manera, aquellos derechos inherentes a la persona humana, aunque no se encuentren regulados en la Constitución, están protegidos por ella[38]. Y, debido a ello, Guatemala tiene la obligación de normar sus relaciones con otros Estados de conformidad con prácticas internacionales y al respeto y defensa de los derechos humanos[39].

Por si lo anterior fuese poco, la Corte[40] de Constitucionalidad[41] en 2011[42] admitió expresamente el bloque de constitucionalidad basándose en los artículos citados anteriormente, aunque ya había hecho referencia al mismo en 1990, 1997 y 2007.[43] Por medio del bloque de constitucionalidad aquellas normas y principios que no forman parte de la Constitución guatemalteca, han sido integradas por otras vías a la Constitución y sirven para el control de constitucionalidad de leyes, lo cual ya es doctrina legal[44] obligatoria para los tribunales.

36 Guatemala "Constitución Política de la República de Guatemala" Asamblea Nacional Constituyente (1985), artículo 46, título I, capítulo II. "Preeminencia del Derecho Internacional. Se establece el principio general de que en materia de derechos humanos, los tratados y convenciones aceptados y ratificados por Guatemala, tienen preeminencia sobre el derecho interno."

37 Constitución Política de la República de Guatemala, en lo subsiguiente "Constitución".

38 Guatemala "Constitución Política de la República de Guatemala" Asamblea Nacional Constituyente (1985), artículo 44, título I, capítulo II. "Derechos inherentes a la persona humana. Los derechos y garantías que otorga la Constitución no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana."

39 Guatemala "Constitución Política de la República de Guatemala" Asamblea Nacional Constituyente (1985), artículo 149, título III, capítulo III. "De las relaciones internacionales. Guatemala normará sus relaciones con otros Estados, de conformidad con los principios, reglas y prácticas internacionales con el propósito de contribuir al (...) respeto y defensa de los derechos humanos, (...)."

40 Corte de Constitucionalidad, en lo subsiguiente Corte o CC.

41 La Corte de Constitucionalidad de acuerdo al artículo 268 de la Constitución tiene como "función esencial" la "defensa del orden constitucional", y es la máxima autoridad en el tema Constitucional.

42 Corte de Constitucionalidad. Inconstitucionalidad general parcial, 2012, http://www.cc.gob.gt/jornadas/JornadasDocs/Contenido/1822-2011.pdf (consultado: 5 noviembre, 2015)

43 Corte de Constitucionalidad. Inconstitucionalidad general parcial. Expedientes 90-90, 159-97, 3004-2007 y 3878-2007, http://www.cc.gob.gt/ (consultado: 5 noviembre, 2015)

44 Guatemala "Ley de Amparo, Exhibición Personal y de Constitucionalidad" Asamblea Nacional Constituyente (1986), artículo 43, http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2006/pdfs/normativa/D001-86.pdf (consultado: 5 noviembre, 2015)

2.1.2. Tratados en materia de Derechos Humanos ratificados por Guatemala que contienen una protección al Derecho a la privacidad

Desde 1978, Guatemala ratificó[45] la Convención Americana sobre Derechos Humanos[46], y en 1992[47] también ratificó el Pacto Internacional de Derechos Civiles y Políticos[48]. Por otro lado, la jurisprudencia de la Corte Interamericana de Derechos Humanos ha señalado que las conversaciones telefónicas[49] y todo el proceso de comunicación[50] se encuentra protegido por la misma Convención. Estas normas y jurisprudencia de tratados internacionales en materia de Derechos Humanos, pueden ser utilizadas por la ciudadanía guatemalteca como herramientas para exigir el cumplimiento de su derecho a la privacidad, a la luz de la doctrina citada anteriormente sobre el bloque de constitucionalidad.

2.2. Constitución Política de la República de Guatemala

2.2.1. Vigilancia

2.2.1.1. Salvaguardas constitucionales del derecho a la privacidad en el contexto de la vigilancia de las comunicaciones

a) Derecho a la intimidad

La Constitución de la República de Guatemala, aunque no regula expresamente el derecho a la privacidad, contiene varias disposiciones que garantizan este derecho. Entre estos artículos se puede mencionar el artículo 24 que protege la inviolabilidad de correspondencia, documentos y libros; el artículo 25, que establece la obligación de guardar respeto a la dignidad, intimidad y decoro de las personas ante los registros personales; y el artículo 23 que regula la inviolabilidad de la vivienda, el cual es un derecho constitucional desde la Constitución Federal de Centroamérica y se le considera derivado del derecho a la intimidad y dignidad de la persona. Por si lo anterior fuese poco, el artículo

45 Guatemala ratificó la Convención Americana sobre Derechos Humanos el 27 de abril de 1978.

46 OEA "Convención Americana de Derechos Humanos" (1969), artículo 11, numeral 2o, Capítulo II, Derechos Civiles y Políticos, http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm (consultado: 6 noviembre, 2015) La Convención Americana de Derechos Humanos regula en el artículo 11, numeral 2o, el derecho a la privacidad: *" (…) 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."* (el énfasis es agregado)

47 Guatemala "Convenio Pacto Internacional Derechos Civiles y Políticos" (1992), decreto 9-92, http://www.iadb.org/Research/legislacionindigena/leyn/docs/GUA-Decreto09-1992-Convenio-Drs-CivilesyPoliticos[1].pdf (consultado: 6 noviembre, 2015)

48 Naciones Unidas "Pacto Internacional de Derechos Civiles y Políticos" (1966), artículo 17, numerales 1 y 2, http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx (consultado: 6 noviembre, 2015) "1. 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. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

49 Corte Interamericana de Derechos Humanos. Caso Tristán Donoso vs. Panamá. (Costa Rica, CorteIDH, 2009), párrafos 55 y 56, http://www.corteidh.or.cr/docs/casos/expedientes/sap6.pdf (consultado: 6 noviembre, 2015)

50 Corte Interamericana de Derechos Humanos. Escher y otros vs. Brasil. (Costa Rica, CorteIDH, 2009), párrafo 114, http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf (consultado: 6 noviembre, 2015)

44 del texto constitucional incorpora aquellos derechos que son inherentes a la persona humana, entre los cuales evidentemente se encuentra el derecho a la intimidad. En este sentido, la Corte de Constitucionalidad ha expresado que en lo que concierne a la intimidad, el elemento central de protección es la vida privada de la persona, es decir, el respeto de ese conjunto de sucesos y circunstancias que constituyen la vida personal y que deben mantenerse reservados del público, salvo que la persona consienta lo contrario. Y agrega que la protección a este derecho se da para impedir injerencias e intromisiones arbitrarias o ilegales en la vida privada de la persona[51].

En el ámbito internacional varios documentos han recogido el derecho a la intimidad. El artículo 12 de la Declaración Universal de Derechos Humanos señala que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. En el mismo sentido lo han hecho el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y el artículo 11 de la Convención Americana sobre Derechos Humanos, ambas ratificadas por Guatemala, por lo que pueden invocarse a la luz de la doctrina del bloque de constitucionalidad.

b) Inviolabilidad de las comunicaciones

La Constitución guatemalteca protege el derecho a la privacidad y reconoce al Estado como responsable de la consolidación del régimen de legalidad, seguridad y justicia, así como la necesidad de impulsar la plena vigencia de los derechos humanos dentro de un orden institucional donde gobernados y gobernantes procedan con absoluto apego al derecho; asimismo, reconoce expresamente el derecho a la privacidad de las comunicaciones y documentos personales[52]. La protección constitucional al derecho a la privacidad es una regulación con dimensión positiva, es decir, protege el derecho enunciando su contenido en sentido positivo.

Se ajusta a esta pauta interpretativa la sentencia de 2007[53] de la Corte de Constitucionalidad que dice que el derecho a la inviolabilidad de la correspondencia es uno de los derechos humanos que protegen la intimidad de la persona, es un derecho personalísimo que permite proteger a las personas de otras turbaciones a su vida privada, y únicamente puede estar limitado por necesidades sociales e interés público.

La Ley del Organismo Judicial[54] menciona que los pasajes de las normas se podrán aclarar atendiendo a la historia fidedigna de su institución, de esta manera, la Corte de Constitucionalidad se ha valido de

51 Corte de Constitucionalidad. Inconstitucionalidad General Total, expediente 1201-2006.

52 Guatemala "Constitución Política de la República de Guatemala" Asamblea Nacional Constituyente (1985), artículo 24, título II, capítulo I.

53 Corte de Constitucionalidad. Inconstitucionalidad General Parcial, expediente 2622-2006, http://vlex.com/vid/-423703874 (consultado: 6 noviembre, 2015)

54 Guatemala "Ley del Organismo Judicial" Congreso de la República de Guatemala (1989), artículo 10, https://www.rgp.org.gt/docs/legislacion_registral/Ley%20del%20Organismo%20Judicial.pdf (consultado: 6 noviembre, 2015)

esta interpretación para determinar la finalidad y el espíritu de una norma constitucional, por lo que deviene necesario acudir a la historia fidedigna de la institución para indagar el sentido del derecho que ahora nos ocupa. En más de una sentencia,[55] la Corte de Constitucionalidad ha dicho que para el análisis de la historia fidedigna de la institución se puede acudir a los cuerpos legales anteriores que la contuvieron.

El derecho a la privacidad se reconoció desde la Constitución Federal de 1823, cuando se incluyó en el artículo una disposición relativa a la correspondencia[56]. Este artículo fue recogido nuevamente en la Constitución de la República Federal de Centroamérica, dada por la Asamblea Nacional Constituyente el 22 de noviembre de 1824 en su artículo 176. El mismo contenido del artículo se mantuvo con las reformas a la Constitución Federal de Centroamérica, decretadas en 1835, en el artículo 182.

Los artículos citados recogían el principio que los documentos y comunicaciones de las personas son privadas, y establecía claramente las limitaciones (tumulto, rebelión o ataque con fuerza armada) por las cuales se podía autorizar una injerencia al derecho a la privacidad. Sin embargo, fue hasta 1879 cuando la Constitución incorporó dos innovaciones fundamentales con respecto a la regulación del derecho a la privacidad, ya que por primera vez se reconoció expresamente que los documentos y la correspondencia de las personas es inviolable, y se estableció que la única limitación que admite este derecho es por medio de juez competente, cumpliendo con los procedimientos que establezca la ley[57].

La reforma a la Constitución de la República decretada en 1921 modificó el artículo[58] que contenía la protección al derecho a la privacidad. Esta modificación a la protección del derecho a la privacidad introduce por primera vez una sanción a aquellos documentos que no son obtenidos conforme las formalidades legales: los mismos no producen fe en juicio, y añade la prohibición de interceptar los documentos privados.

Por su parte, la Constitución Política de la República Federal de Centroamérica de 1921 incorporó regulaciones que protegen el derecho a la privacidad. De esta manera, se establece por primera vez una distinción entre la correspondencia epistolar y telegráfica y la correspondencia particular.

55 Corte de Constitucionalidad. Inconstitucionalidad general parcial, expedientes 113-92, 306-92, y 1089-2003.

56 Guatemala "Constitución Política de la República de Guatemala" Asamblea Nacional Constituyente (1983). "No podrán sino en el caso de tumulto, rebelión o ataque con fuerza armada a las autoridades constituidas (…) 3. Dispensar las formalidades sagradas de la ley, para allanar la casa de algún ciudadano, registrar su correspondencia privada (...)"

57 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."

58 Guatemala "Constitución Política", artículo 37. "La correspondencia de toda persona y sus papeles y libros privados son inviolables y no podrán ser interceptados. Los que fueren substraídos no harán fe en juicio. Sólo podrán ser ocupados en virtud de auto de Juez y competente y con las formalidades legales."

Aunque aparentemente estas regulaciones solamente hacen referencia a la correspondencia epistolar y telegráfica, la prohibición dirigida al Poder Ejecutivo de no abrir y detener este tipo de correspondencia se entiende que se extiende también a la correspondencia particular[59].

En 1927, se hace una nueva reforma a la Constitución de la República en la cual se modifica el artículo 37 que decreta la protección al derecho a la privacidad y elimina la frase "no podrán ser interceptados", lo cual representa un inminente retroceso a la protección de este derecho. Por su parte, la reforma a la Constitución de 1927, decretada en 1935, introduce la distinción entre los papeles privados y los papeles hacendarios, y establece que cuando sea limitado el derecho de privacidad siempre deberá estar presente la persona interesada, su mandatario o uno de sus parientes. Lo anterior se mantiene hasta la Constitución vigente[60]. La reforma de 1945 incluyó en el artículo 35 el derecho a la privacidad, que únicamente parafraseó el artículo de la reforma de 1935.

La Constitución de 1956 amplió la regulación a las limitaciones para el caso de documentos relacionados con impuestos al indicar en el artículo 55 que las oficinas que ejerzan la fiscalización de los impuestos podían, por orden escrita y para casos concretos, disponer la revisión de papeles y libros privados que se relacionen con el pago de los impuestos. Además, prohíbe revelar la cuantía de los montos de donde proceden los impuestos.[61] Diez años más tarde, la Constitución decretada el 15 de septiembre de 1965 mantuvo la protección al derecho a la privacidad con prácticamente la misma redacción de la Constitución de 1956.

Del análisis por el recorrido histórico de la Constitución de la República de Guatemala ante la protección al derecho a la privacidad, se concluye que a lo largo de la historia de la institución de este derecho se advierte que aquella ha venido designando una sólida protección constitucional al derecho de la privacidad que data desde la Constitución Federal de 1823, la cual se consolidó en 1879 con la prohibición clara y expresa de prohibir violar la correspondencia y los documentos privados de las personas, y estableciendo que este derecho solamente puede ser limitado por un juez competente y cumpliendo las formalidades legales que la ley establezca. Este derecho se reconoció en todas las constituciones de Guatemala, hasta concluir con la regulación constitucional actual que amplía su protección a cualquier

59 Costa Rica "Constitución Política de la República Federal de Centroamérica". (1921), artículos 53, 54. "Artículo 53. Son inviolables la correspondencia epistolar, la telegráfica y los papeles privados. En ningún caso el Poder Ejecutivo, ni sus agentes, podrán sustraer, abrir ni detener la correspondencia epistolar o la telegráfica. La sustraída de las estafetas o de cualquier otro lugar no hace fe en juicio.". "Artículo 54. La correspondencia particular, papeles y libros privados, sólo podrán ocuparse o inspeccionarse en virtud de orden de autoridad competente en los casos determinados por la ley."

60 Guatemala "Constitución Política", artículo 37.

61 Guatemala "Constitución Política", artículo 55. "Artículo 55. La correspondencia de toda persona y sus papeles y libros privados son inviolables. Solo podrán ser ocupados o revisados en virtud de auto de Juez competente y con las formalidades legales. Las oficinas que ejerzan la fiscalización de los impuestos podrán también por orden escrita, y para casos concretos, disponer la revisión de papeles y libros privados que se relacionen con el pago de los impuestos, debiéndose practicar en todo caso la ocupación o revisión, en presencia del interesado, o de su mandatario y en defecto de éstos, ante uno de sus parientes mayor de edad, o de dos testigos honorables vecinos del lugar. Es punible revelar la cuantía de la fuente de que procedan los impuestos, así como las utilidades, pérdidas, costos o cualquier otro dato comercial o referente a las empresas tributarias o a su contabilidad. Los documentos que fueren sustraídos y la correspondencia violada no hará fe en juicio."

tipo de comunicación actual o que exista en el futuro, cuando se refiere a "otros productos de la tecnología moderna"

c) Derecho a la autodeterminación informativa

Respecto a este derecho, la Constitución indica en el artículo 31 que toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. La Constitución de Guatemala no incluye una regulación expresa a la autodeterminación informativa; sin embargo, la Constitución propugna el reconocimiento de la dignidad humana como su fundamento, y existen otros derechos que también pueden ser invocados por medio de los artículos 44 y 46 de la misma[62].

Respecto a los derechos a la intimidad, a la vida privada y a la autodeterminación informativa, la Corte de Constitucionalidad se expresó en 2011 contra la comercialización de datos al considerar ilegal la recolección, el procesamiento y la comercialización de datos personales sin el consentimiento del titular de los datos a través de un medio en particular difundido en internet[63].

En 2015, la Corte de Constitucionalidad estableció que los avances de la tecnología informática generan una dificultad en cuanto a proteger la intimidad y privacidad de una persona individual[64]. La solución a esta problemática ha sido reconocer el derecho a la autodeterminación informativa de las personas, que permite establecer el debido control sobre los datos referidos a su persona y, a su vez, le garantiza la tutela correspondiente ante un uso indebido, es decir, sin su autorización y con fines de lucro por parte de un tercero de todos aquellos datos personales susceptibles de tratamiento automatizado, con los cuales se integra una información identificable de una persona. Dicha información cuando es transmitida a terceras personas sin los pertinentes controles que permiten su veracidad o actualización, puede causar afectación del entorno personal, social o profesional de esa persona, causando con ello agravio de sus derechos a la intimidad y al honor[65].

En la sentencia arriba citada, la Corte de Constitucionalidad define lo que se considera como dato personal, establece que la información debe ser proporcionada voluntariamente por la persona, y debe permitir el derecho de actualizar sus datos, rectificación de la información errónea, derecho de reserva o confidencialidad de cierta información, y el derecho a la exclusión de determinada información que pueda considerarse sensible para el interesado. Por lo anterior, aunque en Guatemala

62 Guatemala "Constitución Política", artículo 31, 44 y 46.

63 Corte de Constitucionalidad. Apelación de sentencia de amparo, expediente 863-2011, http://www.cc.gob.gt/jornadas/Jornadas-Docs/Contenido/863-2011.pdf (consultado: 6 noviembre, 2015)

64 Corte de Constitucionalidad. Expediente 3552-2014, http://www.cc.gob.gt/DocumentosCC/ResolucionesIntPub/3552-2014.pdf (consultado: 6 noviembre, 2015)

65 Corte de Constitucionalidad. Apelación de sentencia de amparo, expediente 863-2011, http://www.cc.gob.gt/jornadas/Jornadas-Docs/Contenido/863-2011.pdf (consultado: 6 noviembre, 2015)

no existe una ley de protección de datos personales, la misma debe de proteger como mínimo estos aspectos antes mencionados. Así lo ha expresado la Corte de Constitucionalidad en varias sentencias[66].

Además, la Corte de Constitucionalidad ha señalado[67] los requisitos que deben cumplir las personas que realicen actividades de comercialización, siendo estas: (i) Los datos deben obtenerse de forma legítima y voluntaria por parte de aquel cuyos datos vayan a ser objeto de comercialización y con una finalidad definida, es decir, no se permite la captación de bases de datos sin la autorización previa de la persona; (ii) Previo a la utilización de esos datos personales, se debe tener el consentimiento de la persona interesada, con un propósito compatible con el fin para el cual se obtuvo; (iii) La utilización de los mismos conlleva los controles adecuados que permitan determinar la veracidad y actualización de los mismos, y un amplio derecho a la rectificación.

Respecto a este derecho, en su informe sobre el Derecho a la Privacidad en la Era Digital[68] publicado en 2014, la Alta Comisionada de Naciones Unidas Derechos Humanos, Navi Pillay, expresa que la recolección masiva de información personal es ilegal bajo el derecho internacional de los Derechos Humanos. Entre otras razones, porque dicha recolección, aún bajo el supuesto que esté destinada a proteger otros bienes como la seguridad o si es que dichos datos no son utilizados, no cumple con el test de necesidad ni de proporcionalidad.

d) Otros derechos protegidos por la Constitución frente a la vigilancia estatal

Ciertamente, el libre ejercicio del derecho a la privacidad se ve directamente afectado dentro de un contexto de prácticas sistematizadas de vigilancia masiva. La vigilancia estatal vulnera, además de la penalización de formas legítimas de expresión y otras libertades fundamentales, otros derechos humanos como el derecho a la libertad de expresión y el derecho de asociación y reunión, protegidos por la Constitución guatemalteca en los artículos 33, 34 y 35 respectivamente[69].

El libre ejercicio del derecho a la libertad de expresión a través de internet, es un tema cuyo interés ha evolucionado al ritmo del desarrollo tecnológico, mismo que permite a las personas en todo el mundo utilizar las nuevas tecnologías de la información y de la comunicación. De hecho, en 2011 el entonces Relator Especial de las Naciones Unidad sobre la promoción y protección del derecho

66 Corte de Constitucionalidad. Expediente 1356-2006; Expediente 131-2012; Expediente 1201-2006; Expediente 863-2011.

67 Corte de Constitucionalidad. Expediente 863-2011; Expediente 1356-2006.

68 OACNUDH. Derecho a la Privacidad en la Era Digital. (Naciones Unidas, Oficina Alta Comisionada de Naciones Unidas para Derechos Humanos, 2014). http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf (consultado: 6 noviembre, 2015)

69 Guatemala "Constitución Política", artículos 33 (primeras dos oraciones), 34 (primera oración) y 35 (primera oración). "Artículo 33. Derecho de reunión y manifestación. Se reconoce el derecho de reunión pacífica y sin armas. Los derechos de reunión y de manifestación pública no pueden ser restringidos, disminuidos o coartados; y la ley los regulará con el único objeto de garantizar el orden público. (...)"; "Artículo 34. Derecho de asociación. Se reconoce el derecho de libre asociación. (...)"; y, "Artículo 35. Libertad de emisión del pensamiento. Es libre la emisión del pensamiento por cualesquiera medios de difusión, sin censura ni licencia previa. (...)"

de libertad de opinión y expresión, Frank La Rue, declaró el acceso a internet como un derecho humano[70] al considerar la tecnología como una herramienta facilitadora de otros derechos, cuyo uso se ve condicionado al libre ejercicio de los derechos a la libertad de expresión y el derecho a la privacidad ya que están interrelacionados[71], canalizando además otros derechos como el derecho a ejercer democracia participativa e inclusiva.

Tomando en consideración lo anterior, se evidencia que la vigilancia sistemática y masiva representa una disminución y una restricción de las libertades fundamentales de manera desproporcionada. El derecho al libre acceso a internet se fundamenta en tiempos en los que la red de redes y los diversos medios digitales adquieren tal relevancia que no pueden imaginarse fuera de la tutela jurídica, y menos aún de la que provee el sistema internacional. La vigilancia por parte del Estado interfiere con el derecho la privacidad y la libertad de expresión, dado que en muchos casos esos derechos solo florecerán cuando las personas se sientan seguras que las comunicaciones y asociaciones puedan permanecer libres de vigilancia gubernamental. Cuando el gobierno accede a los datos y metadatos de las comunicaciones por teléfono o internet, las personas están menos dispuestas a expresarse sobre temas delicados o temas políticos.

Es por ello que los Estados no pueden garantizar que las personas sean capaces de expresarse libremente sin respetar, proteger y promover el derecho a la privacidad de las comunicaciones y la libertad de expresión. En consecuencia, los Estados deben considerar las implicaciones de ambos derechos al autorizar la vigilancia y otras técnicas que afectan las comunicaciones privadas. Sobre las múltiples medidas adoptadas por los Estados para impedir o restringir el flujo de información en línea, el Relator señala la inadecuada protección del derecho a la privacidad en internet.

Por otro lado, el Relator Especial sobre el derecho a la libertad de reunión y asociación pacíficas valora el papel determinante que ha tenido internet para facilitar la participación activa de la ciudadanía en la construcción de sociedades democráticas, y también reconoce la posibilidad de ejercer los derechos a la libertad de reunión y de asociación pacífica a través de la red de redes[72].

70 OACNUDH. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de opinión y expresión.* (Naciones Unidas, Oficina de la Alta Comisionada de Derechos Humanos, 2011). http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (consultado: 6 noviembre, 2015)

71 OACNUDH. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de opinión y expresión.* (Naciones Unidas, Oficina de la Alta Comisionada de Derechos Humanos, 2013). http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (consultado: 6 noviembre, 2015)

72 OACNUDH. *Informe del Relator especial sobre el derecho a la libertad de reunión y asociación pacíficas.(*Naciones Unidas, Oficina de la Alta Comisionada de Derechos Humanos, 2012). http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-27_sp.pdf (consultado: 6 noviembre, 2015)

2.2.1.2. Limitaciones constitucionales al derecho a la privacidad en el contexto de la vigilancia de las comunicaciones

El derecho a la privacidad puede ser limitado. La Constitución establece que únicamente pueden revisarse la correspondencia, documentos y libros de la persona en virtud de resolución firme dictada por un juez competente y cumpliendo con las formalidades legales. Otra limitación son los libros, documentos y archivos relacionados con el pago de impuestos, los cuales pueden ser revisados por el Estado de conformidad con la ley[73].

Ante estas restricciones, la Corte de Constitucionalidad ha dicho que el derecho a la privacidad únicamente puede ser limitado por razones de interés público y por necesidades sociales[74]. Realizando una interpretación más extensa sobre las limitaciones a este, la Corte de Constitucionalidad contrastó el derecho a la intimidad, específicamente al secreto de la correspondencia y las comunicaciones telefónicas y otros productos de la tecnología moderna, con el deber del Estado de garantizarle a los habitantes la vida, la libertad, la justicia, la seguridad, la paz, integridad y el desarrollo integral de la persona, contenido en los artículos constitucionales 2 y 3[75]. En esta ocasión la Corte dijo que el derecho a la intimidad admite acotaciones razonables, es decir que no pueden destruir o alterar el derecho limitado, el medio escogido en la limitación debe ser proporcional a la naturaleza del derecho que se condiciona, el medio escogido para alcanzar un fin legítimo debe ser también proporcional a ese fin y, el medio elegido no puede ser más gravoso u oneroso para el derecho que soporta la limitación. Para el caso específico de las escuchas telefónicas reguladas en la Ley contra la Delincuencia Organizada, la Corte consideró que por requerirse una autorización de la Sala de la Corte de Apelaciones y mantenerse bajo reserva la información, no se viola el orden constitucional.

De la regulación constitucional y de la jurisprudencia de la Corte de Constitucionalidad se puede concluir que: (i) En Guatemala se reconoce la inviolabilidad de la correspondencia, documentos y comunicaciones de toda persona; (ii) Solamente se podrá vulnerar este derecho mediante una orden dictada por juez competente y con las formalidades legales; (iii) Se puede limitar este derecho por necesidades sociales e intereses públicos; (iv) La limitación al derecho a la privacidad no puede exceder el margen de lo razonable entre el medio que se utiliza y el fin legítimo que se persigue; (v) La información debe mantenerse bajo reserva, y (vi) Solamente las personas físicas gozan de intimidad, pudiendo la autoridad competente, mediante la ley, revisar los documentos pertinentes. Sin embargo, las personas físicas tienen derecho a que se les respete su privacidad y

73 Guatemala "Constitución Política", artículo 24.

74 Corte de Constitucionalidad. Inconstitucionalidad general parcial, expediente 2622-2006, http://vlex.com/vid/-423703874 (consultado: 6 noviembre, 2015)

75 Corte de Constitucionalidad. Inconstitucionalidad general, expediente 2837-2006, http://vlex.com/vid/-423784230 (consultado: 6 noviembre, 2015)

cuando exista una limitación a esta, se debe cumplir -por supuesto- con las formalidades legales que exige la ley.

Viendo en retrospectiva estas limitaciones, en 1999, la Corte de Constitucionalidad[76] señaló que el derecho a la privacidad es superior sobre el derecho a la libre emisión del pensamiento ya que la persona física tiene derecho inalienable e imprescriptible a su dignidad. La Corte de Constitucionalidad en esta ocasión analizó la inconstitucionalidad de una norma que le prohíbe a los medios de comunicación transmitir las ejecuciones de pena de muerte. Esta es una limitación a la libertad de expresión y la Corte le dio más importancia a la intimidad de la persona. Aunque la Corte de Constitucionalidad en esta ocasión señaló la superioridad de un derecho con respecto a otro, la doctrina moderna hace únicamente ponderaciones entre derechos.

2.2.1.3. Mecanismos de acceso a la justicia en el contexto de la vigilancia

La Constitución guatemalteca contiene una sólida protección a los derechos contenidos en ella[77]. Para la protección de los derechos constitucionales la Constitución instauró varias garantías constitucionales, entre ellas el amparo. Este procede cuando existe una amenaza a la violación de un derecho, restricción a un derecho o para restaurar el imperio de un derecho cuando ya se dio la violación[78]. En el mismo sentido, la Ley de Amparo, Exhibición Personal y de Constitucionalidad que regula el procedimiento del amparo[79], establece que la interpretación de esta ley será siempre en forma extensiva para procurar una mayor protección de los derechos humanos y el funcionamiento eficaz de las garantías y defensas del orden constitucional[80].

Para proteger todos los derechos constitucionales señalados en el apartado anterior, procede el amparo cuando existe una persona que considera que su derecho a la privacidad, en sus distintas manifestaciones, está siendo amenazado, restringido o ya fue violentado. Por otra parte, si una persona considera que alguna ley, reglamento o disposición de carácter general disminuye, tergiversa o violenta el derecho a la privacidad, puede presentar una inconstitucionalidad[81] ante la Corte de Constitucionalidad.

Aunque no existe ningún antecedente jurídico, se podría amparar como mecanismo de protección y se podría argumentar una violación al derecho de libre expresión como lo mencionan los reportes del sistema de derechos humanos.

76 Corte de Constitucionalidad, expediente 248-98, http://www.infile.com/leyes/visualizador_demo/index.php?id=42126 (consultado: 6 noviembre, 2015)
77 Guatemala “Constitución Política”, artículos263.
78 Guatemala “Constitución Política”, artículo 265.
79 Guatemala “Ley de Amparo, Exhibición Personal y de Constitucionalidad” Asamblea Nacional (1986), artículos 8.
80 Guatemala “Ley de Amparo, Exhibición Personal y de Constitucionalidad”, articulo 2.
81 Guatemala “Ley de Amparo, Exhibición Personal y de Constitucionalidad”, articulo 134.

Otro mecanismo que puede ser útil para proteger a las personas contra las violaciones de sus derechos humanos es presentar una denuncia ante la Procuraduría de los Derechos Humanos, que pueden posteriormente accionar legalmente en favor de ellos.

2.2.2. Anonimato y cifrado

El anonimato es definido como actuar o comunicarse sin utilizar o presentar la identidad propia. De esta manera se protege la determinación del nombre o identidad propios utilizando un nombre ficticio que no necesariamente se asocia con la identidad legal o habitual de una persona[82].

El cifrado es el proceso matemático de utilizar códigos y claves para comunicarnos de forma privada. A lo largo de la historia, las personas han utilizado métodos cada vez más sofisticados de cifrado.[83]

2.2.2.1. Salvaguardas constitucionales para la protección del cifrado y el anonimato

Ninguno de estos temas ha sido abordado por el Tribunal Constitucional guatemalteco. Sin embargo, la Constitución guatemalteca protege diversos derechos en los que se incluye la protección al anonimato y al cifrado, como se explicará a continuación.

a) Libertad de acción

La Constitución protege la libertad de acción[84], por lo que si no existe una limitación para el anonimato y el cifrado digital en la legislación, estos son permitidos. En Guatemala está prohibido el uso de capuchas, máscaras o elementos que oculten la identidad de las personas en lugares públicos o manifestaciones[85]; sin embargo, esta norma no es aplicable al anonimato digital. El cifrado para firmas electrónicas está permitido implícitamente en la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas[86] ya que menciona que en las comunicaciones electrónicas se puede utilizar la tecnología de criptografía asimétrica con clave pública y clave privada.

b) Libertad de expresión

La protección a la libre emisión del pensamiento es fuerte y defiende, entre otros, el libre acceso a las fuentes de información, el cual no puede ser limitado por ninguna autoridad[87]. Este libre acceso a las

82 Electronic Frontier Foundation, *Anonimato y cifrado.*(S.l., EFF, 2015), 3.

83 Electronic Frontier Foundation, *Anonimato y cifrado,* 37.

84 Guatemala "Constitución Política de la República de Guatemala" Asamblea Nacional Constituyente (1985), artículo 5.

85 Guatemala "Decreto 41-95" Congreso de la República (1995), artículo 1, http://old.congreso.gob.gt/archivos/decretos/1995/gtdcx41-1995.pdf (consultado 6 noviembre, 2015)

86 Guatemala "Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas" Congreso de la República de Guatemala (2008), artículos 46 y 47, http://www.redipd.es/legislacion/common/legislacion/guatemala/Acuerdo_47-2008_Firmas_Electronicas_Guatemala.pdf (consultado 6 noviembre, 2015)

87 Guatemala "Constitución Política", artículo 35; Guatemala "Ley de Emisión del Pensamiento" Congreso de la República de Guatemala (1985), artículo 5.

fuentes de información implica poder acceder a las mismas de forma anónima y así lo ha expresado la Relatoría de la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos[88]. Además de esto, implica garantizar el anonimato en línea para respetar la voluntad de las personas usuarias de internet de no revelar su identidad[89].

Y, aunque algunos gobiernos se muestran opresivos con el tema del anonimato en línea, existen razones legítimas para que las personas no quieran utilizar sus identidades reales en internet. De hecho, a lo largo de la historia, la buena disposición de las personas para involucrarse en debates sobre temas políticos siempre estuvo ligada a la posibilidad de hacerlo de forma anónima. Internet permite a las personas acceder a la información y participar en el debate público sin tener que revelar su verdadera identidad[90]. De esta manera, el anonimato posibilita la libertad de expresión en aquellos países donde se reprime fuertemente a la disidencia, instalando en el imaginario colectivo la idea de que si se es anónimo en internet es porque se está haciendo algo malo, como por ejemplo conspirar masivamente contra el gobierno y su política del pensamiento único. En definitiva, la doble moral juega a favor del veto a la libertad de opinión.

El actual Relator de libertad de expresión de Naciones Unidas, David Kaye, ha dicho en el 2015 que el cifrado y el anonimato son los principales vehículos para la seguridad en línea, proporcionando a las personas un medio para proteger su privacidad. El cifrado les da el poder de navegar, leer, desarrollar y compartir opiniones e información sin interferencias. También ayuda a periodistas, organizaciones de la sociedad civil, minorías étnicas o grupos religiosos, a las personas perseguidas debido a su orientación sexual o identidad de género, activistas, a la academia, artistas y otras personas que ejerzan el derecho a la libertad de expresión y opinión.[91]

El cifrado y el anonimato, y otros conceptos de seguridad además de estos, ofrecen la privacidad y la seguridad necesaria para poder ejercer el libre ejercicio del derecho a la libertad de opinión y de expresión en la era digital. Dicha garantía puede ser esencial para el ejercicio de otros derechos, incluidos los derechos económicos, la privacidad, el debido proceso, la libertad de reunión y de asociación pacíficas, y el derecho a la vida y la integridad corporal. Debido a su importancia para el derecho a la libertad de opinión y de expresión, las restricciones al cifrado y el anonimato deben ser estrictamente limitadas de acuerdo a los principios de legalidad, necesidad, proporcionalidad y legitimidad en el objetivo y debido

88 Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos., *Libertad de expresión e Internet. (*Organización de Estados Americanos y Open Society Foundations, s.f.), párrafo 109.

89 Electronic Frontier Foundation, *Anonimato y cifrado,* 1.

90 OACNUDH. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de opinión y expresión.* (Naciones Unidas, Oficina de la Alta Comisionada de Derechos Humanos, 2011), http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (consultado 6 noviembre, 2015)

91 OACNUDH. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de opinión y expresión.* (Naciones Unidas, Oficina de la Alta Comisionada de Derechos Humanos, 2015), http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc (consultado: 6 noviembre, 2015)

proceso.[92] Estos principios se explican más adelante dentro de este capítulo.

Se debe entender que el objetivo de los gobiernos no es el de vigilar a una o varias personas en específico, sino al conjunto de la sociedad en concreto, es decir, de forma colectiva.

En conclusión, en Guatemala, por la protección al derecho a la libertad de expresión, estaría protegido el uso del cifrado y el anonimato en línea.

c) Privacidad

La privacidad reconocida, entre otros, en el artículo 24 constitucional, garantiza el secreto de la correspondencia y las comunicaciones producto de la tecnología moderna, en concordancia con los tratados internacionales en materia de derechos humanos. Este derecho protege que la información contenida en las comunicaciones pueda ser cifrada si la persona así lo desea. Dicho de otra forma, la privacidad permite que las personas se expresen libremente y sin temor a represalias. Un ejemplo común a la violación a estos derechos es el requerir la identificación de los usuarios para el acceso a las comunicaciones, incluido los servicios de internet, ciber cafés o la telefonía móvil.[93] En la vida es común que las personas moderen sus posiciones o se autocensuren cuando están en presencia de personas desconocidas. De la misma forma actúan las personas cuando están siendo vigiladas.

d) Derechos inherentes a la persona humana

Desde que la Constitución reconoce que los derechos y garantías que otorga no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana, se podría afirmar que el cifrado y el anonimato son derechos protegidos por ella ya que son inherentes a la persona humana[94] y protegen otros que han sido reconocidos en tratados en materia de derechos humanos ratificados por Guatemala.

2.2.2.2. Mecanismos de acceso a la justicia en el contexto del cifrado y el anonimato a nivel constitucional

Desde el momento en que la Constitución interpretada de forma extensiva y en armonía con los tratados internacionales en materia de derechos humanos que regulan el tema protege el anonimato y el cifrado, ellos pueden ser protegidos cuando exista una amenaza a su violación o para restaurar el imperio de los mismos por medio del amparo[95].

92 OACNUDH. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de opinión y expresión.* (Naciones Unidas, Oficina de la Alta Comisionada de Derechos Humanos, 2015), http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc (consultado: 6 noviembre, 2015)

93 OACNUDH. *Informe del Relator Especial para la promoción y protección del derecho a la libertad de opinión y expresión.* (Naciones Unidas, Oficina de la Alta Comisionada de Derechos Humanos, 2013), 7, párrafo 24, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (consultado: 6 noviembre, 2015)

94 Guatemala "Constitución Política", artículo 44, primer párrafo.

95 Guatemala "Constitución Política", artículo 265; Ley de Amparo, Exhibición Personal y de Constitucionalidad.

2.3. Leyes, reglamentos y jurisprudencia

2.3.1. Vigilancia, cifrado y anonimato en leyes y reglamentos

2.3.1.1. Normas en materia penal

La normativa penal contiene normas que protegen y limitan el derecho a la privacidad.

a. Normativa penal que protege el derecho a la privacidad

El Código Penal[96] sanciona la violación, sustracción e interceptación de comunicaciones a cualquier persona que se apoderare de correspondencia sin previa orden de juez competente. Se exceptúa de estas disposiciones a los padres respecto a sus hijos menores de edad o los tutores respecto de las personas que tengan bajo su custodia o guardia. También prohíbe la revelación de secretos que las personas hayan conocido por su estado, oficio, empleo, profesión o arte, que ocasionare o pudiere ocasionar perjuicio, y sanciona a funcionarios y empleados públicos que revelen secretos, así como a quien acometiere a un conductor de correspondencia para interceptar o detener esta. Esto incluye, por supuesto, a periodistas en el ejercicio de su función.

b. Normativa penal que limita el derecho a la privacidad

El Código Procesal Penal[97] establece que se podrá ordenar la interceptación y el secuestro de la correspondencia (postal, telegráfica o teletipográfica) 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.

Por su parte, la Ley Contra la Delincuencia Organizada[98] establece que para evitar, interrumpir o investigar la comisión de delitos regulados en misma ley, podrá interceptarse, grabarse y reproducirse con autorización judicial comunicaciones orales, escritas, telefónicas, radiotelefónicas, informáticas y similares que utilicen el espectro electromecánico, así como cualesquiera de otra naturaleza que en el futuro existan. De esta manera, la Ley Contra la Delincuencia Organizada limita la interceptación de comunicaciones a cierto tipo de delitos y a que medie una autorización judicial. Sin embargo, es amplio con respecto al tipo de comunicaciones ya que señala que aplica a cualquiera que se utilice

96 Guatemala. Organismo Judicial, Código Penal de 1973, artículos 217, 218, 219, 220, 221, 222, 223 y 422, http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/lex/CodigoPenal.htm (consultado: 6 noviembre, 2015)

97 Guatemala. Organización de los Estados Americanos, Código Procesal Penal de 1992), artículos 203, 204, 205, http://www.cicad.oas.org/fortalecimiento_institucional/legislations/PDF/GT/decreto_congresional_51-92_codigo_procesal_penal.pdf (consultado: 6 noviembre, 2015)

98 Guatemala "Ley Control del Crimen Organizado" Ministerio de Gobernación (2006), artículo 18, 48.

en el espectro electromecánico, así como otras que existan en el futuro.

Contra este artículo fue presentada una acción de inconstitucionalidad, denegada por la Corte de Constitucionalidad al considerar que la garantía de secretividad de las comunicaciones se encuentra resguardada, ya que la norma ordinaria establece que para que se pueda realizar la escucha se debe poseer autorización de una Sala de la Corte de Apelaciones y que la misma se hará bajo reserva, cumpliéndose así con lo establecido por el artículo constitucional[99] que protege el derecho a la privacidad de las comunicaciones.

La solicitud para interceptar comunicaciones únicamente podrá hacerse por fiscales del Ministerio Público, y serán competentes para autorizar dicha interceptación los jueces de primera instancia del ramo penal, correspondiente a la circunscripción territorial donde se haya cometido o se pretenda cometer el delito por miembros de grupos delictivos organizados.[100] Mientras no exista persona ligada a proceso penal, no se tendrá acceso a las actuaciones realizadas por los agentes encubiertos ni a las interceptaciones de comunicaciones.

Es importante mencionar que de acuerdo a la referida ley, los fiscales deben justificar el uso de esta medida fundamentando su necesidad e idoneidad. Se entenderá que existe necesidad cuando en otros medios de investigación se demuestre que se estén utilizando los medios de comunicación establecidos en la presente ley. Se comprenderá que hay idoneidad del uso de la interceptación cuando se pueda determinar que la interceptación de las comunicaciones es eficaz para obtener elementos de investigación[101]. El juez que la autorice, por su parte, deberá en el auto judicial indicar la justificación, señalar el plazo por el que se autoriza la interceptación, y los nombres de las personas que serán afectadas con la medida[102].

Esta ley permite retener números de teléfonos, frecuencias y direcciones electrónicas, según corresponda, o cualesquiera otros datos que sean útiles para determinar el medio electrónico o informático que se pretende interceptar para la escucha, grabación o reproducción de la comunicación respectiva, así como nombres y otros datos que permitan identificar a la persona o personas que serán afectadas con la medida. Y, en los delitos en que esté en peligro la vida o la libertad personal, el Ministerio Público podrá presentar verbalmente la solicitud al juez competente quien resolverá en forma inmediata. Partiendo de este punto, como una ley restrictiva del derecho a la privacidad se reservan diligencias para identificar medidas discrecionales de autoridades o resoluciones del tribunal

99 Corte de Constitucionalidad, Inconstitucionalidad general, expediente 2837-2006, http://vlex.com/vid/-423784230 (consultado: 6 noviembre, 2015)

100 Guatemala "Ley Contra la Delincuencia Organizada" Congreso de la República de Guatemala (2009), artículo 49 y 52, http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2009/pdfs/decretos/D023-2009.pdf (consultado: 6 noviembre, 2015)

101 Guatemala "Ley Contra la Delincuencia Organizada", artículo 51.

102 Guatemala "Ley Contra la Delincuencia Organizada" , artículo 53.

competente para restringir este derecho.

De esta manera, se puede asegurar que la legislación guatemalteca no permite el espionaje telefónico sin orden judicial, es decir, es inconstitucional y está penado por la ley. Aún así, las escuchas telefónicas en Guatemala son una práctica reiterada desde hace más de 35 años. La práctica ilegal de las escuchas telefónicas son controladas desde la oficina de control de inteligencia militar[103].

2.3.1.2. Normas sobre inteligencia y contrainteligencia

La Ley de la Dirección General de Inteligencia Civil (DIGICI) permite limitaciones al derecho a la privacidad, específicamente en el artículo 4 cuando dice que en los casos donde existan indicios de actividades del crimen organizado con énfasis en la narcoactividad y la delincuencia común en las que hubiera peligro para la vida, la integridad física, la libertad y los bienes de personas determinadas, el Ministerio Público puede solicitar como medida de urgencia la autorización de una Sala de la Corte de Apelaciones para intervenir temporalmente comunicaciones telefónicas y radiofónicas, electrónicas y similares.

Esta ley fue aprobada con anterioridad a la Ley contra la Delincuencia Organizada y mantiene los mismos principios: (i) La solicitud únicamente la puede hacer el Ministerio Público; (ii) El Organismo Judicial, en este caso por conducto de una Sala de la Corte de Apelaciones, autoriza la medida, y (iii) La información se recibe bajo reserva de confidencialidad. Sin embargo, la única diferencia es que esta información no podrá ser utilizada como prueba en contra de persona alguna, esto por el carácter preventivo de la información de inteligencia procesada por la Dirección General de Inteligencia Civil.

Por otra parte, la Ley de la Dirección General de Inteligencia Civil[104] señala en su artículo 5 que "serán confidenciales los datos suministrados por particulares bajo garantía de confidencia". Se puede afirmar que no se puede realizar vigilancia sin una orden judicial.

2.3.1.3. Normas en el sector de telecomunicaciones

En la Ley General de Telecomunicaciones[105] no se regula nada con respecto a las interceptaciones telefónicas. Sin embargo, de la regulación del Código Procesal Penal, la Ley Contra la Delincuencia Organizada y la Ley de la Dirección General de Inteligencia Civil, se infiere que las empresas de telecomunicaciones están obligadas a colaborar en la interceptación de comunicaciones. La orden de interceptación de comunicaciones dictada por un juez en el ejercicio legítimo de sus atribuciones

103 Washington Office on Latino America. *Poderes Ocultos: Grupos ilegales armados en la Guatemala post conflicto y las fuerzas detrás de ellos.* (Guatemala, Washington Office on Latino America, s.f.), http://www.wola.org/sites/default/files/downloadable/Citizen%20Security/past/Poderesocultos.pdf (consultado: 6 noviembre, 2015)

104 Guatemala "Ley de la Dirección General de Inteligencia Civil" Congreso de la República de Guatemala (2005), artículo 5.

105 Guatemala "Ley General de Telecomunicaciones" Congreso de la República de Guatemala (Decreto 94-96).

debe ser acatada por las empresas de telecomunicaciones, ya que de lo contrario se les podría imponer una multa como sanción[106].

2.3.1.4. Normativas de acceso a la información o transparencia relacionadas al tema de la vigilancia

La Constitución establece en el artículo 30[107], en forma por demás clara, que todos los actos de la administración son públicos. En consonancia con la Constitución, la Ley de Acceso a la Información Pública[108] garantiza el derecho a solicitar y a tener acceso a la información pública en posesión de las autoridades y la transparencia de la administración pública. El Ministerio Público, el Organismo Judicial y el Organismo Ejecutivo, que son los que participan en el proceso de interceptación de comunicaciones, son sujetos obligados de dicha ley, y en ningún caso podrá ser considerada como confidencial la información relativa a investigaciones de violaciones a los derechos humanos fundamentales. Aunque la Ley Contra la Delincuencia Organizada[109] y la Ley de la Dirección General de Inteligencia Civil[110] señalan que la información obtenida de interceptación de comunicaciones es confidencial, esto no obsta a que se publiquen datos estadísticos con respecto al número de interceptaciones que se realizan.

2.3.1.5. Otras normas relacionadas al tema

Dentro de la legislación guatemalteca existen leyes ordinarias que protegen el derecho a la privacidad de la ciudadanía tales como el Código de Salud[111], la Ley Orgánica del Ministerio Público[112], la Ley de Protección Integral de la Niñez y Adolescencia[113] que protege el derecho a la privacidad de la población menor de edad y la de su familia, y la Ley del Registro Nacional de las Personas que incluye infracciones para aquellas personas que revelen información confidencial y establece una protección específica para los datos personales[114]. También la Ley de Libre Emisión del Pensamiento[115] protege el respeto a la

106 Guatemala "Código Penal" Congreso de la República (1973), artículo 414.

107 Guatemala "Constitución Política", artículo 30.

108 Guatemala "Ley de Acceso a la Información Pública" Congreso Nacional de la República de Guatemala (2008), artículo 1 y 6, http://www.vicepresidencia.gob.gt/archivos/2014/LEY%20ACCESO%20A%20LA%20INFORMACION%20PUBLICA%20COMENTADA.pdf (consultado: 6 noviembre, 2015)

109 Guatemala "Ley Contra la Delincuencia Organizada", artículo 15.

110 Guatemala "Ley de la Dirección General de Inteligencia Civil", artículo 5.

111 Guatemala "Código de Salud" USAID (1997), artículo 6.

112 Guatemala "Ley Orgánica del Ministerio Público" Wikiguate (1994), artículo 7, http://www.wikiguate.com.gt/w/images/7/74/Ley_Organica_del_Ministerio_Publico.pdf (consultado: 6 noviembre, 2015)

113 Guatemala "Ley de Protección Integral de la Niñez y Adolescencia" Procuraduría General de la Nación de Guatemala (2003), artículos 152, 153, http://www.pgn.gob.gt/ley-de-proteccion-integral-de-la-ninez-y-adolescencia-decreto-27-2003/ (consultado: 6 noviembre, 2015)

114 Guatemala "Ley del Registro Nacional de las Personas" Congreso de la República de Guatemala (2005), artículos 24 quinquies y 86.

115 Guatemala "Ley de Emisión del Pensamiento" Congreso Nacional de la República de Guatemala (1996), artículo 32, http://www.congreso.gob.gt/manager/images/4720C806-83C7-604B-1FF6-8DF6AA3AE8B3.pdf (consultado: 6 noviembre, 2015)

vida privada, los impresos[116] que penetren en la intimidad del hogar o de la conducta social de las personas, tendientes a exhibirlas o menoscabar su reputación o dañarlas en sus relaciones sociales. En esta misma vía se encuentra la Ley contra la Delincuencia Organizada[117] que establece que, mientras no exista persona ligada a proceso penal, no se tendrá acceso a las actuaciones realizadas por los agentes encubiertos y a las interceptaciones de comunicaciones. Además, señala una sanción para aquellos funcionarios o empleados públicos que revelen, divulguen o utilicen en forma indebida la información obtenida por medio de interceptaciones telefónicas u otros que regula dicha ley.

2.3.1.6. Otras normas específicas que regulen el cifrado

La Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, aplicable a todo tipo de comunicación electrónica, pública o privada[118], reconoce el uso de la tecnología de criptografía asimétrica. Esta regulación confirma que cualquier persona puede utilizar el cifrado para cualquier comunicación electrónica sin necesidad de contar con una autorización para ello.

2.3.1.7. Otras normas de debido proceso y anonimato digital

Dentro del ordenamiento jurídico penal guatemalteco no existe una norma específica que regule el procedimiento para revelar la identidad de la persona anónima. Sin embargo, la Ley del Organismo Judicial establece que cuando una ley es insuficiente se resolverá de acuerdo, entre otros casos, a disposiciones sobre casos o situaciones análogas[119]. Para revelar la identidad de la persona anónima se puede utilizar cualquiera de los medios de prueba del proceso penal, entre los cuales se encuentra el secuestro de cosas, que podría ser una computadora o teléfono celular; testimonio de personas; peritaje de personas expertas; solicitar el reconocimiento de personas, etc.

2.3.2. Sobre allanamientos y registros

El Código Procesal Penal regula los medios auxiliares para averiguación de la verdad[120]. Esta ley permite inspeccionar lugares, cosas o personas cuando hay motivos suficientes para sospechar que se encontrarán los vestigios de un delito, o se presuma que en determinado lugar está el imputado

116 La Ley de Emisión del Pensamiento define el impreso como la fijación del pensamiento por medio de la imprenta, la litografía, la fotografía, el mimeógrafo, el multígrafo, el fonógrafo y cualesquiera otros procedimientos mecánicos empleados actualmente o que puedan emplearse en el futuro para la reproducción de ideas. Esto último incluye, por supuesto, el internet.

117 Guatemala "Ley Control del Crimen Organizado" Ministerio de Gobernación (2006), artículo 18, 48.

118 Guatemala "Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas" Congreso Nacional de la República de Honduras, artículo 1, 46 y 47, http://www.redipd.es/legislacion/common/legislacion/guatemala/Acuerdo_47-2008_Firmas_Electronicas_Guatemala.pdf (consultado: 6 noviembre, 2015)

119 Guatemala "Ley del Organismo Judicial" Congreso Nacional de la República de Guatemala (1989), artículos 15 y 10, http://www.wikiguate.com.gt/w/images/b/b4/Ley_del_Organismo_Judicial.pdf (consultado: 6 noviembre, 2015)

120 Guatemala "Código Procesal Penal" Congreso Nacional de la República de Guatemala (1992), capítulo V, sección segunda, http://www.cicad.oas.org/fortalecimiento_institucional/legislations/PDF/GT/decreto_congresional_51-92_codigo_procesal_penal.pdf (consultado: 6 noviembre, 2015)

o persona evadida, siempre que medie una autorización judicial[121] debidamente motivada[122], salvo que exista un evento de fuerza mayor como un incendio, se presuma que se está cometiendo el delito o se persiga a una persona para su aprehensión[123]. En la inspección del lugar o de las cosas se comprobará únicamente aquello de utilidad para la averiguación del hecho y se levantará un acta que describa detalladamente lo acontecido. Además, el propietario o la persona que habite en el lugar debe estar presente en la inspección. Si una persona se opone, podrán ser obligados por la fuerza pública[124]. El registro de lugares cerrados o cercados únicamente podrá practicarse entre las seis y las dieciocho horas[125].

Las cosas y documentos relacionados con el delito y que pudieran ser de importancia para la investigación podrán ser depositadas y conservadas o solicitarse su secuestro cuando no sean entregadas voluntariamente. Cualquier persona puede negar la entrega de sus cosas y hasta que no se ordene judicialmente su secuestro no tiene la obligación de entregarlas[126]. Dicha orden de secuestro debe ser expedida por un juez o el Ministerio Público, quien debe solicitar inmediatamente después una autorización judicial. En el secuestro aplican las mismas reglas del registro[127]. Las cosas y documentos que no estén sometidos a comiso, restitución o embargo, serán devueltos a su propietario o tenedor legítimo[128]. Las llaves de cifrado si se encuentran como un archivo de una computadora podrían ser solicitadas por el Ministerio Público. Por otra parte, si la persona únicamente guarda las llaves de cifrado en su dispositivo de almacenamiento (memoria usb), no pueden ser solicitadas. Cabe destacar que no existe una legislación que regule este caso particular y obligue a las personas a entregar las llaves de cifrado, así como no se puede obligar a las personas a declarar contra sí misma.

2.3.3. Supervisión pública

Es importante que un órgano independiente supervise que las labores de vigilancia llevadas a cabo por el Estado sean vigiladas por un ente independiente. En el caso de las interceptaciones de comunicaciones reguladas por la Ley Contra la Delincuencia Organizada, los Jueces de Primera Instancia del Ramo Penal que hayan autorizado las interceptaciones tienen la obligación de acudir a verificar que los procedimientos se estén desarrollando de conformidad con la Ley, y que no se estén desarrollando interceptaciones no autorizadas. Esta verificación se debe realizar por lo menos una vez durante el período de tiempo autorizado[129].

121 Guatemala "Código Procesal Penal", artículo 191.
122 Guatemala "Código Procesal Penal", artículo 187.
123 Guatemala "Código Procesal Penal", artículo 190.
124 Guatemala "Código Procesal Penal", artículo 188.
125 Guatemala "Código Procesal Penal", artículo 189.
126 Guatemala "Código Procesal Penal", artículo 198.
127 Guatemala "Código Procesal Penal", artículo 201.
128 Guatemala "Código Procesal Penal", artículo 202.
129 Guatemala "Ley Contra la Delincuencia Organizada", artículo 57.

Por su parte, la Ley de la Dirección General de Inteligencia Civil contiene dos sistemas de control para el adecuado cumplimiento de dicha ley, lo cual incluye las escuchas telefónicas. El primer sistema de control es uno interno que llevará a cabo un Viceministerio de Gobernación, quien tiene la facultad de imponer sanciones disciplinarias o la respectiva denuncia al Ministerio Público[130]. El sistema de control externo es una Comisión Específica del Congreso de la República[131], que debe velar por el buen cumplimiento de la ley[132].

En cualquiera de los casos, los diputados del Congreso de la República, en cumplimiento de su función de fiscalización, podrían verificar el debido cumplimiento de las leyes que permiten la interceptación de comunicaciones solicitando información sobre cómo se llevan a cabo[133] y, si lo considera conveniente, interpelar al Ministro de Gobernación[134] o al Ministro encargado.

La función principal del Ministerio Público es velar por el debido cumplimiento de las leyes[135], por lo que tiene la obligación de verificar que la vigilancia estatal cumpla con los parámetros de derechos humanos por medio de la Fiscalía de Derechos Humanos o de delitos administrativos.

Los Jueces de Paz, el Congreso de la República y el Ministerio Público tienen amplias facultades para solicitar información precisa sobre el uso y alcance de las técnicas y poderes de vigilancia de las comunicaciones, y para hacer las denuncias correspondientes si consideran que alguna autoridad ha actuado con abuso de autoridad o violado alguna norma.

En el caso de la Ley Contra la Delincuencia Organizada, la persona que está siendo investigada tiene conocimiento de las interceptaciones telefónicas hasta el momento en que se da la primera audiencia penal, y es cuando puede ejercer su derecho de defensa revisando las grabaciones[136]. Por su parte, la Ley de la Dirección General de Inteligencia Civil no contempla ninguna medida de notificación diferida.

2.4. Conclusiones preliminares

1. El derecho a la privacidad contenido en los tratados internacionales de derechos humanos ratificados por Guatemala se encuentra protegidos en la Constitución Guatemalteca. Al ser los tratados materia de derechos humanos, son superiores al derecho interno guatemalteco. De ello se pueden extraer cinco conclusiones básicas sobre el derecho a la privacidad:

130 Guatemala "Ley de la Dirección General de Inteligencia Civil", artículo 25.
131 Guatemala "Ley Orgánica del Organismo Legislativo" Congreso Nacional de la República de Guatemala, artículo 31, numeral 16, http://www.congreso.gob.gt/manager/images/B1C07D30-68A0-B7A4-87F8-52CBC8051522.pdf (consultado: 6 noviembre, 2015)
132 Guatemala "Ley de la Dirección General de Inteligencia Civil" , artículo 26.
133 Guatemala "Ley Orgánica del Organismo Legislativo", artículo 4.
134 Guatemala "Constitución Política", artículo 165, literal j).
135 Guatemala "Constitución Política", artículo 251, primera oración.
136 Guatemala "Ley Contra la Delincuencia Organizada", artículo 61.

(i) El derecho a la privacidad incluye la inviolabilidad de cualquier tipo de comunicación y documentación de la persona, lo cual abarcartodo el proceso de comunicación, desde los metadatos hasta el contenido de las comunicaciones;

(ii) El derecho a la privacidad puede ser limitado pero las injerencias deben estar contenidas en la ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad, proporcionalidad y debido proceso;

(iii) El Estado solamente puede pedir la información de la vida privada que sea indispensable para los intereses de la sociedad;

(iv) La legislación que limite el derecho a la privacidad debe especificar con detalle las circunstancias precisas en que podrá autorizarse las injerencias; y,

(v) La recopilación de información, tanto por ciudadanos o por el gobierno, debe estar establecido por la ley.

2. El derecho a la privacidad ha venido designando una sólida protección constitucional desde la Constitución Federal de 1823, la cual se consolidó en 1879 con la prohibición clara y expresa de prohibir violar la correspondencia y los documentos privados de las personas, y estableciendo que este derecho solamente puede ser limitado por juez competente imparcial e independiente. La Constitucional actual amplía su protección a cualquier tipo de comunicación actual o que exista en el futuro.

3. Según la Corte de Constitucionalidad de Guatemala, el derecho a la privacidad se debe proteger al igual que la libre emisión del pensamiento, ya que la persona física tiene derecho inalienable e imprescriptible a su dignidad.

4. Dentro de la legislación guatemalteca es legal utilizar cifrado. Para levantar la identidad del usuario anónimo en causa penales o civiles es importante cumplir con los requisitos de necesidad, proporcionalidad, legítimo objetivo, idoneidad y debido proceso.

3. Marco legal nacional y su adecuación a los estándares internacionales

La Declaración Universal de Derechos Humanos señala en su artículo 12 que nadie puede ser objeto de injerencias arbitrarias en su vida privada ni en su familia, su domicilio o su correspondencia, y señala que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.[137] En correspondencia, el derecho a la privacidad también se encuentra reconocido en los artículos 11 de la Convención Americana sobre Derechos Humanos[138] y 17 del Pacto Internacional de Derechos Civiles y Políticos.[139]

En en el presente capítulo se evaluará si la normativa guatemalteca relacionada con la vigilancia de las comunicaciones se adhiere a los estándares internacionales de derechos humanos[140]. Utilizaremos los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones,[141] en adelante los 13 Principios, como guía para evaluar si las leyes de vigilancia de las comunicaciones en Guatemala se realizan en el marco de respeto de los derechos humanos. 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.

Los 13 Principios han sido citados en el informe del Grupo de Revisión del Presidente sobre Inteligencia y Tecnologías de las Comunicaciones de los Estados Unidos,[142] en el informe de la Comisión Interamericana de Derechos Humanos,[143] en el reporte sobre anonimato y cifrado del Relator de

137 Naciones Unidas "Declaración Universal de Derechos Humanos" (1948), artículo 12.

138 OEA. "Convención Americana sobre Derechos Humanos" (1969), artículo 11.

139 Pacto Internacional de Derechos Civiles y Políticos, artículo 17.

140 Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/text; Análisis Jurídico Internacional de Apoyo y Antecedentes de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://es.necessaryandproportionate.org/AnalisisLegal; Guía de Implementación Universal de los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://s3.amazonaws.com/access.3cdn.net/a0ea423a1607c836a3_aqm6iyi2u.pdf

141 Ver: https://es.necessaryandproportionate.org/text

142 Grupo de Revisión del Presidente sobre Inteligencia y Tecnologías de las Comunicaciones de los Estados Unidos de América, disponible en: http://www.dni.gov/index.php/intelligence-community/review-group (citado: 7 noviembre, 2015)

143 OEA, Informe anual de la oficina del Relator Especial de la Libertad de Expresión. (Washington, D.C., Organización de Estados Americanos, 2013), http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf (consultado, 7 noviembre, 2015)

Libertad de Expresión de Naciones Unidas,[144] y en el reporte de privacidad en la era digital del Alto Comisionado de Derechos Humanos de Naciones Unidas,[145] entre otros. Al ser ello así, tanto los tratados y decisiones judiciales que interpretan los 13 Principios son aplicables a Guatemala y estos constituyen una fuente de doctrina internacional relevante para analizar las prácticas de vigilancia a nivel nacional.

A continuación se analizará la legislación guatemalteca con respecto a los estándares de derechos humanos:

3.1. Principio de legalidad

> Cualquier limitación a los derechos humanos debe ser prescrita por ley. La Ley debe ser pública y cumplir un estándar de claridad y precisión suficientes para prever el alcance de las medidas de vigilancia de comunicaciones.

La regulación constitucional de la protección a la privacidad guatemalteca no señala expresamente que la limitación a este derecho deba hacerse por medio de una ley,[146] como si lo establece por ejemplo para la protección a la propiedad privada[147] y la libertad de locomoción[148]. Sin embargo, los estándares del sistema interamericano de derechos humanos, como el Relator Especial de las Naciones Unidas para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo y el Relator de Libertad de Expresión y Opinión han señalado que el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos que Guatemala ha ratificado, permite a los Estados Partes la posibilidad de introducir "restricciones o limitaciones al derecho a la privacidad".[149] En ese sentido, "las restricciones que no son prescritas por ley son "ilegales" en el sentido del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, y las restricciones que no son necesarias o no sirven a un fin legítimo constituyen una interferencia "arbitraria" con los derechos previstos en el artículo 17".[150]

144 OACNUDH. Informe del Relator Especial para la promoción y protección del derecho a la libertad de opinión y expresión. (Washington, D.C., Naciones Unidas, Oficina de la Alta Comisionada de Derechos Humanos, 2015), http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc (consultado: 7 noviembre, 2015)

145 OACNUDH. El derecho a la privacidad en la era digital. (Washington, D.C., Naciones Unidas, Oficina de la Alta Comisionada de Derechos Humanos, 2014), http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx (consultado, 7 noviembre, 2015)

146 Guatemala "Constitución Política de la República de Guatemala" Asamblea Nacional Constituyente (1985), artículo 24.

147 Guatemala "Constitución Política", artículo 39, segunda oración "Toda persona puede disponer libremente de sus bienes de acuerdo con la ley."

148 Guatemala "Constitución Política", artículo 26, primera oración "Toda persona tiene libertad de entrar, permanecer, transitar y salir del territorio nacional y cambiar de domicilio o residencia, sin más limitaciones que las establecidas por la ley."

149 Véase también el Relator Especial de Naciones Unidas para la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, A/HRC/23/40, 17 de abril de 2013, párrs. 28-29 y Véase Relator Especial de las Naciones Unidas para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, párrs. 16-18; http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf

150 Véase también Relator Especial de las Naciones Unidas para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, párrs. 16-18; http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf

Sin embargo, en Guatemala las limitaciones se encuentran previstas en ley,.[151] Dado que el artículo 24 Constitucional señala que la correspondencia de la persona únicamente podrá ser revisada si se cumple con las "formalidades legales" y "en virtud de resolución firme dictada por juez competente", se puede inferir que cualquier limitación que se haga al derecho de la privacidad de las comunicaciones únicamente puede hacerse por medio de una ley clara y precisa, conforme a las obligaciones internacionales que Guatemala ha suscrito.

El Código Procesal Penal[152] señala que podrá ordenarse la interceptación y secuestro de correspondencia postal, telegráfica y teletipográfica, y que la orden solamente puede ser expedida por un juez, la cual debe estar debidamente fundamentada. Esta regulación, por establecer qué tipo de interceptación se puede llevar a cabo y los requisitos de ella, se considera que es lo suficientemente clara y precisa.

La Ley Contra la Delincuencia Organizada[153] es clara y precisa con respecto a los motivos por los cuales procede la interceptación de las comunicaciones y las formalidades legales que se deben cumplir, pero NO es precisa con respecto al tipo de comunicaciones que se pueden interceptar, ya que hace una lista y agrega que se podrán interceptar "cualesquiera de otra naturaleza que en el futuro existan". Esto es una regulación demasiado amplia y por lo tanto esta frase no cumple con el principio de legalidad.

La Ley de la Dirección General de Inteligencia Civil[154] establece de forma clara las causales por los cuales proceden las escuchas telefónicas y las formalidades legales que se deben cumplir. Sin embargo, señala que se podrán interceptar comunicaciones "similares", lo cual es demasiado amplio y abre la puerta a que se intercepten otro tipo de comunicaciones. En conclusión, la frase "y similares" del artículo 4 de la Ley de la Dirección General de Inteligencia Civil no cumple con el principio de legalidad por ser imprecisa.

Recomendaciones

Se sugiere reformar la Ley Contra la Delincuencia Organizada para especificar el tipo de comunicaciones que se pueden interceptar y suprimir la frase "y similares" del artículo 4 de la Ley de la Dirección General de Inteligencia Civil.

151 Véase también Ley Contra la Delincuencia Organizada, Código Procesal Penal y Ley de la Dirección General de Inteligencia Civil.

152 Guatemala "Código Procesal Penal" OEA (1992), artículos 203, 204, 205, http://www.cicad.oas.org/fortalecimiento_institucional/legislations/PDF/GT/decreto_congresional_51-92_codigo_procesal_penal.pdf (consultado: 7 noviembre, 2015)

153 Guatemala "Ley Contra la Delincuencia Organizada" Ministerio de Gobernación (2006), artículo 18, 48, http://wikiguate.com.gt/ley-contra-la-delincuencia-organizada-documento/ (consultado: 7 noviembre, 2015)

154 Guatemala "Ley de la Dirección General de Inteligencia Civil" Congreso de la República de Guatemala (2005), artículo 4.

3.2. Objetivo legítimo

Las leyes que establezcan medidas de vigilancia de las comunicaciones deben perseguir objetivos legítimos y no ser aplicada de manera discriminatoria.

Este principio ha sido recogido por la Corte de Constitucionalidad, quien ha dicho que este derecho únicamente puede ser limitado por razones de interés público y por necesidades sociales[155].

El Código Procesal Penal señala que únicamente cuando sea de "utilidad para la averiguación" puede ordenarse el secuestro e interceptación de correspondencia. Una necesidad social e interés público es la averiguación de la verdad cuando se comete un delito. Sin embargo, este medio auxiliar de investigación debe ser utilizado cuando sea estrictamente necesario y de manera proporcional.

La Ley Contra la Delincuencia Organizada señala expresamente los delitos por los cuales se puede interceptar, grabar o reproducir una comunicación, y que cuando sea necesario evitar, interrumpir o investigar la comisión de uno de estos delitos, se puede limitar el derecho a la privacidad de las comunicaciones. Una necesidad social e interés público es evitar, interrumpir o investigar la comisión de este tipo de delitos contenidos en la Ley Contra la Delincuencia Organizada.

La Ley de la Dirección General de Inteligencia Civil señala que únicamente se puede solicitar la autorización de una escucha telefónica cuando existan indicios de actividades del crimen organizado en las que hubiera peligro para la vida, la integridad física, la libertad y los bienes de personas determinadas. Una necesidad e interés público es proteger la vida, la libertad, la integridad personal y los bienes de las personas.

3.3. Principios de necesidad, idoneidad y proporcionalidad

Necesidad: Las vigilancia de las comunicaciones solo debe llevarse a cabo cuando la consecución del objetivo legítimo no pueda alcanzarse a través de métodos menos lesivos a los derechos humanos. La carga de demostrar dicha justificación le corresponde al Estado.

Idoneidad: Las medidas de vigilancia de comunicaciones deben ser apropiadas y capaces de conseguir el objetivo legítimo perseguido.

Proporcionalidad: Las medidas de vigilancia solo deben autorizarse por una autoridad judicial independiente cuando exista un alto grado de probabilidad de que un delito grave o una amenaza específica, actual y comprobable a la seguridad nacional pueda materializarse.

155 Guatemala. Corte de Constitucionalidad, inconstitucionalidad general parcial, expediente 2622-2006, http://vlex.com/vid/-423703874 (consultado, 7 noviembre, 2015)

La Ley Contra la Delincuencia Organizada[156] indica que existe necesidad de la interceptación de comunicaciones cuando los medios de investigación utilizados demuestren que en los delitos cometidos por grupos delictivos organizados se estén utilizando los medios de comunicación establecidos en la Ley.

La ley citada[157] dice que se entenderá que existe idoneidad cuando, atendiendo a la naturaleza del delito, se puede determinar que la interceptación de las comunicaciones es eficaz para obtener los elementos de investigación que permitan evitar, interrumpir o esclarecer la comisión de los delitos contenidos en esta ley. Sin embargo, esto no es suficiente ya que la autoridad judicial debe especificar el alcance de la información necesaria para obtener el objetivo legítimo. Es necesario que la interceptación de comunicaciones se relacione con una persona, cuenta, dispositivo o metadatos que se buscan. El alcance de la vigilancia de las comunicaciones debe ser lo más precisa posible para minimizar el impacto en otro tipo de información no relacionada.

El principio de proporcionalidad requiere que se demuestre a la autoridad judicial competente: i) Que existe un alto grado de probabilidad de un delito grave o amenaza a un fin legítimo; ii) Otras técnicas de investigación menos invasivas ya han sido agotadas o serían inútiles; iii) La información a la que se accederá estará limitada a lo relevante y material para el crimen; iv) Cualquier información excedente no será retenida, y v) La información será accesada solamente por la autoridad específica y utilizada para los propósitos necesarias.

El Código Procesal Penal señala que únicamente cuando sea de utilidad para la averiguación se podrá ordenar la interceptación y el secuestro de correspondencia. Sin embargo, no se le exige a la persona que lo solicite,ni acreditar ante el juez que existe un alto grado de probabilidad que se encontrará evidencia del delito, ni que se han utilizado otras técnicas de investigación menos invasivas, ni que la información que se utilizará será específicamente relevante y material del crimen. El requerimiento de no retener información excedente se cumple en el artículo 204, que indica que si la información contenida en la correspondencia no tuviere relación con el delito, se mantendrá bajo reserva y se le entregará a su destinatario. Además, se cumple con el requisito de solamente recibir la información por la autoridad específica en el mismo artículo que señala que es el tribunal competente quien abre la correspondencia.

La Ley Contra la Delincuencia Organizada es la única legislación guatemalteca que regula los principios de necesidad e idoneidad[158] y que exige que se justifiquen en la solicitud de autorización de la interceptación. La solicitud de autorización para la interceptación de las comunicaciones reguladas en esta ley debe llenar los siguientes requisitos: a. Descripción del hecho que se investiga, indicando

156 Guatemala “Ley Contra la Delincuencia Organizada”, artículo 51.
157 Guatemala “Ley Contra la Delincuencia Organizada”, artículo 51.
158 Guatemala “Ley Contra la Delincuencia Organizada”, artículos 50 y 51.

el delito que se encuadra en el mismo; b. Números de teléfonos, frecuencias, direcciones electrónicas o cualesquiera otros datos que sean útiles para determinar el medio electrónico o informático que se pretende interceptar; c. Descripción de las diligencias y medios de investigación que se han realizado; d. Justificación del uso de la medida, fundamentando su solicitud de idoneidad, y e. Si se tuviere, el nombre y otros datos que permitan identificar a la persona que está siendo afectada.[159]

En cuanto al principio de proporcionalidad, esta ley cumple con el requisito de requerir que exista un alto grado de probabilidad que encontrará evidencia del crimen al autorizar la vigilancia. Podemos decir que en esta norma el objetivo legítimo es claro pues se puede solicitar la interceptación de comunicacion solamente cuando es necesario evitar, interrumpir o investigar la comisión de uno de los delitos serios regulados en esta ley. En cuanto al requisito de agotar otras técnicas de investigación, la ley obliga en la literal c) del artículo 50 a describir las diligencias y medios de investigación que se han utilizado hasta el momento. Aunque no es una obligación agotar otros medios de investigación previo a la interceptación, le da indicios al juez para otorgar o no esta medida.

El requisito de excluir cualquier información que no sea relevante para cumplir con el objetivo legítimo se cumple con el artículo 60 de la ley citada, que señala que únicamente se levantará acta de la información "útil y relevante", por lo que cualquier otra información personal o íntima será excluida del informe. Esta información tampoco será retenida, ya que se obliga a que destruyan las interceptaciones de las comunicaciones un año después de finalizada la persecución penal[160]. Por último, la información de la interceptación solamente puede ser accesada por el personal autorizado de la Policía Nacional Civil, el fiscal del Ministerio Público y posteriormente por los Tribunales[161].

La Ley de la Dirección General de Inteligencia Civil no obliga a justificar la necesidad o idoneidad de una escucha telefónica, por lo que no cumple con estos dos principios. En cuanto al principio de proporcionalidad, que requiere que exista un alto grado de probabilidad de la comisión de un delito, la ley señala que deben existir indicios para poder solicitar la escucha telefónica. Al requerir únicamente que existan indicios del delito no se cumple con el requisito que exista un *alto grado de probabilidad* en la comisión del delito. Por otra parte, se cumple con el requerimiento que la información sea utilizada única y exclusivamente para el objeto de la investigación, ya que la misma ley prevé que aquella información ajena a los fines de la intervención y que ha sido interceptada no podrá ser utilizada. Sin embargo, no se cumple con el principio de agotar otros medios de investigación menos invasivos. Además, la ley es ambigua en cuanto a la información que no es útil para la investigación. La normativa citada no indica claramente si esta información puede ser retenida por el Estado y quiénes son las personas que tienen autorización para ver la información retenida.

159 Guatemala "Ley Contra la Delincuencia Organizada", artículos 50.
160 Guatemala "Ley Contra la Delincuencia Organizada", artículos 65.
161 Guatemala "Ley Contra la Delincuencia Organizada", artículos 55, 60 y 68.

Recomendaciones

Se sugiere hacer una reforma del Código Procesal Penal en el sentido de exigir a la persona que solicite la interceptación o secuestro de la correspondencia acreditar ante el juez que existe un alto grado de probabilidad del delito grave, que ya se han utilizado otras técnicas de investigación menos invasivas y que la información que se utilizará será específicamente para lo relevante y material del crimen.

Se sugiere que se reforme la Ley de la Dirección General de Inteligencia Civil en el sentido de: (i) Requerir que se justifique la necesidad e idoneidad de la ejecución de una escucha telefónica, previa a su autorización; (ii) Requerir que se compruebe que previo a solicitar la escucha se han utilizado otros medios de investigación menos invasivos; (iii) Aclarar que la información que no es útil no puede ser retenida por el Estado; (v) Especificar cuáles funcionarios tienen acceso a las escuchas telefónicas; y (vi) Requerir que exista un alto grado de probabilidad en la comisión del delito para poder solicitar una escucha telefónica.

Aunque la solicitud para la autorización de interceptación de comunicaciones regulada en la Ley Contra la Delincuencia Organizad debe contener varios elementos que le ayudan al juez a determinar la necesidad y proporcionalidad de la medida, esta debe incluir además: i) Identificación del funcionario que solicita la medida; ii) Prestar juramento de la veracidad de la información; iii) Cita del fundamento de derecho para solicitar la interceptación; iv) Precisar el alcance de la solicitud de interceptación de comunicaciones; y, vi) Precisar la información necesaria para lograr ese objetivo legítimo y por qué es necesaria. En el caso de la la solicitud de interceptaciones regulada en la Ley de la Dirección General de Inteligencia Civil se recomienda que se regule al igual que como lo está en la Ley Contra la Delincuencia Organizada y además, se incluyan los requisitos señalados anteriormente.

3.4. Principio de autoridad judicial competente

En Guatemala se respeta este principio ya que es siempre una autoridad distinta a la que está encargada de la vigilancia de las comunicaciones la que autoriza este tipo de medidas. En el caso de la interceptación y secuestro de correspondencia, regulado en el Código Procesal Penal, la autoridad judicial competente es el juez que esté conociendo el procedimiento o el Presidente del Tribunal, si fuere colegiado[162]; las interceptaciones

> Las medidas de vigilancia de comunicaciones deben ser autorizadas de manera previa, o inmediata con efecto retroactivo en casos de emergencia, por una autoridad judicial competente, independiente e imparcial.

162 Guatemala "Código Procesal Penal", artículo 203, http://www.cicad.oas.org/fortalecimiento_institucional/legislations/PDF/GT/decreto_congresional_51-92_codigo_procesal_penal.pdf (consultado: 7 noviembre, 2015)

de comunicaciones reguladas en la Ley Contra la Delincuencia Organizada son autorizadas por los Jueces de Primera Instancia del Ramo Penal[163]; y las escuchas telefónicas reguladas en la Ley de la Dirección General de Inteligencia Civil las autoriza una Sala de la Corte de Apelaciones[164]. En todos los casos, la autoridad encargada de ejecutar la vigilancia de la comunicación es un funcionario del Ministerio de Gobernación.

Recomendaciones

Se recomienda que la Escuela de Estudios Judiciales y la unidad de capacitación institucional del Organismo Judicial, capaciten constantemente a las autoridades judiciales competentes de autorizar la vigilancia de las comunicaciones y publique las autorizaciones, para que cumplan con los estándares internacionales en materia de Derechos Humanos. Además, se sugiere asignar los recursos adecuados en el ejercicio de las funciones que se le asignen en materia de vigilancia de las comunicaciones.

3.5. Debido proceso

En la legislación guatemalteca está regulado el procedimiento para llevar a cabo una interceptación de las comunicaciones y está disponible para el público. Sin embargo, en ninguno de los casos se le da audiencia pública a la persona que están vigilando o a una persona que lo pueda representar. El juez o tribunal correspondiente debe únicamente aceptar la solicitud de vigilancia de las comunicaciones cuando esta llena todos los requisitos de forma y fondo establecidos en la ley. Además, el juez o tribunal competente debe determinar que existen suficientes indicios para dictaminar que hay una relación entre el dispositivo a vigilar y la información necesaria que se busca, es decir, que ocurreuna alta probabilidad de encontrar, por ejemplo, evidencia de un delito.

> Las decisiones de autorización de medidas de vigilancia de comunicaciones deben garantizar el debido proceso. Lo anterior implica que, cuando para la consecución del objetivo legítimo, y en particular, la protección de la vida de una persona, sea necesaria la secretividad de la medida o su aplicación inmediata, existan otras medidas que garanticen la protección de los intereses del afectado como la designación de una persona o institución que asuma representación general de sus intereses en la audiencia o en caso de emergencia, que la autorización judicial se lleve a cabo con efecto retroactivo

La autorización de la Corte debería contener, como mínimo, la siguiente información: (i) Nombre del juez o tribunal que autoriza la medida y la fecha; (ii) Fundamento de derecho; (iii) Metodología que se utilizará en la vigilancia de las comunicaciones, y (iv) El alcance y duración de la autorización, indicando las cuentas o dispositivos a vigilar.

163 Guatemala "Ley Contra la Delincuencia Organizada", artículo 52.
164 Guatemala "Ley de la Dirección General de Inteligencia Civil", artículo 4.

Recomendaciones

Se recomienda una reforma legal que permita que un representante -el cual podría ser el Procurador de los Derechos Humanos- pueda emitir una opinión en favor de la persona que se estará vigilando.

3.6. Notificación del usuario

En Guatemala ninguna de las legislaciones que regula la interceptación de comunicaciones contempla la notificación al usuario que está siendo vigilado, previo a su vigilancia. Lo anterior, porque se utiliza para obtener información para la averiguación de la verdad en la comisión o la prevención de la comisión de un delito. Sin embargo, si el delito no se comete o si la persona no está implicada se le debería notificar, ya que se le notifica a la persona hasta que se lleva a cabo la primera audiencia o durante el desarrollo del juicio penal.

> Las personas afectadas por medidas de vigilancia de comunicaciones deben ser notificadas de ello y tener acceso a las materiales que pretendan ser o hayan sido obtenidos. La notificación podrá diferirse cuando la misma ponga en riesgo la consecución del objetivo legítimo o exista un riesgo inminente de peligro a la vida humana.

Recomendaciones

La normativa guatemalteca debería incluir una disposición que obligue al Estado a notificar al usuario que ha sido vigilado cuando no se presente una acusación formal contra este. La notificación diferida debería ser la excepción y no la regla, por lo que debería de otorgarse por el juez únicamente en casos muy específicos. El tiempo de notificación diferida al usuario no debería ser mayor a 30 días.

Por su parte, se sugiere reformar la Ley de la Dirección General de Inteligencia Civil para obligar a que las personas sean notificadas, al menos después de haber sido vigiladas.

3.7. Transparencia

En Guatemala todos los actos de la administración son públicos[165]. Sin embargo, ninguna ley obliga a la publicación de este tipo de información.

> El Estado debe publicar de manera periódica información estadística sobre las medidas de vigilancia encubierta llevadas a cabo. Como mínimo debe publicar el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad, tipo y propósito, y el número de personas afectadas.

165 Guatemala "Constitución Política de la República de Guatemala" Asamblea Nacional Constituyente (1985), artículo 30.

Recomendaciones

Se sugiere añadir a la Ley de Acceso a la Información Pública, como información pública de oficio, la información detallada anteriormente sobre la vigilancia de las comunicaciones. Se sugiere que el Estado publique estadísticas de solicitudes de interceptación por parte de las autoridades judiciales a los proveedores de servicios de telecomunicaciones. Entre esta información se sugiere incluir: (i) Número total de solicitudes realizadas por las autoridades judiciales; (ii) Número para cada tipo de interceptaciones, y (iii) Número de usuarios y cuentas vigiladas.

La información de parte del Estado debería incluir: (i) Número total de cada uno de los tipos de solicitudes, especificando la autoridad que los validó y la autoridad que lo solicitó; (ii) Número de solicitudes recibidas, haciendo una separación entre las aceptadas y las rechazadas; (iii) Número de usuarios y cuentas vigiladas; (iv) Número de personas afectadas con este tipo de medidas; (v) Número de solicitudes que fueron utilizadas efectivamente en un juicio, y (vi) Si hubo algún recurso que se interpuso en respuesta a la vigilancia de las comunicaciones.

En la medida de lo posible los proveedores deben asegurarse que los usuarios han sido notificados que sus comunicaciones están siendo interceptadas.

3.8. Supervisión pública

Deben establecerse mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones.

En el caso de las interceptaciones de comunicaciones reguladas por la Ley Contra la Delincuencia Organizada, los Jueces de Primera Instancia del Ramo Penal que hayan autorizado las interceptaciones tienen la obligación de acudir a verificar que los procedimientos se estén desarrollando de conformidad con la ley, y que no se estén desarrollando interceptaciones no autorizadas.[166]

Por su parte, la Ley de la Dirección General de Inteligencia Civil contiene dos sistemas de control para el adecuado cumplimiento de dicha ley, lo cual incluye las escuchas telefónicas, un sistema interno por medio del Viceministerio de Gobernación[167] y un sistema externo que es una Comisión del Congreso de la República[168].

166 Guatemala "Ley Contra la Delincuencia Organizada", artículo 57.
167 Guatemala "Ley de la Dirección General de Inteligencia Civil", artículo 25.
168 Guatemala "Ley Orgánica del Organismo Legislativo" Congreso Nacional de la República de Guatemala, artículo 31, numeral 16, http://www.congreso.gob.gt/manager/images/B1C07D30-68A0-B7A4-87F8-52CBC8051522.pdf (consultado: 7 noviembre, 2015)

En cualquiera de los casos, los diputados del Congreso de la República o el Ministerio Público[169] podrían verificar el debido cumplimiento de las leyes que permiten la interceptación de comunicaciones solicitando información sobre cómo se llevan a cabo[170] y, si lo considera conveniente, interpelar al ministro de Gobernación[171] o al ministro encargado, en el caso del Congreso, o presentar una denuncia formal por medio de la Fiscalía de Derechos Humanos.[172]

Se recomienda una reforma legal que obligue a la entidad que realiza la interceptacióna informar cada 30 días o menos a la autoridad judicial que autorizó la medida. Este reporte debe contener la información buscada, el alcance de la información obtenida en el período del reporte, la información que no se considera necesaria y la razón por la cual se continúa la investigación. De esta forma, la autoridad judicial puede asegurarse que la aplicación de la vigilancia de las comunicaciones fue aplicada de tal forma que cumple con todos los términos de la autorización judicial.

3.9. Integridad de las comunicaciones y sistemas

En Guatemala no existe una obligación con los proveedores de crear puertas traseras que permita a las autoridades que conducen la vigilancia acceso directo a sus servicios o dispositivos. En algunos casos como el de los bancos, el Estado solicita que en sus comunicaciones utilicen información cifrada.

No debe obligarse a proveedores de servicios o desarrolladores de "hardware" o "software" a desarrollar capacidades de vigilancia que comprometan la seguridad de las comunicaciones y los dispositivos. No debe exigirse la retención indiscriminada y masiva de datos de las personas que usan dichos servicios ni debe comprometerse el derecho a la expresión anónima a través del establecimiento de obligaciones de identificación o prohibiciones respecto del uso de herramientas de cifrado y otras para proteger la identidad y la seguridad de las personas, sus comunicaciones y sus dispositivos.

Tampoco existe una norma de retención que obligue a los proveedores de servicios de telecomunicaciones a retener ciertos datos de la comunicación de la población por un tiempo determinado. Por el contrario, los proveedores deben asegurarse de utilizar sistemas de seguridad confiables que minimicen los riesgos de hacer vigilancia de las comunicaciones en sus sistemas. Los proveedores deben ser transparentes con los usuarios con respecto a los términos de uso, políticas de privacidad y otras formas de restringir sus derechos. Esta información debe estar redactada de una forma clara y precisa.

169 Guatemala "Constitución Política", artículo 251, primera oración.
170 Guatemala "Ley Orgánica del Organismo Legislativo", artículo 4.
171 Guatemala "Constitución Política", artículo 165, literal j).
172 Para más información sobre el tema ver el numeral 4 del capítulo II, marco legal, supervisión.

Los datos no deben ser retenidos por la empresa por más del tiempo necesario para el desarrollo normal del negocio. Cuando los datos de las comunicaciones no sean imperiosos deben ser destruidos.

3.10. Garantías contra el acceso ilegítimo y derecho a recurso efectivo

La vigilancia ilegal de comunicaciones debe ser castigada mediante sanciones civiles y penales suficientes y adecuadas. Los *whistleblowers* de interés público deben ser protegidos por la ley de cualquier repercusión legal por el incumplimiento de su deber de secrecía.

En Guatemala está penalizada la violación, sustracción e interceptación de comunicaciones a cualquier persona sin previa orden de juez competente[173]. También está prohibida la revelación de secretos que las personas hayan conocido por su estado, oficio, empleo, profesión o arte, que ocasionare o pudiere ocasionar perjurio, y sanciona a funcionarios y empleados públicos que revelen secretos. La Ley Contra la Delincuencia Organizada estipula, en forma por demás clara, que no tiene validez como medio de prueba cualquier información que sea resultado de una interceptación que no cumpla con los requisitos establecidos en esta ley[174]. La información obtenida por medio de escuchas telefónicas regulada en la Ley de la Dirección General de Inteligencia Civil no puede ser utilizada como prueba[175]. El Código Penal no regula qué ocurre con la prueba obtenida violando el procedimiento de interceptación de comunicaciones; sin embargo, la Constitución protege el debido proceso[176] y este implica que únicamente hace prueba en juicio la obtenida cumpliendo con las formalidades legales.

Por otra parte, no existe una regulación que proteja a los *whistleblowers* y ninguna ley dice lo que ocurre con el material obtenido a través de la vigilancia de las comunicaciones, después que ha sido utilizado para la finalidad. Por si lo anterior fuese poco, la Constitución es clara al señalar que la información obtenida violando la ley no producen fe ni hacen prueba en juicio.[177]

Recomendación

Se sugiere incluir una legislación que proteja a los *whistleblowers* y hacer una adición a las distintas leyes que regulan la interceptación de comunicaciones, para que la información sea destruida luego de utilizada para su fin.

173 Guatemala "Código Penal" Organismo Judicial (1973), artículos 217, 218, 219, 220, 221, 222, 223 y 422, http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/lex/CodigoPenal.htm (consultado: 7 noviembre, 2015)

174 Guatemala "Ley Contra la Delincuencia Organizada", artículo 62.

175 Guatemala "Ley de la Dirección General de Inteligencia Civil",artículo 62.

176 Guatemala "Constitución Política", artículo 12.

177 Guatemala "Constitución Política", artículo 24.

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

El objetivo fundamental para el desarrollo de este capítulo fue identificar las principales experiencias e inquietudes de profesionales del Derecho, activistas, técnicos y técnicas en Informática, relacionadas con el derecho a la privacidad digital, en internet y en las telecomunicaciones.

El logro del objetivo se fundamentó en la valoración de la experiencia directa, relacionada con vigilancia, anonimato, cifrado, allanamientos y requisas, que han tenido las personas entrevistadas a lo largo de sus carreras profesionales y como activistas de derechos humanos. Así como recoger las principales dudas e inquietudes sobre el marco legal guatemalteco respecto a la vigilancia de las telecomunicaciones encaminada a criminalizar la labor de promoción y defensa de derechos humanos.

4.1. Metodología

La realización de este proceso, que propició el compartir diversas experiencias e inquietudes de quienes enfrentan día a día los desafíos que conlleva la labor de promover y defender derechos humanos, contó con la participación de un grupo selecto de personas que ejercen la labor del Derecho, activistas de derechos humanos y técnicos y técnicas en Informática. Las personas entrevistadas se eligieron bajo un perfil específico tomando en consideración su alto compromiso en materia de derechos humanos y profundos valores democráticos. La metodología utilizada durante este proceso fue cualitativa, y se eligió la entrevista como herramienta de investigación.

Para lograr el objetivo de este capítulo se realizaron dos (2) diferentes guías de entrevistas, procurando que se ajustasen explícitamente a las experiencias individuales de cada una de las personas seleccionadas. Además, se elaboró también una tercera guía de preguntas para el desarrollo de un grupo focal dirigido a técnicos y técnicas en Informática que tuvo como fin recabar de manera colectiva diversas experiencias, así como generar el debate respecto al conjunto de leyes que pueden llegar a vulnerar el derecho a la privacidad de la ciudadanía guatemalteca en el entorno digital y de las telecomunicaciones. Asimismo, fue objetivo de este grupo focal atender las dudas e inquietudes, de orden legal, que se generan desde la mirada técnica.

De esta manera, se realizaron seis (6) entrevistas a técnicos en Informática que a diario atienden

casos e incidentes relacionados con la seguridad de la información y de la comunicación de diversas organizaciones defensoras de derechos humanos a nivel nacional, que a su vez trabajan con mujeres, indígenas, comunidad LGBTIQ, estudiantes, periodistas, comunicadores y comunicadoras sociales, entre otros. En este punto, resulta importante destacar que el hecho de que las entrevistas se hayan realizado solamente con técnicos, varones, denota la necesidad de empoderar a las mujeres en materia de acceso a las tecnologías de la información y de la comunicación, y cómo hacer frente a este tipo de ataques que ponen en jaque el derecho a la privacidad digital. De igual forma, se entrevistaron cuatro (4) profesionales del Derecho, quienes compartieron sus experiencias desde el área legal.

El grupo focal se llevó a cabo con técnicos expertos en seguridad digital, y todos los años de experiencia previa resultaron sumamente enriquecedores a fin de entender cómo es que se producen estos ataques a la privacidad digital. El grupo focal también posibilitó la discusión sobre el tema del anonimato dentro del actual contexto que embarga al país. También, se abrió el debate sobre lo que se entiende como privado, y cómo tradicionalmente se asocia -nuestra- la privacidad exclusivamente a espacios privados; la interpretación ventajosa de los conceptos: espacios privados y espacios cerrados; y la necesidad de buscar maneras privadas en internet.

Y, por otro lado, se realizó una jornada de validación donde se presentaron los resultados de la investigación ante un selecto grupo de profesionales del derecho, activistas y técnicos, que manejan ampliamente el tema seguridad desde sus respectivas áreas de incidencia.

Es importante resaltar que las opiniones vertidas a lo largo de este proceso, las cuales se comparten a continuación en este capítulo, provienen todas de activistas de derechos humanos que han sido víctimas del sistema de vigilancia. Sin embargo, por el tipo de metodología utilizada no podemos hacer afirmaciones ni 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.

4.2. Experiencias (hallazgos y casos paradigmáticos)

4.2.1. Vigilancia

Al preguntar a las personas entrevistadas sobre su percepción del sistema de vigilancia en internet y en las telecomunicaciones en Guatemala, nueve de diez personas manifestaron que sus teléfonos celulares han sido interceptados (señal interrumpida, ruidos, eco, etc), además de saber que sus teléfonos han sido utilizados como micrófono en más de una ocasión. También manifestaron conocer otras personas activistas de derechos humanos a quienes les ha sucedido lo mismo, debido a lo cual

el derecho a la libertad de expresión está siendo limitado en el sentido que las personas ya no se expresan como antes lo harían ya que están siendo vigiladas:

> Las revelaciones de [Edward] Snowden nos dan certeza que el gobierno de Estados Unidos realiza vigilancia. En Guatemala hay algunas entidades del gobierno que lo pueden hacer en determinados casos, además de algunas personas, y grupos, que lo hacen ilegalmente, por eso estamos constantemente revisando si nuestro teléfono ha sido intervenido, cambiamos de números de celular constantemente, no utilizamos una tarjeta de crédito al comprar un dominio, usamos aplicaciones para proteger información, etc.[178]

Posteriormente, las personas entrevistadas lograron identificar fácilmente que los principales ataques que vulneran el derecho a la privacidad en internet y las telecomunicaciones provienen del Gobierno. Y, paralelamente al control y monitoreo ejercido por el Gobierno, se evidencia el liderazgo que ha tomado el Ejército en el tema de seguridad a través de una red de espionaje instalada con la asesoría del Ejército de los Estados Unidos[179]:

> La intervención a las comunicaciones en Guatemala es una práctica reiterada que data desde el periodo de dictaduras militares, y es controlada desde la oficina de Control de Inteligencia Militar, por medio del centro de telecomunicaciones del ejercito operado por la Secretaría de Asuntos Administrativos y de Seguridad (SAAS). El gobierno guatemalteco cuenta con una oficina para el monitoreo de la opinión pública en las redes sociales, que depende de la Secretaría de Comunicación Social de la Presidencia de la República.[180]

Casi todas las personas entrevistadas dijeron que es de conocimiento público que la Secretaría de Inteligencia Estratégica de la Presidencia, que ejecuta labor de espionaje contra principales dirigentes de oposición, adquirió en 2013 un software denominado MEMEX que es capaz de alcanzar e interrelacionar bases de datos públicas y privadas para obtener información en tiempo real[181], y así tener control sobre la información personal de la ciudadanía. MEMEX fue desarrollado hace años atrás por la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) de Estados Unidos[182].

Además, los técnicos especialistas en seguridad digital entrevistados durante el grupo focal, señalaron que tienen conocimiento de las negociaciones del gobierno de Guatemala con la empresa italiana Hacking Team[183]. Esta empresa italiana vende a los gobiernos diversos programas de vigilancia que

178 Entrevista activista de derechos humanos. Guatemala, agosto 2015.

179 Plaza Pública, "Pequeñas cosas que no cuadran", http://www.plazapublica.com.gt/content/pequenas-cosas-que-no-cuadran (consultado 4 noviembre, 2015)

180 Soy 502, "La oficina del Gobierno que monitorea las redes sociales", http://www.soy502.com/articulo/opinion-publica-en-redes-sociales-es-monitoreada-desde-el-inguat (consultado 4 noviembre, 2015)

181 NTVGuatemala, "¿Nos vigilan?", http://www.ntv.com.gt/testimonial/somos-vigilados/ (consultado 4 noviembre, 2015)

182 DARPA. "Memex (Domain-Specific Search)", http://www.darpa.mil/program/memex http://www.darpa.mil/program/memex (consultado 4 noviembre, 2015)

183 Wikileaks, "Hacking Team/Guatemala", https://wikileaks.org/hackingteam/emails/emailid/5179 (consultado 4 noviembre, 2015)

infectan teléfonos inteligentes y computadoras con *malware* para grabar secretamente conversaciones y robar datos. Desde hace años, Hacking Team viene siendo objeto de escrutinio por parte de periodistas y activistas de derechos humanos por sus vínculos con regímenes militares alrededor del mundo.[184] Por otro lado, las personas entrevistadas dijeron tener fuertes sospechas de la contratación de empresas prestadoras de servicios por parte del gobierno para perpetrar ataques de denegación de servicio (DdoS), orientados a callar medios en momentos coyunturalmente específicos, además de perpetrar otros ataques como *deface*, *hacking* y *phishing*.

En adición a las fuerzas de poder arriba mencionadas por las personas entrevistadas, se encuentran las instituciones de poder económico que funcionan con la protección de los altos mandos del ejercito, y, claro, del Gobierno también.

La alianza entre el binomio gobierno y empresa privada se genera desde el período de dictaduras militares, misma que han legitimado con la aprobación de la ley de alianza publico-privada, dándole vida normativa al sector privado.[185]

Preocupa la creciente dinámica de privatización de la seguridad y vigilancia, mediante empresas privadas y comerciales, y el establecimiento de una policía comunitaria que está conformada por ex miembros del ejercito o de grupos paramilitares, y no se cuenta con un proceso de depuración de estas instancias.

Asimismo, se logró identificar y describir el contexto, aparentemente circunstancial, bajo el que se producen esos ataques, como por ejemplo durante el caso de genocidio el poder económico utilizó al ejercito para realizar ataques a organizaciones defensoras de derechos humanos, y también durante las movilizaciones pacíficas que han tenido lugar en 2015. Estos ataques recaen sobre activistas de derechos humanos, líderes y liderezas del movimiento social. En el interior del país la criminalización a la labor de promoción y defensa de derechos humanos se intensifica.

Ante este escenario, los técnicos y activistas manifestaron su preocupación por el poco conocimiento técnico que existe sobre la Seguridad de la Información y de las Comunicaciones (SIC) en relación al contexto de represión, que fácilmente podría confundirse con la falta de interés. No hay un empoderamiento por parte de las organizaciones debido a la comodidad del uso de windows, por ejemplo. Las organizaciones no tienen una estrategia definida para enfrentar ataques a la privacidad digital. A inicios del año 2000 con el apoyo de (se reserva el nombre por motivos de seguridad),

184 The Intercept, "Hacking Team Emails Expose Proposed Death Squad Deal, Secret U.K. Sales Push and Much More", https://theintercept.com/2015/07/08/hacking-team-emails-exposed-death-squad-uk-spying/ (consultado 4 noviembre, 2015)

185 Guatemala. "Ley de Alianzas para el Desarrollo de Infraestructura Económica". Congreso de la República de Guatemala, http://www.oj.gob.gt/es/QueEsOJ/EstructuraOJ/UnidadesAdministrativas/CentroAnalisisDocumentacionJudicial/cds/CDs%20leyes/2010/pdfs/decretos/D016-2010.pdf (consultado 5 noviembre, 2015)

se inició la implementación de ciertas estrategias de seguridad digital para enfrentar este tipo de ataques a organizaciones como la Fundación Rigoberta Menchú, pero cuando ya no se pudo seguir con el acompañamiento y seguimiento, las organizaciones descontinuaron los procesos.

Lo anterior, repercute en el hecho que la seguridad digital, como herramienta de protección de las comunicaciones, no es, en la mayoría de las organizaciones, una política organizacional. Las personas entrevistadas relacionan los ataques a su privacidad digital directamente con su seguridad, como una violación a sus derechos humanos.

4.2.2. Anonimato y cifrado

En cuanto al anonimato y cifrado no se encontraron hallazgos significativos, ya que tanto uno como otro no se contemplan dentro del marco legal guatemalteco. Debido a esto tan solo se manifestaron ciertas dudas dado que la constitución guatemalteca no prohíbe ni el anonimato ni el cifrado, de hecho no lo menciona, y de esta manera: "Todo lo que no se prohíbe en la constitución está permitido, hasta que se prohíbe"[186]

Es importante tomar en consideración que en junio de 2015, David Kaye, el Relator Especial de las Naciones Unidas en materia de libertad de expresión, publicó un informe[187] especial haciendo un llamado a las naciones a proteger y promover el cifrado y el anonimato, reafirmando la libertad de usar la tecnología de cifrado y proteger el derecho a expresarse, acceder y leer la información de forma anónima. De este informe, por cierto, la República de Guatemala es peticionaria.[188]

4.2.3. Requisas y allanamientos

La mayoría de las personas entrevistadas dijeron conocer al menos un caso de allanamiento a organizaciones de derechos humanos, entre ellas organizaciones donde laboran. Varios de estos allanamientos han sido en manos de la Fiscalía de Delitos de Propiedad Intelectual, cuyo aparente propósito era solicitar licencias de software de los equipos, pero en la mayoría de los casos la Fiscalía decomisó dichos equipos.

Otros allanamientos a organizaciones de derechos humanos se han producido en contextos determinados y en, por ejemplo, situaciones específicas de denuncia:

186 Entrevista abogada activista derechos humanos. Jornada de validación. Guatemala, octubre, 2015,

187 OACDH, "Informe sobre el cifrado, el anonimato y el marco de derechos humanos",. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx (consultado 4 noviembre, 2015)

188 OACDH, "Petición Guatemala", http://www.ohchr.org/Documents/Issues/Opinion/Communications/States/Guatemala.pdf (consultado 4 noviembre, 2015)

> La organización Guillermo Toriello, quien promueve derechos humanos en comunidades rurales apoyando demandas de acceso a la tierra, fue allanada en 2011 mientras emprendía una campaña internacional de denuncia contra los desalojos ilegales en el departamento Izabal. Se sustrajeron 15 computadoras de escritorio, 2 computadoras portátiles conteniendo información sensible e importante.[189]

Asimismo, destaca el allanamiento de UDEFEGUA, organización que desempeñó un papel esencial en la protección de testigos en el proceso de juicio por genocidio contra Efraín Ríos Montt.

Días antes del allanamiento, la coordinadora general de la organización fue acusada, en un documento[190]publicado por la Fundación Contra el Terrorismo, organización fundada por ex-oficiales militares.[191] Por suerte no se llevaron equipo porque como medida de seguridad durante el proceso la oficina [de Nebaj, en el Departamento de El Quiché] no estaban dejando equipo adentro.

También se suma el caso de la pesquisa al despacho privado del ex Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión para Naciones Unidas, Frank La Rue, ubicado dentro de la organización DEMOS. Este ataque sucedió a mediados de 2013 donde varias computadoras y documentos pertenecientes al Relator Especial fueron sustraídos de su oficina.[192]

No es casualidad que durante estos allanamientos y ataques físicos se extraigan computadoras, discos duros, memorias USB, CDs, ya que estos actos se realizan con la ventajosa intención de desaparecer información sensible, así como de investigar a detalle la labor que ejercen organizaciones de derechos humanos y de la sociedad civil. Ante estos ataques no se ha tomado otra medida más que la denuncia pública.

4.2.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones

Como se ha mencionado anteriormente a lo largo de este capítulo, se toma la Constitución guatemalteca como una salvaguarda para proteger el derecho a la privacidad digital. En este punto es importante recordar que la protección a este derecho se percibe de manera implícita dentro del texto constitucional, ya que no se menciona:

189 FLD, "Guatemala: allanamiento y robo en las instalaciones de la organización Fundación Guillermo Toriello", https://www.frontlinedefenders.org/es/node/15765 (consultado 4 noviembre, 2015)

190 Asociación de Estudios Políticos Militares, "La Farsa del Genocidio en Guatemala – Conspiración Marxista desde la Iglesia Católica", http://asociacionepm.org/wp-content/uploads/2013/04/LA-FARSA-DEL-GENOCIDIO-EN-GUATEMALA5-1.pdf (consultado 4 noviembre, 2015)

191 FLD, "Guatemala: Difamación contra la defensora de derechos humanos Claudia Virginia Samayoa y allanamiento en las oficinas de UDEFEGUA", https://www.frontlinedefenders.org/es/node/22452 (consultado 4 noviembre, 2015)

192 La Prensa Gráfica, "Guatemala: asaltan oficinas de relator de la ONU", http://www.laprensagrafica.com/guatemala--asaltan-oficinas-de-relator-de-la-onu (consultado 4 noviembre, 2015)

> El único instrumento jurídico para la defensa del derecho a la privacidad, entiéndase en el ámbito digital, es la Constitución, junto con ella, están los tratados internacionales de derechos humanos que forman parte del bloque constitucional consagrado por la Constitución. Además, se puede presentar una denuncia penal en el Ministerio Público. Así como hacer uso del amparo.[193]

No obstante, las personas entrevistadas consideran que el derecho a la privacidad digital está siendo limitado por medio de las escuchas telefónicas, reguladas por leyes penales que, dicho sea de paso, han sido muy útiles en algunos casos penales, pero propician la criminalización de formas legitimas de expresión mediante la vigilancia masiva e indiscriminada. La existencia de leyes como la Ley de la Dirección General de Inteligencia Civil, Ley Contra la Delincuencia Organizada, Ley de Pánico Financiero, Ley General de Telecomunicaciones, así como el proyecto de tipificación del ciberdelito son una amenaza latente para la criminalización vinculada al derecho a la privacidad digital y en las telecomunicaciones.

4.3. Inquietudes

4.3.1. Vigilancia

Debido a que no existe una ley o normativa que exprese claramente las obligaciones y compromisos de las empresas privadas, se generan dudas respecto al uso de la información proveniente de las escuchas telefónicas autorizada por la autoridad competente, ya que es de conocimiento de las personas entrevistadas que dicha información también es compartida entre empresas.

Sobre esta inquietud, durante la jornada de validación se trajeron a colación dos casos emblemáticos respecto a las cuestionadas responsabilidades de las empresas:

> Cristina Siekavizza, asesinada por su esposo, caso en que además se involucra a un ente del Estado que colaboró en la desaparición del cuerpo, la empresa Tigo borró los mensajes [de texto] que inculpan al agresor.[194]

> La presentadora [presentadora de televisión nacional, Diana Guerra] a quien le robaron el celular, denunció el robo y los empleados de la empresa telefónica compartieron fotos personales, las cuales se transformaron en imágenes virales [en las redes sociales] a nivel de país. El caso no fue a nivel político sino social"[195]

Este último caso en particular, puede ser penalizado por la Ley contra la Violencia Sexual, Explotación

193 Entrevista abogado activista de derechos humanos. Guatemala, Guatemala, Agosto, 2015.

194 Prensa Libre, "Más de 300 indicios podrían demostrar culpabilidad de Roberto Barreda ", http://www.prensalibre.com/guatemala/justicia/mas-de-300-indicios-podrian-demostrar-culpabilidad-de-roberto-barreda (consultado 4 noviembre, 2015)

195 502, "Publican fotografías íntimas de presentadora tras robo de su celular", http://www.soy502.com/articulo/publican-fotografias-intimas-presentadora-tras-robo-celular (consultado 4 noviembre, 2015)

y Trata de Personas[196], que en su artículo 190 establece que será sancionado con prisión de uno a tres años quien por cualquier medio sin el consentimiento de la persona, atentare contra su intimidad sexual y se apodere o capte mensajes, conversaciones, comunicaciones, sonidos, imágenes en general o imágenes de su cuerpo, para afectar su dignidad. Además de esta, no hay herramientas que favorezcan el proceso.

Durante este proceso se generaron las siguientes dudas sobre el tema:

- ¿Cuál es el límite que hay entre la investigación criminal y la investigación preventiva y el uso de las tecnologías?
- ¿Cómo regular el uso de la inteligencia para las operaciones criminales?
- Las acciones de la Dirección General de Inteligencia Civil para recolectar información ¿contravienen todos los principios de obtención de información?
- Los acuerdos entre el gobierno y las empresas de telecomunicaciones no son públicas para la sociedad civil y, al momento de solicitar la información, puede ser denegada.

4.3.2. Anonimato y cifrado

Aunque el anonimato y cifrado no se menciona dentro del ordenamiento jurídico guatemalteco, existe ya una iniciativa de ley contra el ciberdelito. Esto ha generado manifestaciones aisladas, que aún no se materializan de forma colectiva, contra esta iniciativa por parte de personas individuales, no organizadas, conocedoras de la tecnología: “El hecho de saber que estás siendo vigilado/escuchado, te cohíbe para expresarte. De hecho, debido a la historia reciente guatemalteca, hay mucha gente que aún tiene miedo de decir abiertamente que participó en la guerra”.

Es importante resaltar que la aprobación de la ley contra ciberdelitos trae consigo la conformación de un comité operativo, unidad que dará respuesta a incidentes de seguridad informática, aún no especificados, integrado por el Ministerio de Defensa, Ministerio de Relaciones Exteriores, Ministerio Público, Ministerio de Gobernación, la Superintendencia de Bancos, Superintendencia de Comunicaciones y la Secretaría de Consejo Nacional de Seguridad.

Durante este proceso se generaron las siguientes dudas sobre el tema:

- ¿Qué puedo hacer si me piden una contraseña?

196 Guatemala. “Ley Contra la Violencia Sexual, Explotación y Trata de Personas”, http://ww2.oj.gob.gt/justiciadegenero/wp-content/uploads/2015/03/Ley-contra-la-Violencia-sexual-explotaci%C3%B2n-y-trata-de-personas.pdf, art. 190 (consultado: 4 noviembre, 2015)

- ¿En qué casos estoy en la obligación de entregar mi contraseña, y en qué casos no?
- ¿Si me niego a entregar una contraseña pueden inculparme de desacato?

4.3.3. Requisas y allanamientos

Sobre las requisas y allanamientos no se generaron mayores dudas e inquietudes al respecto.

4.3.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones

Las personas entrevistadas consideran que es necesario revisar la vigencia de leyes que tienen que ver con los medios de comunicación y con lo que publican. Por ejemplo, la Ley de Emisión del Pensamiento obliga a los medios a guardar registro por seis (6) meses de las grabaciones, comunicaciones, emisiones de radios, los periódicos, imágenes y estos registros pueden ser, a su vez, entregados por orden de juez para casos particulares.

Durante este proceso se generaron las siguientes dudas sobre el tema:

- ¿Cuál es el procedimiento legal de interceptación de datos y escuchas telefónicas?
- ¿Qué normas regulan la retención de datos en las empresas de telecomunicación?
- ¿Cuál es el debido proceso para la solicitud de acceso a la información?

5. Conclusiones nacionales

La discusión sobre el derecho a la privacidad no está en la discusión política-social guatemalteca a pesar de su importancia. Aunque podemos encontrar algunos informes de situación producidos y publicados por ONG nacionales u organismos internacionales, y una incipiente producción académica, el tema aún no tiene un lugar prominente en la agenda nacional.

Si bien la legislación guatemalteca contiene una sólida protección a derechos inherentes y fundamentales de las personas, como el derecho a la inviolabilidad del domicilio, de la correspondencia y de las escuchas telefónicas, no menciona expresamente el derecho a la privacidad. Este derecho se reconoce únicamente de manera implícita en el Artículo 44 constitucional al establecer que los "derechos y garantías que otorga la Constitución no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana". A pesar de esto, Guatemala tiene una sólida protección constitucional desde la Constitución Federal de 1823, la cual se consolidó en 1879 con la prohibición clara y expresa de violar la correspondencia y los documentos privados de las personas, y estableciendo que este derecho solamente puede ser limitado por juez competente imparcial e independiente. La Constitución actual amplía su protección a cualquier tipo de comunicación actual o que exista en el futuro.

A pesar de lo anterior, existen leyes como la Ley de la Dirección General de Inteligencia Civil, Ley Contra la Delincuencia Organizada, Ley de Pánico Financiero y el Código Procesal Penal, las cuales son una amenaza latente para el derecho a la privacidad digital y en las telecomunicaciones.

Aunado a lo anterior, los tratados internacionales en materia de derechos humanos ratificados por Guatemala forman parte del bloque de constitucionalidad y pueden ser utilizados por cualquier persona para la defensa de su derecho a la privacidad de las comunicaciones. Este aspecto es de suma importancia porque amplía la protección del derecho a la privacidad a cualquier tipo de comunicación y documentación de la persona, lo cual incluye –por supuesto– los metadatos contenidos en las comunicaciones.

La protección anterior permite que cualquier persona que considere que su derecho a la privacidad está siendo vulnerado o que existe una amenaza pueda presentar una denuncia ante el Ministerio Público o la Procuraduría de los Derechos Humanos; interponer un amparo, siempre que se hayan cumplido los requisitos para este; o presentar una acción de inconstitucionalidad si considera que alguna normativa de carácter general lo vulnera.

Con el objeto de proteger su privacidad, las personas tienen derecho al anonimato en internet y a la utilización de cifrado, lo cual está en consonancia con una interpretación de los tratados

internacionales en materia de derechos humanos ratificados en Guatemala. 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 que Guatemala ha suscrito. Analizando estas obligaciones suscritas por 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 no es clara ni precisa sobre las causales y formalidades legales que se deben cumplir.

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.

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

Para poder entender el actual contexto guatemalteco, resulta indispensable tomar en consideración la historia guatemalteca, los años de dictaduras militares en los cuales se estigmatizó a víctimas y organizaciones sociales, convirtiéndoles en objetos de represión. En general, los principales ataques que vulneran el derecho a la privacidad, en internet y las telecomunicaciones en Guatemala se ejecutan desde instancias del Gobierno. Paralelamente, se evidencia la labor del ejército en el tema de seguridad con la asesoría del gobierno de los Estados Unidos.

Es de conocimiento de profesionales activistas de derechos humanos que el derecho a la privacidad digital está siendo limitado por medio de las escuchas telefónicas, reguladas por leyes penales. Un hallazgo sumamente interesante y oportuno es La Ley contra la Violencia Sexual, Explotación y Trata de Personas, como mecanismo de protección al derecho a la privacidad digital pues establece sanciones para quien por cualquier medio, sin el consentimiento de la persona, capte mensajes, conversaciones, comunicaciones, sonidos, e imágenes en general para afectar la dignidad de la persona.

Bibliografía

Libros

OCDE/CEPAL. 2012. *Perspectivas económicas de América Latina para 2012*. OCDE, 2012.

OGP..2014. *Segundo Plan de Acción Nacional de Gobierno Abierto, Guatemala 2014-2016.* Guatemala: Open Govermment Partnership, 2014.

Renata Ávila, Renata y Alejandra Gutiérrez, Alejandra. 2013. *Los Medios Digitales: Guatemala*. Guatemala: Open Society Foundation, 2013.

Tesis

Boj Saavedra, Lourdes. 2012. "Análisis sobre la ilegalidad en el funcionamiento del Sistema de Información en Red "INFORNET" y el respeto al derecho a la privacidad, seguridad y dignidad." Tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2012.

Díaz Sontay, Julio. 2011. "Análisis del derecho a la intimidad en el ordenamiento jurídico guatemalteco referido a empresas mercantíiles que comercializan datos personales". Tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2011.

González Rivera, Sandra. 2007. "La regulación del derecho a la intimidad en el derecho constitucional guatemalteco." Tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2007.

Juarez del Cid, Vilma. 2014. "El rol del Estado en la tutela del derecho fundamental de privacidad de los usuarios del servicio de Internet como producto de la tecnología moderna." Tesis de Licenciatura, Facultad de Ciencias Jurídicas y Sociales, 2014.

Mazariegos de León, Max. 2012. "El correo electrónico o SPAM y el derecho humano a la intimidad o privacidad; Visión desde el ámbito del derecho internacional de los Derechos Humanos." Tesis de Maestría, Facultad de Ciencias Jurídicas y Sociales, 2012.

Portillo Menjívar, William. 2012. "El conflicto que existe entre la libertad de la información y la vida privada de las personas en la República de Guatemala". Tesis de Licenciatura, de Ciencias Jurídicas y Sociales, 2012.

Legislación nacional

Corte de Constitucionalidad. Inconstitucionalidad general parcial. Congreso Jurídico Guatemalteco de 1965.

Guatemala. "Constitución Política de la República de Guatemala". Asamblea Nacional Constituyente (1985).

Guatemala. “Ley de Amparo, Exhibición Personal y de Constitucionalidad”. Asamblea Nacional Constituyente (1986).

Guatemala. “Ley de Emisión del Pensamiento”. Congreso de la República de Guatemala (1985).

Guatemala. “Ley del Organismo Judicial”. Congreso de la República de la Guatemala (1989).

Guatemala. “Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas”. Congreso de la República (2008).

Jurisprudencia

Corte Interamericana de Derechos Humanos. Caso Tristán Donoso vs. Panamá. San José: CIDH: 2009.

Corte Interamericana de Derechos Humanos. Escher y otros vs. Brasil. San José: CIDH: 2009.

Costa Rica. “Constitución Política de la República Federal de Centroamérica.” (1921).

Naciones Unidas. “Pacto Internacional de Derechos Civiles y Políticos”. Naciones Unidas (1966).

Organización de Estados Americanos. “Convención Americana de Derechos Humanos”. OEA (1969).

Honduras

Edy Tábora Gonzales

1. Antecedentes

El Estado hondureño ha ratificado los principales instrumentos internacionales sobre derechos humanos, como la Convención Americana de Derechos Humanos y el Pacto Internacional de Derecho Civiles y Políticos, así, Honduras es un país con una enorme producción de normas para la protección, pero también para la criminalización.

A nivel político, el Estado ha abordado la necesidad de utilizar herramientas para la intervención a las comunicaciones como un mecanismo de ataque a la delincuencia organizada: la justificación de la vigilancia es la seguridad pública. Sin embargo, al analizar las normas que regulan estas intervenciones, nos damos cuenta que las mismas son aplicables a la investigación de cualquier delito, incluidos los delitos comunes o políticos, lo cual nos genera dudas democráticas.

1.1. Estado de la discusión nacional

En el país, es mínima la discusión sobre el "derecho a la privacidad, relacionada con la criminalización, vigilancia y/o censura digital, en internet y en las telecomunicaciones". Encontramos poco desarrollo académico o de la sociedad civil respecto del derecho al acceso a internet y las vigilancias desde las nuevas tecnologías, sin embargo sí encontramos normas regulatorias sobre el acceso a internet y las vigilancias por parte del Estado.

Para efectuar el análisis que se presenta, a continuación se revisaron las fuentes secundarias producidas por organizaciones civiles como Artículo 19, el Instituto Nacional de Derechos Humanos de Chile, la Coalición Dinámica por los Derechos y Principios de Internet, la Asociación para el Progreso de las Comunicaciones (APC), y el Centro de Estudios en Libertad de Expresión y Acceso a la Información de la Universidad de Palermo (CELE), entre otros, sin encontrar trabajos relacionados con el contexto hondureño. Por otra parte, se revisaron los informes producidos por los mecanismos de protección de derechos humanos tanto del Sistema Universal (Relatoría Especial de Libertad de Expresión y de Defensores/as de Derechos Humanos) así como del Sistema Regional (Relatoría Especial de la Libertad de Expresión y de Defensores/as de Derechos Humanos), en estos informes se encontraron algunas referencias importantes al tema. Por otra parte, se visitaron librerías, organizaciones de derechos humanos y la biblioteca (en físico y en digital) de la Universidad Nacional Autónoma de Honduras, pero no se encontraron investigaciones relacionadas con el tema.

En la búsqueda en internet se utilizaron los descriptores "privacidad, seguridad de la información, seguridad informática, telecomunicación, tecnologías de información y comunicación, criminalización, defensores/as de derechos humanos, intervención de las comunicaciones", sin embargo, se encontró muy poca información de utilidad para esta investigación.

En la sociedad civil hondureña, los únicos documentos que se encontraron fueron los producidos por el "Comité por la Libre Expresión" (C LIBRE)[1], que en sus informes anuales de 2012, 2013 y 2014, sobre todo el de 2013 en el capítulo III titulado "Espionaje estadounidense somete a Honduras a un régimen mundial de censura previa, una nación vigilada, todos bajo sospecha"[2], aborda la situación de afectación al derecho a la privacidad y la libertad de expresión por parte del gobierno de Estados Unidos a partir de los programas de seguridad publica implementados en la región centroamericana con el consentimiento de los gobiernos locales.

En la academia, es importante el desarrollo que hizo Hedme Castro Sierra en su tesis de máster "Aplicación de los derechos humanos a la intervención de las comunicaciones; internet libre y comunicaciones seguras en la labor de promoción y defensa de los derechos humanos"[3], en la que hizo un abordaje sobre la consecuencias a los derechos humanos con la aprobación de la Ley Especial sobre la Intervención de las Comunicaciones Privadas[4]; además esta tesis trata otros temas como: sociedad de vigilancia, derechos humanos, seguridad digital, comunicaciones privadas, libertad de expresión, reunión pacífica, espionaje, poder, Estado.

1.2. Brecha digital

Para abordar el tema de la privacidad digital es necesario darnos cuenta del estado actual sobre el acceso que tiene la población a la tecnología relacionada con este derecho (computadoras, telefonía e internet). Esto porque las intromisiones a la privacidad digital se hacen a través de las vigilancias a estos aparatos, de tal manera que se vuelve necesario analizar la brecha digital.

En Honduras se aprobó la Ley de Alfabetización en Tecnologías de Información y Comunicación, existe una definición del concepto "brecha digital" que la detalla como "la diferencia socio económica existente entre grupos, comunidades y personas según el acceso o falta del mismo, así como su calidad, en el uso de internet y demás Tecnologías de la Información y Comunicación, lo que genera inequidad social y económica"[5].

1 Comité por la Libre Expresión (C-LIBRE), http://www.clibrehonduras.com/publicaciones

2 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013* (Tegucigalpa, M.D.C., Honduras, 2013), 61-73, http://www.clibrehonduras.com/content/informe-libertad-de-expresi%C3%B3n-2013 (consultado: 4 de noviembre, 2015)

3 Sierra Castro, Hedme. "Aplicación de los derechos humanos a la intervención de las comunicaciones; Internet libre y comunicaciones seguras en la labor de promoción y defensa de los derechos humanos". Tesis de maestría, Centro Internacional de Estudios Políticos, Universidad Nacional de San Martín, http://www.unsam.edu.ar/ciep/wp-content/uploads/2014/11/Hedme-Sierra-Castro.pdf (consultado: 4 de noviembre, 2015)

4 Honduras "Ley Especial sobre la Intervención de las Comunicaciones Privadas" La Gaceta No. 32, 731 (26 enero, 2012).

5 Honduras. "Ley de Alfabetización en Tecnologías de Información y Comunicación", Poder Legislativo, artículo 1.

Según el Índice de Desarrollo de las Tecnologías de la Información y la Comunicación (IDI)[6], en 2011 Honduras ocupaba la posición 107 de 155 países evaluados, y siguiendo el Índice de Desarrollo de Gobierno Digital (EGDI, por sus siglas en inglés) generado por Naciones Unidas a través de una encuesta llamada "e-Government", en 2012 Honduras se encontraba en la posición 117 de 190 países[7].

1.2.1. Acceso a computadoras

Un informe del año 2013 de la Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI), establece que el porcentaje de hogares con computadoras en el país era de 12.9% [8].

Según cifras oficiales del Estado hondureño, en 2013 el 20.1% de los hogares poseían computadora y la brecha digital entre el área urbana y rural de Honduras era del 24.7%. En el área urbana, el 32.7% de los hogares hondureños poseía una computadora, mientras en la zona rural apenas el 7.9% disponía de esta herramienta tecnológica[9]. Por otra parte, el porcentaje de personas que "nunca o casi nunca" usan la computadora por motivos de ocio / interés personal, según país es de un 70%"[10]. En cuanto al "porcentaje de personas que diariamente usan la computadora por motivos de ocio / interés personal y regularidad de uso, según país, Honduras presenta un 6%"[11].

1.2.2. Acceso a teléfonos

1.2.2.1. Telefonía fija

Para finalizar el año 2014, "las líneas telefónicas fijas resultaron en un total de 532,583 abonados. La cantidad de personas usuarias de teléfonos fijos tuvo un decrecimiento de 1.44% con respecto al trimestre junio-septiembre 2014". La densidad correspondiente al número de líneas telefónicas fijas por cada 100 habitantes, "alcanzó un valor de 6.1 al finalizar el tercer trimestre del año 2014, lo que corresponde a que 6 de cada 100 hondureños y hondureñas posee una línea telefónica fija".[12]

---

6 El Índice de Desarrollo de las Tecnologías de la Información y la Comunicación (IDI) evaluado por la Unión Internacional de Telecomunicaciones (UIT), indican que Honduras ocupa la posición 107 de los 155 países en 2011, véase: Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN), *Agenda Digital de Honduras, 2014-2018* (Tegucigalpa, M.D.C.: Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN), 2013), 12.

7 Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN), *Agenda Digital de Honduras, 2014-2018*, 15.

8 Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI), *Informe de la Encuesta latinoamericana de hábitos y prácticas culturales 2013* (Madrid: Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura, 2013) http://oei.es/xxivcie/encuestalatinoamericana2013.pdf (consultado: 17 mayo, 2015)

9 Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN), *Agenda Digital de Honduras, 2014-2018*, 14.

10 Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI), *Informe de la Encuesta latinoamericana de hábitos y prácticas culturales 2013.*

11 Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI), *Informe de la Encuesta latinoamericana de hábitos y prácticas culturales 2013.*

12 Comisión Nacional de Telecomunicaciones (CONATEL), *Desempeño del sector telecomunicaciones. Informe Trimestral, cuarto trimestre 2014 (*Tegucigalpa, M.D.C.: Comisión Nacional de Telecomunicaciones (CONATEL), 2015), 3, http://www.conatel.gob.hn/doc/indicadores/2015/Desempe%C3%B1o_del_Sector_De_Telecomunicaciones_4to_Trimestre_2014.pdf (consultado: 12 julio, 2015)

1.2.2.2.Telefonía móvil

Las líneas telefónicas móviles alcanzaron "un total de abonados de 7, 725,092 al finalizar el año 2014". La densidad correspondiente al número de líneas telefónicas móviles "por cada 100 habitantes, alcanzó un valor de 88.54 al finalizar el año, lo que representa que 88 de cada 100 hondureños y hondureñas posee una línea telefónica móvil". Del total de abonados de telefonía móvil en el país, "562,412 abonados pertenecen a la modalidad de post-pago, lo que representa el 7. 28% del total de abonados y 7,162,680 pertenecen a la modalidad de pre-pago, lo que representa el 92.72% del total de abonados".[13]

1.2.3. Acceso a internet

El acceso a internet continúa siendo el problema primario relacionado con la brecha digital en Honduras. El número de personas suscriptoras o abonadas de internet fijo alcanzó un "total de 159,276 al finalizar el año, observándose un crecimiento de 21.24%" con respecto al trimestre junio/ septiembre 2014. El número de personas suscriptoras o abonadas de internet móvil alcanzó un total de 1,350,109, observándose un crecimiento de 19.73% con respecto al trimestre junio/septiembre 2014. El número de personas usuarias de internet por cada 100 habitantes "alcanzó un valor de 17.8 durante el año 2013, lo que representa que 17 de cada 100 hondureños y hondureñas acceden a internet. Se observa un incremento del 16.4% en la cantidad de hondureños y hondureñas que utilizan el internet con respecto al año 2012".[14]

1.2.3.1 Personas suscriptoras de internet con conectividad de banda ancha

El número de personas suscriptoras fijos de internet con conectividad de banda ancha alcanzaron un valor de 114,483 al finalizar este año, observándose un decrecimiento de 5.76% con respecto al trimestre anterior. Se percibe que descendió el número de personas suscriptoras en banda ancha con respecto al trimestre anterior en vista que ahora la persona suscriptora de banda ancha paso de 512 Kbps a 1Mbps, según resolución NR013/14. El número de personas suscriptoras móviles de internet con conectividad de banda ancha fue de 1,350,109 observándose un crecimiento de 23.4% con respeto al trimestre anterior.

13 Comisión Nacional de Telecomunicaciones (CONATEL), *Desempeño del sector telecomunicaciones. Informe Trimestral, cuarto trimestre 2014,* 4-5.

14 Comisión Nacional de Telecomunicaciones (CONATEL), *Desempeño del sector telecomunicaciones. Informe Trimestral, cuarto trimestre 2014,* 7.

1.2.3.2 Densidad de personas suscriptoras de internet con conectividad de banda ancha por 100 habitantes

Al último trimestre de este año la densidad de personas abonadas de internet fijo con conectividad de banda ancha por cada 100 habitantes alcanzó un valor de 1.31, lo que representa que 1 de cada 100 hondureños y hondureñas está suscrito al internet de banda ancha a través de conexiones de internet fijo. La densidad de personas usuarias de internet móvil con conectividad de banda ancha por cada 100 habitantes alcanzó un valor de 15.47 para finales del año, lo que representa que 15 de cada 100 hondureños y hondureñas están suscritos al internet de banda ancha a través de conexiones de internet móvil.[15]

La diferencia en cuanto al acceso entre zonas urbanas y rurales es sumamente significativa, de manera que en las primeras el acceso a internet llega al 31.1%, mientras que en las segundas es de apenas un 6% (datos de 2012).[16]

La disponibilidad de servidores seguros (aquellos que utilizan tecnología de encriptación para realizar transacciones en la web, lo cual es importante para contar con mayor seguridad al enviar y recibir información digital a través de la red)[17], de internet por cada millón de habitantes es de las más bajas de la región[18].

En el país se inició un proyecto denominado Agenda Digital 2014-2018, que establece como finalidad reducir la brecha digital. El documento determina que

> la Agenda comprende cuatro ejes estratégicos (…) con líneas de acción y un conjunto de iniciativas. El primer eje se orienta a incrementar los índices de penetración de Internet y otras tecnologías de información (...), así como el reforzamiento de la infraestructura de telecomunicaciones y el desarrollo de la banda ancha; el segundo eje se concentra en un conjunto de iniciativas de gobierno digital (...) el tercer eje tiene como propósito fortalecer la inclusión de la formación y capacitación en TIC en los diferentes niveles del sistema educativo (...) y, el cuarto eje enfatiza en los aspectos legislativos y de marco institucional, como elementos básicos para el desarrollo de las TIC.[19]

La Agenda Digital maneja como concepto sobre las las TIC, que las Tecnologías de Información y Comunicación son factores que impulsan la competitividad y, con ello, el crecimiento económico y la productividad de los países.[20]

15 Comisión Nacional de Telecomunicaciones (CONATEL), *Desempeño del sector telecomunicaciones. Informe Trimestral, cuarto trimestre 2014,* 8.
16 Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN), *Agenda Digital de Honduras, 2014-2018*, 9.
17 Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN), *Agenda Digital de Honduras, 2014-2018*, 14.
18 Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN), *Agenda Digital de Honduras, 2014-2018*, 14.
19 Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN), *Agenda Digital de Honduras, 2014-2018, 7.*
20 Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN), *Agenda Digital de Honduras,*12.

El ordenamiento jurídico que propone implementar la Agenda Digital en el país, incluye varias leyes abordadas desde lo mercantil, salvo una que se refiere a la protección de datos, pero ninguna se refiere a la protección frente a las vigilancias en internet y en las telecomunicaciones ni tampoco reformas a las leyes ya existentes que el Estado ocupa para realizar las vigilancias:

a) Ley de Tecnologías de la Información y Comunicación.

b) Ley de Firma Electrónica (aprobada y vigente)[21]

c) Ley Fondo Social de Telecomunicaciones y Tecnologías de la Información (FOSTEL).

d) Ley de Comercio Electrónico[22].

e) Plan nacional de banda ancha.

f) Ley de Protección de la Información[23].

g) Ley de Gobierno Digital.

h) Ley de Delito Cibernético[24].

1.3. Criminalización de defensoras y defensores de derechos humanos

En diciembre de 2014, la Comisión Interamericana de Derechos Humanos realizó una visita *in loco* a Honduras y emitió un informe preliminar que contiene algunos datos muy importantes que reflejan la situación de las y los defensores de derecho humanos en el país[25]:

21 Honduras "Ley de Firmas Electrónicas" La Gaceta No. 33, 301 (11 diciembre, 2013)

22 Honduras "Ley de Compras Eficientes Transparentes a través de Medios Electrónicos" La Gaceta No. 33, 497 (21 marzo, 2013)

23 Ya existe un Anteproyecto denominado "Ley de Protección de Datos Personales y Acción de Habeas Data de Honduras", de enero de 2014.

24 En el Código Penal ya se han establecido tipo penales relacionados con delito cibernético, mediante reformas de 2004 y 2011: art. 242: Incurrirá en las penas de Estafas y otros Fraudes: (…) 14) Quien cometiera fraude en telecomunicaciones, medios u ondas y sistemas informáticos o de la información como tráfico irregular, a través de la reoriginación (refilling),de llamada internacional (callback), ingreso de tráfico internacional de forma ilegal evitando pagar las debidas tasas de terminación entre operadores internacionales (bypass), piratería informativa (hackeo), reventa no autorizada y clonación de números telefónicos móviles. Art. 394-I. Utilización Indebida de Sistemas de Procesamiento de Datos: Quien acceda ilegalmente a los sistemas de procesamiento de datos de las instituciones supervisadas, para alterar, borrar, dañar o sustraer registros, archivos u otra información de la institución o de sus clientes, en beneficio propio o ajeno, será sancionado con reclusión de tres (3) a seis (6) años cuando el monto de lo defraudado no exceda de diez mil (10,000.00) lempiras y de seis (6) a doce (12) años cuando exceda de dicho monto. En las mismas penas incurrirán quienes bajo cualquier procedimiento ingrese o utilice indebidamente la base de datos de una institución supervisada para sustraer dinero mediante transferencias electrónicas de una cuenta a otra en la misma o diferente institución. Véase: Honduras "Código Penal"La Gaceta No. 24, 264 (12, marzo 1984).

25 Comisión Interamericana de Derechos Humanos. *Observaciones Preliminares sobre la situación de los derechos humanos en Honduras*. (Washington, D.C.: CIDH, 2014), https://www.oas.org/es/cidh/prensa/comunicados/2014/146A.asp (consultado: 14 junio, 2015)

> los defensores y las defensoras de derechos humanos son en Honduras blancos de ataques por parte de aquellas personas que han sido señaladas como responsables de violaciones a derechos, o bien, de sectores y grupos que tienen intereses opuestos a sus causas. La Comisión observó con preocupación las cifras presentadas por el Comité de Familiares Desaparecidos en Honduras (COFADEH), según las cuales desde 2010 habrían 3,064 criminalizaciones, como resultado del uso indebido del derecho penal para amedrentar a defensores y defensoras; 22 asesinatos; 2 desapariciones; 15 secuestros; 88 casos de robos de información y 53 sabotajes a los vehículos donde se transportaban.[26]

En la sociedad civil encontramos varios informes sobre la criminalización de defensores y defensoras de derechos humanos, emitidos por parte de organizaciones de derechos humanos como el Comité de Familiares Desaparecidos de Honduras (COFADEH)[27] y el Comité por la Libre Expresión (C LIBRE). El que recoge la situación sobre vigilancia a defensores y defensoras de derechos y políticos en el país es un documento de 2013[28] en el cual encontramos un análisis importante.

Según este documento, con la entrada en vigencia del "Plan Mérida y la Iniciativa Regional de Seguridad para Centroamérica (CARSI)", la región estaría transitando de una guerra anti narcóticos hacia formas de contraterrorismo. Intentar identificar la narcoactividad como una posible narco guerrilla que controla determinados territorios nacionales sirve para introducir operaciones especiales de una guerra no convencional, irregular, en la que la vigilancia y presión a las organizaciones sociales y a los defensores de derechos humanos se vuelve estratégica. Siendo sustancial, en ella, la aplicación de operaciones psicológicas, el espionaje y el engaño en la información (…) Consorcios mediáticos, sobre todo tras el golpe de Estado en Honduras, lanzaron historias suspicaces, descontinuadas y poco profundas sobre la existencia de grupos irregulares en El Aguán, contadas por altos funcionarios que sugirieron vínculos con organizaciones enlistadas por EE.UU. como terroristas (FARC, ETA, Hezbolah).[29]

El informe mencionado dice que

> un entramado de espionaje mundial por la Agencia de Seguridad Nacional (NSA) estadounidense, compone una red que atrapa y perturba la libertad de información y ejecuta una vigilancia y censura mundial que violenta la libre expresión de millones de personas. Incluida Honduras. El 2013 es un año en sumo violento contra esos derechos, atrapados por tal fuerza dominante que se impone, solapada y mentirosa, en las estructuras comunicativas informativas, personales y nacionales, so pretexto de leyes anticrimen. (...) Con programas como el *Xkeyscore,* revelado por el periódico The Guardian en julio de 2013, se utilizan técnicas sofisticadas para rastrear "trillones" de comunicaciones privadas. La NSA desarrollaría una vigilancia marcada a organizaciones sociales, gobiernos, mandatarios y al sistema industrial empresarial, con unos 150 centros de espionaje en varios países. Y,

26 Comisión Interamericana de Derechos Humanos. Observaciones Preliminares sobre la situación de los derechos humanos en Honduras, 2014.

27 Comité de Familiares Desaparecidos de Honduras (COFADEH), http://www.cofadeh.hn/

28 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013.*

29 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013*, 13.

> muy posible, una sede instalada en Honduras, otros países de América Central y México, a través de las Iniciativas Mérida y de Seguridad para Centroamérica (CARSI).[30]

En el mismo informe, se establece que Honduras pasó de gastar cinco millones dos mil seiscientos dólares, en 2009, a mil trecientos noventa y un millones de dólares en los dos años siguientes de la CARSI (2011), de esta cantidad, mil trecientos ochenta y ocho millones se destinó a la compra de "*Equipos Electrónicos de uso Militar*, una categoría que incluye: radares, equipos electrónicos para combate, radios, equipos electrónicos para vigilancia y artículos similares".[31]

Siguiendo el documento,

> Honduras no solo es vigilada, también estaría albergando un centro de espionaje mundial regional, según un mapeo de uno de los documentos revelados por Snowden. La vigilancia es parte oficial de la iniciativa Mérida en México, y sería, también de CARSI en Centroamérica. Incluye, legalmente, un centro de observación en El Salvador. Los indicios de equipos instalados recaen sobre las embajadas. Según informes, ninguna de las empresas transnacionales de telefonía y de internet, pagadas con dinero, se habría resistido, en absoluto, a cooperar en la vigilancia".[32]

El 31 de julio, The Guardian publicó la existencia del programa *XKeyscore*, de espionaje masivo que opera con 700 servidores en 150 sitios ubicados en todo el planeta, incluyendo Honduras y países centroamericanos. Así, evidencia un mapa publicado en uno de los materiales de entrenamiento.[33]

C-Libre documentó que

> tras el golpe de Estado de 2009, aumentaron en Honduras la percepción y las denuncias públicas, no investigadas, de dirigentes sociales y de sus organizaciones; de políticos y de otras personas, de tener intervenidos sus teléfonos fijos, celulares, y observadas y atacadas sus computadoras y sistemas. El reclamo se intensificó en el tiempo de elecciones, de las internas en 2102 y de las generales, en 2013. Entre otros, el excandidato del Partido Anticorrupción (PAC), Salvador Nasralla, denunció ante C-Libre que tenía su teléfono intervenido, hacía un año; por lo que calificó esto como un delito y señaló directamente al Partido Nacional, en el Gobierno.[34]

Todo el proceso electoral de 2012-2013 en Honduras se basó en el manipuleo evidente de la información pre y pos electoral. Entre los rasgos que, por su evidencia burda, son de rápida identificación, es posible mencionar[35] la vigilancia telefónica y electrónica, incluida la militarización del área de transmisores de medios audiovisuales; trabas y adulteración de la información contenida en documentos electorales

30 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013*, 14.
31 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013*, 56.
32 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013*, 62.
33 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013*, 71.
34 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013*.
35 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013*, 74.

impresos y electrónicos (papeletas, actas, credenciales).[36] El mismo C-Libre denunció las intrusiones a celulares de sus integrantes y a su sistema electrónico entre abril y mayo de 2012.[37]

El ex-presidente Porfirio Lobo en 2012 advirtió a los y las funcionarias que tuvieran cuidado porque sus conversaciones en teléfonos celulares estarían vigiladas con una tecnología tan avanzada que podían ser localizados, aún si estos estuvieran apagados. El programa puede tomar fotografías cada tres segundos, incluso en tercera dimensión, independientemente de si el "chip" o tarjeta SIM se cambie a otro teléfono celular, se permitió detallar el gobernante.[38]

El periódico Conexihon de Honduras, publicó el 6 de julio de 2015 que el gobierno de Honduras pagó trecientos cincuenta y cinco mil dólares desde 2014 a la compañía Hacking Team[39] para espiar a sus ciudadanos.[40] De acuerdo con los documentos que fueron revelados por hackers anónimos, los documentos de contratación entre el Estado de Honduras y la empresa en mención fueron firmados por el director de la Dirección Nacional de Investigación e Inteligencia.

1.4. Conclusiones preliminares

En Honduras, la investigación por parte de la sociedad civil y la academia para la discusión los derechos humanos que no tienen que ver con los violaciones tradicionales (vida, integridad física) es mínima, lo que dificulta avanzar en la exigencia de protección de los derechos como el derecho a la privacidad. También es escasa la investigación en el tema de la vigilancia en internet y en las telecomunicaciones.

Al analizar la brecha digital en Honduras nos damos cuenta que es en la telefonía celular donde esta más reducida y, asimismo, que el acceso a internet crece a través del uso de celulares y que la mayor parte de las conexiones se hacen a través de los mismos, esto implica que hay terreno fértil en el país para las vigilancias en internet y en las telecomunicaciones.

La criminalización hacia defensores y defensoras y políticos mediante las vigilancias en internet y las telecomunicaciones se han hecho notorias después del golpe de Estado y agravadas en las cercanías a las elecciones de 2012 y 2013. Son preocupantes las publicaciones mencionadas en esta sección, que refieren a Honduras como un consumidor de servicios de espionaje y como centro de espionaje mundial.

36 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013*, 75.
37 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013*, 63.
38 Comité por la Libre Expresión (C LIBRE), *Informe Libertad de expresión 2013*, 69.
39 La controvertida compañía es acusada de diseñar y vender herramientas de software destinado al espionaje.
40 Conexihon, "Honduras: Gobierno paga L.8 millones en software de espionaje telefónico". *Conexihon, Sec. Libertad de Expresión*, 6 de julio de 2015.

2. Marco legal nacional

La presente sección desarrolla las protecciones constitucionales del derecho a la privacidad únicamente en los contextos de la vigilancia del Estado y del sector privado cuando actúa en colaboración con el Estado. El texto describe la normativa de la materia en el ámbito constitucional, jurisprudencia de altas cortes, legislación y reglamentos internos relacionado a la vigilancia. El objetivo en términos prácticos es contar con las herramientas para posteriormente responder las interrogantes que las defensoras y defensores de derechos humanos tienen frente a la vigilancia cometida por el Estado y la potencial criminalización de los usos de herramientas necesarias para proteger su privacidad o la enseñanza de esos usos.

2.1. Tratados internacionales

De acuerdo con la Constitución de la República de Honduras, en su artículo 15 "los tratados internacionales celebrados por Honduras con otros Estados, una vez que entran en vigor, forman parte del derecho interno". En este sentido, se desprende que el Estado de Honduras asume expresamente el proceso de incorporación del derecho internacional,[41] aunque algunos autores consideran —evocando la clásica concepción monista que juzga que los tratados internacionales son parte del derecho interno desde el momento en que son ratificados por el Estado— que Honduras asume un «monismo moderado», dado que si bien reconoce la primacía del derecho internacional sobre el derecho interno; esta no es automática sino que se produce mediante determinados mecanismos de adaptación, como la aprobación legislativa por mayoría simple o calificada que requiere la reforma constitucional.[42]

De cualquier manera, en materia de derechos humanos, el derecho internacional, una vez ratificado de forma soberana por el Estado hondureño, se amalgama con el derecho interno y produce derechos y obligaciones no solo para los poderes públicos, sino también para los particulares; y sus posibles violaciones deben ser prevenidas, tratadas y reparadas con la eficacia debida, so pena de que los órganos supranacionales encargados de vigilar el acatamiento de las normas internacionales determinen el incumplimiento de las obligaciones internacionales por parte del Estado.[43]

Con respecto a la jerarquía de las normas internacionales, la Constitución hondureña en su artículo 18 señala que en

41 Joaquín Mejía, *Honduras y los sistemas internacionales de protección de derechos humanos, (*Tegucigalpa: Editorial Casa San Ignacio, 2010), 151-153.

42 Jorge Ramón Hernández Alcerro,*Comentarios a la Constitución de la República de Honduras de 1982 (Los Tratados en la Constitución),* (Tegucigalpa: Editorial Universitaria, 1982), 38.

43 Joaquín Mejía, *Una mirada a la Justicia Constitucional hondureña, desde la óptica de los Derechos Humanos,* 34.

> caso de conflicto entre el tratado o la convención y la Ley prevalecerá el primero, o sea que los tratados asumen un rango supralegal. Lo cual lo refuerza el artículo 320 de la Constitución, al establecer que en caso de incompatibilidad entre una norma constitucional y una legal ordinaria, se aplicará la primera.[44]

Así, para la Constitución hondureña, el derecho internacional y el derecho interno constituyen un sistema normativo unitario, por lo que la validez del segundo depende primordialmente del derecho internacional.[45] Es por eso que el artículo 17 establece que "cuando un tratado internacional afecte una disposición constitucional, debe ser aprobado por el mismo procedimiento que rige la reforma de la Constitución". Es decir, que la Constitución prevé la reforma de la Constitución para poder adaptarla al contenido de un tratado que *prima facie* es contrario a la misma y con ello garantizar la uniformidad del sistema normativo. Por tanto, con el proceso de *incorporación,* la norma internacional adquiere validez jurídica como fuente de derecho interno y un rango o jerarquía determinado frente al resto de fuentes nacionales.[46]

A nivel jurisprudencial, la Sala de lo Constitucional de la Corte Suprema de Justicia, mediante la sentencia AA 406-13, del 28 de junio de 2013[47], desarrolla el tema sobre la obligatoriedad de las normas internacionales de derechos humanos a nivel interno a través del "Control de Convencionalidad". La Sala de lo Constitucional comienza diciendo que

> la Corte Interamericana de Derechos Humanos,[48] establece que la ratificación de un tratado sobre derechos humanos implica que los Estados se someten a una orden legal dentro del cual ellos, por el bien común, asumen varias obligaciones, no en relación con otros Estados, sino hacia los individuos bajo su jurisdicción.[49]

Según la Sala de lo Constitucional:

> El Control de Convencionalidad consiste en que la interpretación del derecho contenido en las Convenciones y los tratados de que un Estado sea signatario, es la competencia propia y peculiar de los tribunales. Una Convención o Tratado Internacional son, de hecho y deben ser mirados por los jueces como normas de Derecho Fundamental, que forman parte de nuestro Bloque Constitucional. Y por ello pertenece a los jueces concretar su significado, tanto como el significado de cualquier Ley particular que proceda del Cuerpo Legislativo. Si ocurriese que hay una diferencia irreconciliable entre los dos, la que tiene vinculación y validez más fuerte debe ser preferida, así "en caso de conflicto entre el tratado

44 Honduras "Constitución de la República" La Gaceta No. 23,612 (20, enero 1982), artículo 18.

45 Francisco Villagrán Kramer, *Derecho de los tratados (*Guatemala: F&G Editores, 2002), 205.

46 Víctor Hugo Mata Tobar, *La aplicabilidad del derecho internacional de los derechos humanos en el orden jurídico de los Estados de Centroamérica* (San José, Costa Rica: CODEHUCA, 1998), 25.

47 Sala de lo Constitucional. Corte Suprema de Justicia de Honduras. Fallo recaído en el Recurso de Amparo número AA 406-13 del 28 de junio de 2013.

48 La Sala de lo Constitucional cita la siguiente opinión consultiva: Corte Interamericana de Derechos Humanos, opinión consultiva OC-2/82, de fecha 24 de septiembre del año 1982.

49 Sala de lo Constitucional. Fallo recaído en el Recurso de Amparo número AA 406-13, considerando 5.

> o convención y la Ley prevalecerá el primero", evidentemente; o, en otras palabras, éstos deben ser preferidos a la Ley, la intención del pueblo manifiesta a través de la Convención o el Tratado a la intención del agente del Estado. Pudiendo ir más allá inclusive y ampliar este tipo de control, para permitir la inclusión en el mismo, de los pactos y demás instrumentos internacionales de Derechos Humanos de que un Estado sea parte.[50]

La Sala de lo Constitucional establece que los efectos que produce el control de convencionalidad son:

> a) Los jueces y juezas y en última instancia la Sala de lo Constitucional de la Corte Suprema de Justicia, al conocer de controversias constitucionales, acciones de inconstitucionalidad y de amparo, pueden declarar la invalidez de las normas que contravengan (…) los tratados vigentes, pactos y demás declaraciones internacionales en materia de derechos humanos;[51] es decir que los jueces y juezas y magistrados y magistradas pueden declarar inconvencionales las normas ya sean constitucionales, legales secundarias y reglamentarias.
>
> b) Los demás jueces y juezas del país, en los asuntos de su competencia y de conformidad a lo previsto por nuestra Constitución y la Ley Sobre Justicia Constitucional, podrán inaplicar las normas que infrinjan (…) los tratados internacionales que reconozcan derechos humanos, solo para efectos del caso concreto y sin hacer una declaración de invalidez de las disposiciones;[52] en este caso las normas inconvencionales solo se dejan de aplicar para el caso concreto.
>
> c) Las autoridades del país que no ejerzan funciones jurisdiccionales deben interpretar los derechos humanos de la manera que más los favorezca, sin que estén facultadas para declarar la invalidez de las normas o para desaplicarlas en los casos concretos.[53] En este caso la Sala de lo Constitucional señala que los funcionarios y funcionarias están obligados a efectuar un examen convencional de derechos humanos en los actos y resoluciones administrativas aplicando el principio pro-homine, es decir el que más beneficie a la persona humana.

También la Sala de lo Constitucional se refiere a la uniformidad de las normas internacionales con la normativa interna, al decir

> que se incorporan a nuestro derecho interno las normas y derechos fundamentales de origen supranacional, para formar parte de nuestro Bloque de Constitucionalidad, al tenor de lo establecido en la Constitución en sus artículos 16 y 17:

50 Sala de lo Constitucional. Fallo recaído en el Recurso de Amparo número AA 406-13, considerando 10.
51 Sala de lo Constitucional, considerando 10.
52 Sala de lo Constitucional, considerando 10.
53 Sala de lo Constitucional, fallo recaído en el Recurso de Amparo número AA 406-13, considerando 11.

> Todos los tratados internacionales deben ser aprobados por el Congreso Nacional antes de su ratificación por el Poder Ejecutivo. Los tratados internacionales celebrados por Honduras con otros Estados, una vez que entran en vigor, forman parte del derecho interno. Y
>
> Cuando un tratado internacional afecte una disposición constitucional, debe ser aprobado por el mismo procedimiento que rige la reforma de la Constitución antes de ser ratificado por el Poder Ejecutivo.[54]

Pero es necesario

> observar un procedimiento interno por parte del legislativo mediante el cual se garantiza la uniformidad de nuestra legislación Constitucional y secundaria vigente, con lo previsto por el tratado, previo a su ratificación por el ejecutivo, lo que se relaciona directamente al carácter vinculante de estas normas supranacionales en nuestro derecho interno una vez observado el referido procedimiento legislativo.[55]

2.2. Constitución Política de Honduras

2.2.1. Vigilancia

2.2.1.1. Salvaguardas constitucionales del derecho a la privacidad en el contexto de la vigilancia de las comunicaciones

Como parte de este trabajo entendemos el derecho a la privacidad como una serie de derechos que incluyen el derecho a la vida privada, el derecho a la intimidad, el derecho a controlar nuestra propia información personal frente a terceras personas, es decir el derecho a la autodeterminación informativa y protección de datos personales, y la inviolabilidad del domicilio, correspondencia y comunicaciones. Este trabajo se refiere sobre todo al derecho a la intimidad o privacidad.

a) Derecho a la intimidad

En Honduras, al derecho a la privacidad cualquiera que sea su esfera se le denomina “derecho a la intimidad”, tanto en las normas como en la jurisprudencia. Este derecho está constitucionalizado pero no se define, solo establece que “se garantiza el derecho a (…) a la intimidad personal, familiar y a la propia imagen”.[56]

La Sala de lo Penal de la Corte Suprema de Justicia, le dio contenido al derecho al decir que:

54 Sala de lo Constitucional, considerando 12.

55 Sala de lo Constitucional, considerando 13.

56 Art. 76: Se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen. Honduras “Constitución de la República”, La Gaceta No. 23,612 (20, enero 1982).

> debe entenderse [por intimidad], en su aspecto positivo, 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 y, en su aspecto negativo, 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.[57]

Es decir, que la dimensión positiva es el derecho al goce de la intimidad, quedando obligado el Estado a crear las condiciones para que la persona humana pueda disfrutar libremente del derecho. En su dimensión negativa o prohibitiva implica que, especialmente el Estado, debe abstenerse de vulnerar el derecho a la privacidad de cualquier persona.

Continúa la Sala de lo Penal de la Corte Suprema de Justicia estableciendo algunas de las esferas de la privacidad que merecen protección:

> dentro de las múltiples esferas en que se desarrolla la persona humana y que puede realizar de manera íntima, están 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 (...)[58]

Con esta sentencia, la Sala de lo Penal amplia el contenido del derecho a la intimidad a lo digital.

b) Derecho a la inviolabilidad de la comunicaciones

La Constitución protege el derecho a la inviolabilidad de las comunicaciones al establecer en su artículo 100 que "toda persona tiene derecho a la inviolabilidad y al secreto de las comunicaciones, en especial de las postales, telegráficas y telefónicas, salvo resolución judicial". La Constitución se refiere de manera general a cualquier comunicación. Esta protección es de aplicación a cualquier forma moderna de comunicarse, ya que la primera parte del artículo se refiere de manera general a cualquier comunicación, como serían las comunicaciones a través de internet.

En la misma sentencia CP-48-2011, la Sala de lo Penal de la Corte Suprema de Justicia desarrolló el contenido del derecho a la inviolabilidad de las comunicaciones, determinando 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, intercepción, 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

57 Sala de lo Penal. Corte Suprema de Justicia de Honduras, Sentencia número CP-48-2011, 20, disponible en: http://www.poderjudicial.gob.hn/Jurisprudencia/Documents/CP-48-2011.pdf (consultado: 8 noviembre, 2015)

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

> (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.[59]

Esto implica un desarrollo jurisprudencial en lo referente a la privacidad digital.

c) Derecho a la autodeterminación informativa

Otro de los derechos relacionados con la privacidad es el derecho a la **autodeterminación informativa**, que se refiere a un aspecto de la intimidad, la "intimidad informática". Tiene relación con datos personales (como los relativos a la filiación política, origen, salud, parentesco, orientación sexual, etc).

> Lo que caracteriza el dato personal es la posibilidad de identificar con alguna precisión a la persona, física o jurídica, a la que el dato pertenece. Dicha posibilidad es lo que origina la protección, pues a través del dato se puede llegar no sólo a la persona sino incluso a establecer conductas y prácticas que sólo mediando la expresa voluntad de esta pueden trascender la esfera de su intimidad.[60]

En la Constitución de la República no encontramos una referencia concreta a la autodeterminación informativa, solo el medio para su protección, el *habeas data*, mismo que existe a partir de 2013 como una "Garantía Constitucional".[61] No hay una definición del *habeas data*, solo se describe que consiste en el "derecho de toda persona a 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", con la finalidad de "actualizarla, rectificarla y/o suprimirla".[62]

59 Sala de lo Penal. Sentencia número CP-48-2011, 20.

60 Marcela I. Basterra, *Protección de Datos Personales* (México: Universidad Nacional Autónoma de México, UNAM, 2008), 29-30.

61 Honduras "Reforma a la Constitución de la República" La Gaceta No. 33, 033 del 24 de enero de 2013.

62 Artículo 182. El Estado reconoce el derecho (…) de Hábeas Data. (…) unicamente puede promover la acción la persona cuyos datos personales o familiares consten en archivos, registros públicos o privados de la siguiente manera: (…) 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 el caso de que fuere necesario, actualizarla, rectificarla y/o suprimirla. No podrá afectarse el secreto de las fuentes de información periodística. Las acciones de Hábeas Corpus y Hábeas Data se deben ejercer sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles e inhábiles y libres de costas. Únicamente deben conocer de la garantía de Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia, quien tiene la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación a los derechos del honor, intimidad personal o familiar y a la propia imagen. Los titulares de los órganos jurisdiccionales no pueden desechar la acción de Hábeas Corpus o Exhibición Personal e igualmente tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación de la libertad y a la seguridad personal. En ambos casos, los titulares de los órganos jurisdiccionales que dejen de admitir estas acciones constitucionales, incurren en responsabilidad penal y administrativa. Honduras "Constitución de la República."

d) Derecho a la inviolabilidad del domicilio

Otro de los aspectos de la vida humana relacionado con el derecho a la intimidad es la **intimidad en el domicilio,** mismo que está normativizado constitucionalmente en su aspecto negativo. Es decir, a la protección frente a injerencias arbitrarias y la obligación de las y los demás de no transgredirlo, incluido el Estado. La Constitución de la República establece el derecho a "la inviolabilidad del domicilio" y regula las excepciones en que puede limitarse el derecho.[63]

Ni la norma constitucional ni las normas secundarias definen este derecho de inviolabilidad del domicilio. Sin embargo, la Corte Suprema de Justicia sí lo ha hecho a través de la Sala de lo Penal, que estableció que "la inviolabilidad del domicilio es un instrumento para la salvaguarda el derecho a la intimidad". La Sala también define qué se entiende por domicilio al decir que

> es el espacio físico delimitado estructuralmente, bajo el dominio, uso o goce de una o más personas determinadas, destinado para realizar en él, de manera permanente o temporal, un conjunto de actos privados, generalmente emancipados de las norma sociales imperantes en el exterior; el domicilio comprende no solo el lugar o edificación de la residencia, sino cualquier extensión que la componga, como patios interiores, bodegas, sótanos, etc., que se interconecten entre sí y en donde se evidencia que forman parte de un todo, conforme lo conceptualiza el artículo 220 del Código Penal. [64]

Como elementos del domicilio, la Sala de lo Penal ha establecido:

> 1. Elementos objetivos: a) Espacio físico, debidamente delimitado y separado del exterior por una estructura de cualquier tipo; b) Que se impida desde el exterior acceso visual de todos los espacios internos de la estructura, y c) Que sea apto para el desarrollo de la vida privada;
>
> 2. Elementos subjetivos: a) Que el espacio físico esté siendo usado (permanente o temporalmente) para el desarrollo de la esfera privada de la vida, y b) Aprovechar las condiciones físicas estructurales para excluir la participación de terceros en las actividades de la vida de personas, segregando los mismos a dicho espacio. En conclusión, el domicilio, con independencia de la relación jurídica entre el lugar y sus moradores puede consistir en una estructura natural o artificial, mueble o inmueble, siempre que sea un ambiente cerrado

63 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."

64 Art. 220: Se considera casa habitada todo albergue que constituya la morada de una o más personas, aunque se encuentren accidentalmente ausentes de ella cuando el [delito tuviere lugar]. Se consideran dependencias de casa habitada o de los establecimientos enumerados en el inciso 2 del artículo anterior, los corrales, bodegas […] y demás departamentos o sitios cercados y contiguos al edificio, y en comunicación interior con el mismo y con el cual formen un solo todo. Honduras "Código Penal" Poder Ejecutivo (1985).

> al cual solo tengan acceso aquellas personas que moran en el, usándolo para resguardar sus actos y posesiones íntimas." [65]

De acuerdo con este desarrollo jurisprudencial, podemos decir que el derecho a la inviolabilidad del domicilio protege también frente a las vigilancias electrónicas, que impliquen observar las acciones y actividades de las personas en los espacios que se consideran como domicilio.

2.2.1.2. Limitaciones constitucionales al derecho a la privacidad en el contexto de la vigilancia de las comunicaciones

a) Limitación del derecho al secreto de las comunicaciones

El artículo 100 de la Constitución de la República establece como requisito para la limitación del derecho a la inviolabilidad y al secreto de las comunicaciones que se haga mediante "resolución judicial".[66]

La Sala de lo Penal de la Corte Suprema de Justicia ha dicho que:

> este derecho no es de carácter absoluto, reconociendo el constituyente que en ciertas circunstancias específicas puede el Estado ordenar la intervención de las comunicaciones realizadas por cualquier medio, aún sin consentimiento o previo aviso de las personas que la sostengan, ello con el afán de proteger otros bienes jurídicos que se consideran preponderantes, siendo la autoridad judicial la única competente para ordenarlo cuando existan causas legítimas, mismas que están previstas en el Código Procesal Penal y a partir de enero de 2012 también en la Ley Especial sobre Intervención de las Comunicaciones Privadas [...][67]

La Sala sienta su posición frente a la facultad del Estado para vigilar cualquier tipo de comunicación, sin importar el medio utilizado, al considerar que hay otros bienes jurídicos superiores a la privacidad (pero no los menciona). También señala que debe existir una causa legítima para la vigilancia, mencionando que las causas enumeradas en la Ley de Intervención de las Comunicaciones son causas legítimas.

b) Limitación del derecho a la inviolabilidad del domicilio

El artículo 99 de la Constitución de la República elabora algunas maneras de limitar el derecho a la inviolabilidad del domicilio: a) El consentimiento de la persona que lo habita; b) Por "resolución de autoridad competente, y c) Sin consentimiento, ni resolución de autoridad competente en caso de urgencia, para impedir la comisión o impunidad de delitos o evitar daños graves a la persona o a la propiedad.

---

65 Sala de lo Penal. Sentencia número CP-303-2010, 20.

66 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 Política."

67 Sala de lo Penal. Sentencia número CP-48-2011, 21.

De acuerdo con la Sala de lo Penal de la Corte Suprema de Justicia, de los tres supuestos del artículo 99 antes descritos se deriva la "diferencia entre un ingreso y/o registro autorizado, un allanamiento como acto investigativo y un allanamiento ante un estado de necesidad o delito flagrante."[68] En este último caso, la Constitución no establece la necesidad de una revisión posterior por autoridad judicial, pero sí lo establece el Código Procesal Penal en su artículo 2012, que ordena que el juez en este caso deberá "por auto motivado convalidar o anular lo actuado".

2.2.1.3. Mecanismos de acceso a la justicia en el contexto de la vigilancia

Existen tres mecanismos de acceso a la justicia en el contexto de la vigilancia por violación a derechos fundamentales como el derecho a la intimidad, a la inviolabilidad de las comunicaciones, al domicilio y a la autodeterminación informativa.

a) El recurso de amparo: de acuerdo con el artículo 183 constitucional, toda persona agraviada o cualquiera en nombre de esta, tiene derecho a interponer recurso de amparo: 1) Para que se le mantenga o restituya en el goce y disfrute de los derechos o garantías que la Constitución, los Tratados, Convenciones y otros instrumentos internacionales establecen, y, 2) Para que se declare en casos concretos que un reglamento, hecho, acto o resolución de autoridad, no obliga al recurrente ni es aplicable por contravenir, disminuir o tergiversar cualesquiera de los derechos reconocidos por esta Constitución.

b) El recurso de *habeas data*: la finalidad de la acción es que la información se pueda actualizar, rectificar y/o suprimir.[69] Está legitimado para ejercer la acción la persona cuyos datos personales o familiares consten en archivos, registros públicos o privados.[70] Las bases de datos objeto de control son los registros públicos o privados.[71] Tiene competencia para conocer y resolver el recurso la Sala de lo Constitucional de la Corte Suprema de Justicia, después de agotarse el procedimiento administrativo ante el Instituto de Acceso a la Información Pública[72].

c) El recurso de inconstitucionalidad: de acuerdo con el artículo 184 de la Constitución de la República, "las leyes podrán ser declaradas inconstitucionales por razón de forma o de contenido." Y es la "Corte Suprema de Justicia, quien tiene competencia para conocer y resolver de manera exclusiva en la materia, y deberá pronunciarse con los requisitos de las sentencias definitivas." La declaración de inconstitucionalidad de una ley y su derogación debe solicitarse por quien se considere lesionado en su interés directo, personal y legítimo.[73]

68 Sala de lo Penal. Sentencia número CP-303-2010, 21-22

69 Honduras "Constitución de la República", artículo 182 y Honduras "Ley Sobre Justicia Constitucional" La Gaceta No. 30,792 (agosto 2004), artículo 13.

70 Honduras "Constitución de la República", artículo 182 y Honduras "Ley de Justicia Constitucional", artículo 13.

71 Honduras "Constitución de la República", artículo 182 y Honduras "Ley de Justicia Constitucional", artículo 13.

72 Honduras "Constitución de la República", artículo 182 y Honduras "Ley de Justicia Constitucional", artículo 13.

73 Honduras "Constitución de la República", artículo 185,

2.2.2. Anonimato y cifrado

El cifrado es el proceso matemático de utilizar códigos y claves para comunicarnos de forma privada. A lo largo de la historia, la gente ha utilizado métodos cada vez más sofisticados de cifrado para enviarse mensajes entre sí con el objetivo de que no puedan ser leídos por cualquier persona además de los destinatarios. Hoy en día, las computadoras son capaces de realizar un cifrado mucho más complejo y seguro[1].

El anonimato se puede definir como actuar o comunicarse sin usar o presentar el nombre o identidad propios; o como actuar o comunicarse en una manera que protege la determinación del nombre o identidad propios, o usando un nombre asumido o inventado que no puede necesariamente asociarse con la identidad legal o habitual de uno[2].

2.2.2.1. Salvaguardas constitucionales para la protección del cifrado y el anonimato

La Constitución hondureña protege el derecho a la privacidad y la libertad de expresión, el cual incluye el derecho a hablar, leer y comunicarse anónimamente. Esto comprende el derecho de cada persona a utilizar herramientas para la protección de su expresión porque el derecho a buscar y recibir información incluye el derecho a leer anónimamente. El derecho a la privacidad de las comunicaciones y la libertad de expresión abarca el derecho de todas las personas a utilizar tecnología de cifrado. Esto significa que los y las proveedores de servicios deben ser capaces de diseñar sistemas que protejan la privacidad de extremo a extremo.

El Relator sobre Libertad de Expresión de Naciones Unidas, David Kaye, ha dicho que

> el Cifrado y el Anonimato son los principales vehículos para la seguridad en línea, proporcionando a los individuos un medio para proteger su privacidad, dándoles el poder de navegar, leer, desarrollar y compartir opiniones e información sin interferencias y fortaleciendo el derecho a la libertad de expresión y opinión de periodistas, organizaciones de la sociedad civil, miembros de las minorías étnicas o grupos religiosos, a los perseguidos debido a sus orientación sexual o identidad de género, activistas, académicos, artistas y a otros.[74]

El cifrado y el anonimato son herramientas frente a un Estado vigilante. El Relator ha señalado que tanto el cifrado como el anonimato y los conceptos de seguridad detrás de ellos ofrecen la privacidad y la seguridad necesaria para el ejercicio del derecho a la libertad de opinión y de expresión en la era digital.[75] Es decir, que el cifrado y el anonimato además de ser necesario para proteger la privacidad

74 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, David Kaye, Resolución A/HRC/29/32 del 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)

75 Naciones Unidas. Informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión.

digital, también protege el ejercicio al derecho a la libertad de expresión. Además, el Relator refiere que estas herramientas sirven para la garantía de otros derechos, "dicha garantía puede ser esencial para el ejercicio de otros derechos, como los derechos económicos, el debido proceso la libertad de reunión y de asociación pacíficas, y el derecho a la vida y la integridad corporal.[76]

En otros informes de la Relatoría sobre la Libertad de Expresión de Naciones Unidas se ha indicado que

> el derecho a la privacidad suele entenderse como un requisito esencial para la realización del derecho a la libertad de expresión. La injerencia indebida en la intimidad de las personas puede limitar en forma tanto directa como indirecta el libreintercambio y evolución de ideas. Las restricciones al anonimato de las comunicaciones, por ejemplo, tienen un efecto intimidatorio en las víctimas de todas las formas de violencia y abuso, que podrían ser renuentes a denunciarlaspor temor a la doble victimización".[77]

El Relator, al referirse a las modalidades de las vigilancias con las nuevas tecnologías, manifiesta que permiten a los Estados injerirse en la vida privada de las personas, atentan contra una diferenciación clara entre el ámbito público y el privado,[78] esto implica que el Estado considera la vida de las personas como pública para efecto de vigilancias. También el Relator cuestiona la falta de notificación y publicidad de la vigilancia con el uso de las nuevas tecnologías: "facilitan la vigilancia invasiva y arbitraria de las personas, que podrían ni siquiera saber que han sido objeto de esta vigilancia, y menos aún cuestionarla".[79]

El Relator asimismo se refirió a la situación de los atentados contra el anonimato "el Estado tiene la obligación de abstenerse de requerir la identificación de las personas usuarias, como condición previa para el acceso a las comunicaciones, incluidos los servicios en línea, los cibercafés o la telefonía móvil".[80]

2.2.2.2. Limitaciones constitucionales al cifrado y el anonimato

No existe ninguna norma constitucional que regule la promoción ni las limitaciones al cifrado o al anonimato. Ninguno de estos temas ha sido abordado por la Sala de lo Constitucional de la Corte Suprema de Justicia.

76 Naciones Unidas. Informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y de expresión.

77 Naciones Unidas. Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue, resolución A/HRC/23/40 del 17 de abril de 2013, párr. 24.

78 Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue, resolución A/HRC/23/40 del 17 de abril de 2013, párr. 33.

79 Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue, resolución A/HRC/23/40 del 17 de abril de 2013, párr. 33.

80 Naciones Unidas. Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, resolución A/HRC/17/27 del 16 de mayo de 2011, párr. 65, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/132/04/PDF/G1113204.pdf?OpenElement (consultado: 14 abril, 2015)

2.2.2.3. Mecanismos de acceso a la justicia en el contexto del cifrado y el anonimato a nivel constitucional

Como mecanismos de acceso a la justicia puede aplicarse el recurso de amparo, pues el mismo se utiliza para la protección de cualquier derecho fundamental.

2.3. Leyes, reglamentos y jurisprudencia

2.3.1. Vigilancia, cifrado y anonimato en leyes y reglamentos

La Ley de Intervención de las Comunicaciones define comunicación como "la acción y efecto de transmisión del pensamiento, mediante un código común, mediante cualquier medio que se utilice entre el emisor y receptor."[81] Las telecomunicaciones son declaradas inviolables por la ley y para ser interceptadas o interferidas es necesaria resolución judicial. Las informaciones obtenidas en contravención de esta norma no podrán ser utilizadas en ninguna forma y originarán responsabilidad civil y penal.[82] El contenido del derecho a la inviolabilidad de las telecomunicaciones lo amplía una norma reglamentaria sobre telecomunicaciones, al establecer que:

> la inviolabilidad de las telecomunicaciones es un derecho que asiste a todos los personas usuarias de estos servicio. Se atenta contra el derecho de inviolabilidad de las telecomunicaciones cuando una persona que no es la que origina la comunicación ni es la destinataria, la sustrae, intercepta, o la interfiere, o de otro modo, cambia o altera su contenido, desvía su curso, utiliza, publica, trata de facilitar que él mismo u otra persona conozcan la existencia o el contenido de la comunicación.[83]

En enero de 2011 entró en vigencia una ley especial sobre **"**intervención de las comunicaciones",[84] que derogó las normas incluidas en el Código Procesal Penal el año 2002 sobre intervención de las comunicaciones (estas normas reunían los requisitos de autorización judicial de exigencia de motivar sobre la proporcionalidad de la vigilancia, etc. En definitiva, estas normas estaban orientadas

81 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas" La Gaceta No. 32, 731 (26, enero 2012), artículo 3 numeral 1.

82 Artículo 3 de la Ley Marco del Sector de Telecomunicaciones: Las telecomunicaciones son inviolables. No podrán, por consiguiente, ser interceptadas o interferidas, salvo por resolución judicial. Las informaciones obtenidas en contravención de esta norma no podrán ser utilizadas en ninguna forma y originarán responsabilidad civil y penal. Y el artículo 1, párrafo segundo de la Ley Especial Sobre la Intervención de las Comunicaciones Privadas indica: Esta ley también tiene como fin garantizar el secreto de las comunicaciones y el derecho a la intimidad, así como otros derechos fundamentales, sea que estén establecidos o no en la Constitución de la República. Las disposiciones contenidas en esta ley son de orden público.

83 Honduras "Reglamento de la Ley Marco del Sector de Telecomunicaciones" Secretaría de Estado en el Despacho de Gobernación y Justicia, Acuerdo Número 141-2002, artículo 8.

84 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas".

exclusivamente a la persecución de delitos de crimen organizado).[85] Esta nueva ley tiene por finalidad "establecer el marco legal de regulación procedimental de la intervención de las comunicaciones"[86] y "que constituya una herramienta esencial en la lucha contra la criminalidad tradicional, y sobre todo contra la criminalidad organizada o no convencional";[87] es decir que la ley tiene aplicabilidad en la investigación de cualquier delito.

La ley determina lo que se considera como intervención de las comunicaciones, estableciéndola como:

> una técnica especial de investigación, que consiste en el procedimiento a través del cual, se escucha, capta, registra, guarda, graba, u observa, por parte de la autoridad, sin el consentimiento de sus titulares o participantes, una comunicación que se efectúa, mediante cualquier tipo de transmisión, emisión o recepción de signos, símbolos, señales escritas, imágenes, sonidos, correos electrónicos o información de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros medios, sistemas electromagnéticos, telefonía, radiocomunicación, telegrafía, medios informáticos o telemáticos, o de naturaleza similar o análogo, así como la comunicación que se efectúe a través de cualquier medio o tipo de transmisión.[88]

La Ley de Intervención de las Comunicaciones en su artículo 5[89] establece cinco principios para la intervención de las comunicaciones:

1. Proporcionalidad: La intervención de las comunicaciones tendrá carácter excepcional y solo podrá realizarse cuando resulte útil para una investigación penal y se justifique la medida, ponderándose un equilibrio entre lo que se pretende lograr con la medida y el derecho que ha de resultar afectado;

2. Necesidad e idoneidad: La intervención de las comunicaciones se ordenará solo cuando sea necesaria para la obtención de la información respecto a la investigación y no existan otras formas menos gravosas para la investigación efectiva de los delitos;

85 Art. 223. Intervención de las comunicaciones. El juez a petición del Ministerio Público o de parte acusadora, podrá ordenar, mediante resolución fundada, la grabación de la comunicaciones telefónicas, informáticas, o de cualquier otra índole análoga que tenga el imputado o cualquier otra persona directa o indirectamente relacionada con el delito que se investiga. El juez valorará en su resolución, la gravedad del delito investigado, la utilidad y proporcionalidad de la medida. La intervención de comunicaciones de que se trata en este artículo, podrá consistir en la identificación y registro de su origen, de su destinatario o de ambas cosas a la vez, o en el conocimiento y registro de su contenido. La intervención no podrá durar más de 15 días, pero podrá ser prorrogado por el juez, a instancia del Ministerio Público o de parte acusadora, por periodos sucesivos de quince días, en virtud de un auto motivado, siempre que se mantengan los presupuestos que inicialmente justificaron la adopción de la medida. Las grabaciones, una vez hechas, serán entregadas exclusivamente al juez que las ordenó […]. El juez tomará conocimiento de su contenido en forma exclusiva. Si las mismas tienen relación con el hecho que se investiga, podrá ordenar que se transcriban para ser oportunamente presentadas en el proceso. Las personas encargadas de realizar las grabaciones o la transcripción de éstas, mantendrán en secreto su contenido y en caso de incumplimiento incurrirán en la correspondiente responsabilidad penal. La grabación de una comunicación realizada por uno de los comunicantes sin llenar los requisitos establecidos en este artículo, carece de valor probatorio. Honduras "Código Procesal Penal."

86 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", 2011, artículo 1

87 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", 2011, artículo 1

88 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", 2011, artículo 3 numeral 11.

89 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", 2011

3. Confidencialidad: El procedimiento de intervención de las comunicaciones será reservado y la información obtenida será estrictamente confidencial durante el desarrollo de la intervención;

4. Reserva judicial: La intervención de las comunicaciones solamente podrán autorizarse por el órgano jurisdiccional competente, en forma, escrita y debidamente motivada, en los términos de la presente ley, y

5. Temporalidad: La intervención se autorizará por tiempo definido por el juez o jueza y no excederá del máximo permitido por la ley.

En cuanto a los motivos, la ley es totalmente abierta, pues se puede autorizar la intervención de las comunicaciones en la investigación, persecución y el procesamiento de cualquier delito ya sea de criminalidad tradicional o de criminalidad organizada[90], y requiera la utilización de esta técnica especial;[91] que no existan otras formas menos gravosas para la investigación efectiva de los delitos.[92] Como requisito, basta que esté abierta la investigación y que cuente con un número asignado o que está judicializada la investigación[93], estableciendo que el juez o jueza solo deberá valorar la gravedad, utilidad y proporcionalidad de la medida en relación al delito que se trate.[94]

El ámbito de aplicación de la ley sobre intervención de las comunicaciones recae:

> sobre las comunicaciones y medios de soporte, físicos o virtuales, de que hacen uso o están haciendo uso las personas investigadas o imputadas implicadas en la actividad ilícita, ya sea que éstos la transmitan o remitan, o si por el contrario se destinan a estos, aunque sea con un nombre falso, aparente o inexistente o por medio de otra persona que está siendo usada como conexión, ya sean sus titulares o personas usuarias habituales o eventuales, directa o indirectamente. También se intervendrán, cuando se trate de las comunicaciones y medios de soporte de aquellos con los cuales las personas investigadas o imputadas se comunican, sean sus titulares o personas usuarias habituales o eventuales. La intervención también puede recaer sobre aparatos de comunicación y otros medios de soporte similar.[95]

90 Tal como lo plantea la finalidad de la Ley en el Artículo 1 de la Ley Especial Sobre la Intervención de las Comunicaciones Privadas: esta ley tiene por finalidad establecer el marco legal de regulación procedimental de la intervención de las comunicaciones, como mecanismo excepcional de investigación, a fin que constituya una herramienta esencial en la lucha contra la criminalidad tradicional, y sobre todo contra la criminalidad organizada o no convencional, garantizando el derecho humano de las personas a la comunicación, sin mas limitaciones que las dispuestas por la Constitución y las leyes.

91 Artículo 8: La autorización de la intervención de las comunicaciones procederá en la investigación, persecución y el procesamiento de los delitos en que se requieran la utilización de esta técnica especial, valorando para ello la gravedad, utilidad y proporcionalidad de la medida en relación al delito que se trate. Honduras “Ley Especial Sobre la Intervención de las Comunicaciones Privadas.”

92 Honduras “Ley Especial Sobre la Intervención de las Comunicaciones Privadas”, artículo 5.

93 Artículo 14: requisito previo de intervención. Será requisito imprescindible para presentar solicitud de intervención de las comunicaciones, que exista una investigación abierta, o una causa judicial en curso, cuyo número de registro de inscripción se hará mención en la solicitud presentada por el Ministerio Público y la Procuraduría General de la República, en su caso. Honduras “Ley Especial Sobre la Intervención de las Comunicaciones Privadas.”

94 Honduras “Ley Especial Sobre la Intervención de las Comunicaciones Privadas”, artículos 1 y 8.

95 Honduras “Ley Especial Sobre la Intervención de las Comunicaciones Privadas”, artículo 10

Esta parte de la ley determina las comunicaciones de quién o de quiénes pueden vigilarse. Por otra parte, la Ley de Intervención establece y enumera algunos tipos de intervenciones o vigilancias:

- **Comunicación entre personas presentes:**

  Es la intervención de las comunicaciones orales, o las que se realicen entre personas presentes, siempre que se lleven a cabo en lugares considerados privados. En caso de que la intervención recaiga sobre comunicaciones entre presentes, realizadas en sitios o lugares públicos, la misma podrá efectuarse sin ningún procedimiento ni requisito legal[96]. Este tipo de vigilancias no responden a los objetivos de esta investigación, sin embargo, es necesario resaltar la gravedad de esta vigilancia, pues no necesita control jurisdiccional, por lo que las autoridades con facultades investigativas pueden vigilar espacios en los que las y los defensores desempeñan sus labores como pueden ser las oficinas, pues estas no se consideran espacio privado de acuerdo con la normativa hondureña.

- **Intervención de llamadas entrantes o salientes:**

  Es la que se practica sobre información de llamadas entrantes y salientes de un número de teléfono identificado, el juez o juez ordenará que esta sea proporcionada en forma impresa y en aparatos de almacenamiento electrónico.[97]

- **Intervención sobre e-mail:**

  Es la practicada sobre los mensajes de correo electrónico.[98]

- **Intervención sobre aparatos:**

  Es la practicada sobre el aparato celular o sim, u otro aparato de soporte en el cual se encuentre almacenada, guardada o registrada información sobre comunicaciones.[99] Es decir que puede incluir la computadora, USB, discos externos, etc.

96 Artículo 6: Comunicación entre personas presentes: también se podrá autorizar la intervención de las comunicaciones orales, o las que se realicen entre personas presentes. No se considerará intervención de la comunicaciones orales, a que se refiere el párrafo anterior, si las mismas se desarrollan en sitios o lugares públicos. Cuando la comunicación entre presentes se produzcan en el interior de domicilios o recintos privados, sólo podrá autorizarse la intervención, si existen indicios que revelen que se llevará a cabo una actividad delictiva o que ésta se ha estado realizando. Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas."

97 Artículo 40: Cuando se trate de intervención sobre información de llamadas entrantes y salientes de un número de teléfono identificado, o se trate de información que obra en un e-mail o aparato celular o sim, o cualquier otra información u otro aparato de soporte, en el cual se encuentre almacenada, guardada o registrada información sobre comunicaciones, el juez, ordenara que ésta sea proporcionada en forma impresa y en aparatos de almacenamiento electrónico. En el mandamiento judicial el juez dispondrá que la información y los aparatos de almacenamiento que sirvieron para proporcionar la información, sean entregados a la UIC para la realización del análisis que se requiera. Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas."

98 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 40.

99 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 40.

- **Intervención sobre cualquier otra información:**

  La norma faculta la intervención de "cualquier otra información", lo que deja abierta la posibilidad de intervenir las comunicaciones, como por ejemplo aquellas efectuadas en redes sociales.[100] En estos últimos casos[101], el juez o jueza ordenará que la información sea proporcionada en forma impresa y en aparatos de almacenamiento electrónico.[102]

- **Facultad de peticionar la intervención**

  El Ministerio Público, la Policía Nacional o cualquier otra autoridad competente, podrá peticionar intervención de las comunicaciones en las investigaciones que realicen.[103] Es decir, que lo que se exige para solicitar la intervención es estar realizando una investigación por causa delictiva y tener competencia para la investigación.[104]

- **Facultad para autorizar**

  La ley establece que será el órgano jurisdiccional en materia penal quien autorizará la intervención por cualquier investigación que se realice[105].

- **Plazo de las intervenciones**

  Puede autorizarse hasta por tres meses, pudiéndose prorrogar el plazo hasta por tres períodos más, es decir que las vigilancias pueden durar hasta 12 meses continuos.[106]

2.3.1.1. Normas en materia penal

a) Sanciones frente a la vigilancia

Mediante el delito de "violación a las comunicaciones privadas", se sanciona cualquier apoderamiento de documentos y correspondencia en físico o la intervención (o procura de intervención) de las

100 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 40.

101 Intervención de llamadas entrantes o salientes e intervención de e-mail, aparato celular o sim, o cualquier otra información u otro aparato de soporte en el cual se encuentre almacenada, guardada o registrada información sobre comunicaciones.

102 Y es lo que dice el artículo 25 de la Ley Especial Sobre la Intervención de las Comunicaciones Privadas, acerca del registro de las intervenciones: La intervención sobre escuchas, grabaciones, observación de correos o cualquier otra comunicación que se esté ejecutando, se registrarán documentalmente y en forma completa por los peritos asignados.

103 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 7.

104 Actualmente, en Honduras tienen facultades para investigar delitos la Policía Nacional, las Fuerzas Armadas y la Dirección Nacional de Investigación e Inteligencia, la Agencia Técnica de Investigación Criminal, la Dirección de Lucha Contra el Narcotráfico y la Procuraduría General de la República.

105 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 5 numeral 4, 7 y 12.

106 Artículo 32. Plazos y prórrogas de la intervención: la intervención que se refiere a grabaciones, observaciones de correos o cualquier otra comunicación que se esté ejecutando a los investigados o imputados durante el desarrollo de la investigación, se autorizará por plazos no superiores a tres (3) meses, que podrán prorrogarse hasta por tres (3) periodos más. Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas"..

comunicaciones. Incluso sanciona la intervención física de los aparatos electrónicos de cualquier naturaleza que contengan información, cuando se realizan sin la debida autorización judicial.[107]

b) Delitos electrónicos

Encontramos en las normas penales el delito de "utilización indebida de sistemas de procesamiento de datos", relacionado con el acceso sin autorización a datos de las instituciones financieras, pero todavía no existen en la legislación hondureña delitos relacionados directamente con este nuevo campo del ámbito penal aunque de acuerdo con lo que se dice en algunos espacios de las organizaciones de derechos humanos sí se prevén en el nuevo anteproyecto de Código Penal, que no se citan en este documento porque no hay un documento oficial.[108]

c) Criminalizacion del uso de herramienta de privacidad

Mediante una reforma al Código Penal en 2011, se incorporaron nuevas conductas típicas dentro de la categoría de "estafas y otros fraudes" que hasta el momento no se han aplicado. Estos nuevos delitos están relacionados con el fraude en telecomunicaciones, medios u ondas y sistemas informáticos o de la información como tráfico irregular, a través de la reoriginación (*refilling*), de llamada internacional (*callback*), ingreso de tráfico internacional de forma ilegal evitando pagar las debidas tasas de terminación entre operadores internacionales (*bypass*), piratería informativa (*hackeo*), reventa no autorizada y clonación de números telefónicos móviles.[109] Dentro del tipo penal antes citado existe una regulación de diferentes conductas delictivas, entre las cuales se menciona la "piratería informática", que genera seria preocupación pues podría utilizarse para criminalizar ya sea a los técnicos y técnicas, a los defensores y defensoras de derechos humanos o periodistas que utilicen mecanismos de seguridad informática, esta norma es abierta por lo que viola el principio de legalidad penal que implica que los verbos rectores de los tipo penales deben estar muy concretos sin permitir que se deje a la interpretación del persecutor penal o del juzgador.

---

107 Artículo 214: Quien sin la debida autorización judicial, con cualquier propósito, se apodere de los papeles, correspondencia, intercepta o hace interceptar sus comunicaciones telefónicas […] o Telegráficas, soportes electrónicos o computadoras, facsimilares o cualquier otra naturaleza, incluyendo las electrónicas, será sancionado con seis (6) a ocho (8) años si fuere un particular y de ocho (8) a doce (12) años si se tratare de un funcionario o empleado público. Honduras "Código Penal."

108 Artículo 394-I : Utilización Indebida de Sistemas de Procesamiento de Datos: Quién acceda ilegalmente a los sistemas de procesamiento de datos de las instituciones supervisadas, para alterar, borrar, dañar o sustraer registros, archivos u otra información de la institución o de sus clientes, en beneficio propio o ajeno, será sancionado con reclusión de tres (3) a seis (6) años cuando el monto de lo defraudado no exceda de diez mil (10,000.00) lempiras y de seis (6) a doce (12) años cuando exceda de dicho monto. En las mismas penas incurrirán quienes bajo cualquier procedimiento ingrese o utilice indebidamente la base de datos de una institución supervisada para sustraer dinero mediante transferencias electrónicas de una cuenta a otra en la misma o diferente institución. Honduras "Código Penal."

109 Artículo 242: incurrirá en las penas de Estafas y otros Fraudes: (…) numeral 14) Quien cometiera fraude en telecomunicaciones, medios u ondas y sistemas informáticos o de la información como tráfico irregular, a través de la reoriginación (*refilling*), de llamada internacional (*callback*), ingreso de tráfico internacional de forma ilegal evitando pagar las debidas tasas de terminación entre operadores internacionales (*bypass*), piratería informativa (*hackeo*), reventa no autorizada y clonación de números telefónicos móviles. Honduras "Código Penal."

Por otra parte, en la Ley de Intervención de las Comunicaciones Privadas, en el artículo 50, se dispone que se sancionará

> a quien por cualquier motivo evadiere cualquier tipo de medida tecnológica que controle el acceso a las bases, sistemas operativos o registros informáticos de Unidad de Información de las Comunicaciones (UIC) o de las compañías u operadoras que estén brindando la intervención, con fines de impedir la obtención de resultados por parte de la autoridad.[110]

La redacción de este artículo genera un riesgo frente a la interpretación que se puede hacer por parte de los/as fiscales y jueces/as, pues parece que se refiere al ingreso ilegal a las bases de datos de la UIC y compañías operadoras, pero por la palabra "evadiere" pareciera que también se refiere al uso de cifrado.[111] En la legislación hondureña muchas normas tienen la característica de la ambigüedad, por lo que hay un espacio peligroso para la interpretación contra derechos.

La figura penal de "financiamiento al terrorismo",[112] al ser muy ambigua y amplia puede abrir la puerta para interpretaciones desproporcionadas. La norma dice que "quien con el propósito de facilitar la comisión de las actividades delictivas vinculadas al terrorismo, proporcione capacitación, equipo de comunicaciones y cualquier otro tipo de apoyo material o personal"; también a

> quien con la finalidad de facilitar la comisión de las actividades delictivas vinculadas al terrorismo, aporte apoyo o servicio con la intención que sean utilizados o a sabiendas que serán utilizados con la finalidad de cometer actos terroristas o que traslade, administre, custodie u oculte apoyo material a personas u organizaciones terroristas.[113]

además "quien, teniendo conocimiento de la intención de la organización terrorista para la realización de actos de terrorismo, contribuya con esta organización, a través de cualquier medio o forma de colaboración".[114]

---

110 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 50.

111 Artículo 50: Delito por acceso ilegítimo a captar información: será sancionado con pena de reclusión de seis (6) a nueve (9) años a quien por cualquier medio evadiere cualquier tipo de medida tecnológica que controle el acceso a las bases, sistemas operativos o registros informáticos de U.I.C. o de las compañías u operadoras que estén brindando la intervención, con fines de impedir la obtención de resultados por parte de la autoridad. Si en razón del acceso se obtiene información, sobre los procedimientos de intervención de las comunicaciones, la pena se aumentará en un tercio. Asimismo, esta disposición será aplicable a quienes acceden ilegítimamente a captar información, aumentada en un tercio si se tratare de un funcionario público. Honduras " Ley Especial Sobre la Intervención de las Comunicaciones Privadas".

112 Honduras "Ley Contra el Financiamiento del Terrorismo" La Gaceta No. 32, 389 (11, diciembre 2010).

113 Honduras "Ley Contra el Financiamiento del Terrorismo".

114 Artículo 3**.** Delito de financiamiento al terrorismo**.** Incurre en el delito de financiamiento al terrorismo: (…) 2). Quien, con el propósito de facilitar la comisión de las actividades delictivas vinculadas al terrorismo, proporcione (...) capacitación (…) equipo de comunicaciones (...) y cualquier otro tipo de apoyo material o personal; 3). Quien, con la finalidad de facilitar la comisión de las actividades delictivas vinculadas al terrorismo, aporte apoyo o servicio con la intención que sean utilizados o a sabiendas que serán utilizados con la finalidad de cometer actos terroristas o que traslade, administre, custodie u oculte apoyo material a personas u organizaciones terroristas; 4). Quien, teniendo conocimiento de la intención de la organización terrorista para la realización de actos de terrorismo, contribuya con esta organización, a través de cualquier medio o forma de colaboración. El delito de financiamiento existe y será sancionado independientemente que los actos de terrorismo lleguen a consumarse; por consiguiente no será necesario que los activos o fondos efectivamente se hayan usado para cometerlo.

La norma exige para la comisión del delito que la persona tenga la "intención de facilitar las actividades vinculadas al terrorismo", sin embargo, el artículo 3 de la Ley Contra el Financiamiento del Terrorismo, en su párrafo siete, deja al arbitrio de las autoridades la interpretación pues establece que "el delito de financiamiento existe y será sancionado independientemente que los actos terroristas lleguen a consumarse; por consiguiente no será necesario que los activos o fondos efectivamente se hayan usado para cometerlo"; con esto el Estado puede fácilmente abrir la puerta para acusaciones desproporcionadas no relacionadas a las actividades de terrorismo, sino más bien a talleres de capacitación que pueden darse a grupos de derechos humanos. Ello lo hemos visto cuando defensores y defensoras de la tierra fueron acusados de terrorismo por participar en una protesta pública.

2.3.1.2. Normas sobre inteligencia y contrainteligencia

En Honduras se creó un nuevo Sistema Nacional de Inteligencia en 2011, coordinado por la Dirección Nacional de Investigación e Inteligencia,[115] cuya finalidad es: a) Desarrollar actividades de investigación e inteligencia estratégica para prevenir y contrarrestar amenazas internas o externas contra el orden constitucional;[116] b) Producir inteligencia, para la toma de decisiones en el ámbito interno y externo con el fin de proteger al Estado de las amenazas a la seguridad y la defensa nacional;[117] c) Desarrollar actividades de investigación e inteligencia estratégica con el propósito de contrarrestar actos que atentan gravemente contra la gobernabilidad, la administración pública y proteger a las instituciones del Estado de la influencia del crimen organizado;[118] d) Contribuir a la protección de recursos naturales, tecnológicos y económicos del Estado, contra la interferencia de agentes internos y externos que comprometan el orden público y los objetivos nacionales[119], y f) Proteger a las instituciones públicas de actos de penetración, infiltración, espionaje, sabotaje u otras actividades de inteligencia desarrolladas por organizaciones criminales y otros agentes que representen una amenaza.[120]

El origen del Sistema de Inteligencia es el Consejo Nacional de Defensa y Seguridad (CNDS),[121] cuya finalidad legal es la de diseñar, rectorar y supervisar las políticas generales en seguridad, defensa

115 Artículo 6: Para su funcionamiento el Consejo Nacional de Defensa y Seguridad, conformarán la Dirección Nacional de Investigación e Inteligencia como ente encargado de ejecutar las políticas públicas que en materia de Defensa y Seguridad establezcan el Consejo, a través de las Unidades Especiales de Investigación que al efecto se creen mediante ley, gozará de independencia funcional, administrativa y presupuestaria y responderá directamente ante el Consejo Nacional de Defensa y Seguridad. Honduras "Ley Especial del Consejo Nacional de Defensa y Seguridad". Además véase: Honduras "Ley de Inteligencia Nacional" La Gaceta No. 33, 099 (15, abril 2013).

116 Honduras "Ley de Inteligencia Nacional" Poder Legislativo (2012), artículo 2.

117 Honduras "Ley de Inteligencia Nacional", artículo 5.

118 Honduras "Ley de Inteligencia Nacional", artículo 9, numeral 1, literal d.

119 Honduras "Ley de Inteligencia Nacional", artículo 9, numeral 1, literal e.

120 Honduras "Ley de Inteligencia Nacional", artículo 9, numeral 1, literal f.

121 Este órgano lo contempla el art. 287 de la CR y está dentro del capítulo X (De la Defensa Nacional), pero esta norma no describe en qué consistirá. Se le dio operatividad en 2011 a través de la Ley Especial del Consejo Nacional de Defensa y Seguridad.

nacional e inteligencia,[122] y está conformado por el presidente de la República (quien lo preside); sus subordinados los Secretarios de Defensa y Seguridad (todos ejecutores de la administración pública); el presidente de la Corte Suprema de Justicia (el presidente de este poder concentra funciones tanto jurisdiccionales como administrativas del Poder Judicial; poder encargado de controlar la inconstitucionalidad de las leyes, los actos ilegales de la administración pública y juzgar los delitos); el presidente del Congreso Nacional (el presidente de este poder tiene la exclusividad de la agenda legislativa de acuerdo con su Ley Orgánica),[123] y el Fiscal General de la República (representante de los intereses de la sociedad con varias funciones entre ellas la persecución del delito de acción pública, la vigilancia del respeto a la Constitución de la República).[124]

Con la existencia del CNDS se pone en duda el principio de independencia y separación de poderes que forman parte del Estado de Derecho, que en Honduras al menos normativamente ha existido desde 1982.[125] Todas estas instituciones que conforman el CNDS poseen competencias separadas para mantener un equilibrio de poder que garantiza los contrapesos institucionales, pero que, con la creación del CNDS, se eliminan, ya que en las decisiones participan todos; esto implica que ninguna decisión que se tome en el seno de este organismo pueda ser objeto de un verdadero control democrático aunque se presenten las solicitudes respectivas, como ser la inconstitucionalidad de una ley (todas la leyes relacionadas con seguridad y defensa en estos años se diseñan en el CNDS), o recurrir en amparo frente a una resolución del Consejo, porque el Presidente de la CSJ forma parte. Por otro lado, no se puede investigar una acción delictiva con imparcialidad pues el Fiscal General integra el CNDS. Tampoco es posible que una iniciativa o proyecto de ley, con el objetivo de derogar una ley o normas que hayan sido promovida desde el CNDS y que sean contrarias a los derechos fundamentales, sea discutida por la cámara legislativa, ya que el presidente del Congreso tiene el manejo discrecional de la agenda legislativa.[126]

122 Artículo 5: Son atribuciones del Consejo Nacional de Defensa y Seguridad: 1). Diseñar las políticas públicas en materia de Seguridad, Defensa e Inteligencia; 2). Armonizar las acciones entre los distintos operadores en materia de Seguridad, Defensa e Inteligencia para el mejor desempeño de sus funciones; 3). Vigilar el funcionamiento y cumplimiento de las funciones y atribuciones de la Dirección Nacional de Investigación e Inteligencia. 4). Nombrar, suspender y sustituir al Director Nacional y Director Nacional Adjunto de la Dirección Nacional de Investigación e Inteligencia; y, 5). Elaborar las acciones estratégicas que en materia de Inteligencia que sirvan para diseñar las políticas en materia de Defensa y Seguridad. Honduras "Ley Especial del Consejo Nacional de Defensa y Seguridad."

123 Honduras "Ley Orgánica del Poder Legislativo" La Gaceta No. 33, 335 del 22 de enero 2014, artículo 22.

124 Artículo 1: El consejo Nacional de Defensa y Seguridad, creado al tenor del Artículo 278 de la Constitución de la República, estará integrado por: 1.) El Presidente de la República, quien lo presidirá; 2.) El Presidente del Congreso Nacional; 3.) El Presidente de la Corte Suprema de Justicia; 4.) El Fiscal General; 5.) El Secretario de Estado en el Despacho de Seguridad; y, 6.) El Secretario de Estado en el Despacho de Defensa Nacional (…) Honduras "Ley Especial del Consejo Nacional de Defensa y Seguridad".

125 Honduras "Constitución de la República", artículo 4.

126 Honduras "Ley Orgánica del Poder Legislativo", artículo 22.

El CNDS cuenta con sus propios agentes (de investigación e inteligencia) que forman parte de la Dirección Nacional de Investigación e Inteligencia,[127] asimismo, controla la Unidad de Intervención de las Comunicaciones[128] y la División de Seguridad Aeroportuaria.[129] Estos entes no tienen supervisión ni control público independiente, ni están obligados a rendir cuentas a la población.

2.3.1.3. Normas en el sector de telecomunicaciones

A los proveedores autorizados para explotar el servicio de internet o acceso a redes informáticas, se les ha impuesto la obligación de colaboración con las autoridades de la Unidad de Intervención de las Comunicaciones y la Comisión Nacional de Telecomunicaciones en las actividades de vigilancia, al exigirles que deben:

> disponer de un sistema de seguridad para prevenir, controlar, detectar e impedir actividades ilícitas que puedan cometerse por personas usuarias/as propios o no propios del servicio [no se establece quiénes son los personas usuarias no propios, pero consideramos que se refieren a los que no han contratado directamente el servicio], mediante las cuales puedan dañar o abusar en el uso de los recursos de red internos o externos del servicio, así como, interferir, perturbar o afectar la calidad del mismo, en perjuicio, tanto del operador que le provee el servicio, así como perjudicar a otros usuarios/as y/o operadores de servicios de telecomunicaciones. Si aún disponiendo de dicho sistema, los Suscriptores/Usuarios incurren en tales actividades, los operadores están obligados a ponerlo en conocimiento, por escrito, ante las autoridades correspondientes (Ministerio Público, Comisión Nacional de Telecomunicaciones, Unidad de Intervención de las Comunicaciones, Dirección Nacional de Investigación e Inteligencia) y a prestar estas últimas toda la colaboración necesaria durante la etapa investigativa.[130]

Esto es lo que se podría denominar la tercerización en las vigilancias sin costos para el Estado. Por otra parte, a través de la Ley de Intervención a las Comunicaciones Privadas, se les impuso a las empresas de telecomunicaciones el deber de brindar la colaboración necesaria en la vigilancias en las telecomunicaciones. Esta ley en su artículo 38 establece que

> las empresas y las instituciones que brindan los servicios de comunicación [no se establece qué tipo comunicación, pero creemos que se refiere a los servicios de telefonía e internet] o cualquier otro ente natural o jurídico que se dedique a este tipo de actividad comercial están obligados a proporcionar al órgano jurisdiccional competente, a la Unidad de Intervención de las Comunicaciones y al Ministerio Público o por la Procuraduría General de la República en su caso, todas las facilidades materiales, técnicas y humanas para que

127 Artículo 6: Para su funcionamiento el Consejo Nacional de Defensa y Seguridad, conformarán la Dirección Nacional de Investigación e Inteligencia como ente encargado de ejecutar las políticas públicas que en materia de Defensa y Seguridad establezcan el Consejo, a través de las Unidades Especiales de Investigación que al efecto se creen mediante Ley, gozará de independencia funcional, administrativa y presupuestaria y responderá directamente ante el Consejo Nacional de Defensa y Seguridad. Honduras "Ley Especial del Consejo Nacional de Defensa y Seguridad". Además véase: Honduras "Ley de Inteligencia Nacional."

128 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 33.

129 Honduras "Decreto Ejecutivo PCM- 053-2014" La Gaceta No. 33, 514 (25, agosto 2014).

130 Honduras "Reglamento del Servicio de Internet o Acceso a Redes Informáticas" La Gaceta No. 32, 520 (20, mayo 2011), artículo 22.

> las intervenciones sean efectivas, seguras y confidenciales. En ese sentido, están en la obligación de adaptar a su sistema los aparatos técnicos y recursos humanos necesarios para la captación y derivación que se requieran para realizar la intervención de las comunicaciones, indistintamente del tipo de comunicación a intervenir.[131]

En cuanto a la retención de datos, se les impone el deber a todas las empresas (públicas y privadas) que brindan servicios de telefonía (no menciona qué tipo telefonía, por lo que al dejarla abierta puede incluir telefonía fija, móvil y satelital) de "guardar los datos de todas las conexiones de cada usuario por el plazo de cinco años". Los datos incluyen los números de teléfono que participan en cada conversación, su duración y la hora de la llamada. En el caso de llamadas con teléfono móvil, deberá guardarse el lugar donde se encuentra una persona usuaria cuando hace la llamada, contesta, o envía un mensaje de texto (no especifica la norma el tipo de mensaje de texto, por lo que queda abierta).

Esta obligación de retención de datos se aplica a toda empresa que brinde servicio de comunicaciones cualquiera que sea, pero no dice la norma si la retención de datos solo serán los telefónicos o si también incluye datos de internet.[132] Si estas empresas no cumplen se les sanciona con una multa y la cancelación de la licencia, sin perjuicio de la responsabilidad en que incurran sus accionistas o representantes legales.

De acuerdo con el reglamento sobre internet, las empresas que brindan este servicio tienen obligación de retener datos de sus personas usuarias por el plazo de un año. Estos datos son las direcciones IP utilizadas que sirvan como fuente para investigación judicial, sobre actividades de índole ilícita, que realicen las autoridades correspondientes (pueden ser el Ministerio Público, la Policía Nacional, las Fuerzas Armadas y la Dirección de Inteligencia). [133] La norma no refiere cuáles datos específicos deben retenerse.

Existe un grave problema además de la retención de datos, y es que ni la Ley de Intervención de las Comunicaciones ni el Reglamento de Internet prevén qué hacer con los datos una vez que transcurre

131 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 38,

132 Artículo 39: Obligación de guardar información por cinco (5) años. Las compañías que brindan servicios de telefonía, están en la obligación de guardar los datos de todas las conexiones de cada usuario por el plazo de cinco (5) años. Los datos incluyen los números de teléfono que participan en cada conversación, su duración y la hora de la llamada. En el caso de llamadas con teléfono móvil, deberá guardarse el lugar donde se encuentra un usuario cuando hace la llamada, contesta, o envía un mensaje de texto. Esta obligación es aplicable a cualquier otra empresa, institución o cualquier otro ente natural o jurídico que brindan servicios de comunicación. El incumplimiento de esta disposición, dará lugar a la aplicación de una sanción de cinco mil (5,000) a diez mil (10,000) salarios mínimos y la cancelación de la licencia, sin perjuicio de la responsabilidad en que incurran sus accionistas o representantes legales. Honduras " Ley de Intervención de las Comunicaciones Privadas."

133 Artículo 20: Los operadores del Servicio de Internet o Acceso a Redes Informáticas deben conservar la información fuente que se utilizó para la medición de los Parámetros de Calidad de Servicio, así como la de los Indicadores de Calidad, por el plazo de tiempo mínimo de un (1) año. Asimismo, por el mismo plazo de tiempo deben conservar las direcciones IP utilizadas por los usuarios del servicio, que sirva como fuente para investigación judicial o de las autoridades correspondientes sobre actividades de índole ilícitas cuando corresponde. Hondura "Reglamento del Servicio de Internet o Acceso a Redes Informáticas" La Gaceta Núm. 32,520 (20, mayo 2011)

el plazo establecido, no hay protocolos de control sobre el manejo ni la destrucción de los datos cuando estos ya no sean necesarios para la investigación.

Mediante la Ley de Portabilidad Numérica,[134] el Estado se atribuyó la propiedad de la información sobre las personas usuarias de telefonía móvil relacionada con el nombre del propietario o propietaria de un número telefónico, tal como lo dispone la norma: "la base de datos de la Central de Portabilidad Numérica es propiedad exclusiva del Estado de Honduras"; información que va a parar a la Dirección Nacional de Investigación e Inteligencia.[135]

En cuanto a las restricciones al anonimato, el Congreso Nacional realizó una reforma a la Ley de Intervención de las Comunicaciones Privadas que obliga a las empresas que prestan servicios de telefonía y cibercafés a llevar un registro de sus clientes. Asimismo, los proveedores y personas usuarias de internet que tengan asignadas IP públicas (la IP que tiene asignado cualquier equipo o dispositivo conectado a internet) de las cuales, en algunos casos, derivan IP privadas, deberán instalar en su negocio un sistema de cámaras que permita identificar en fecha y hora los clientes que hacen uso del servicio, debiendo llevar en sus sistemas un registro de la información por lo menos de los últimos treinta (30) días.[136] Esta remisión de los datos a Inteligencia de manera indiscriminada es una violación al derecho a la privacidad.

Por último, la Ley de Inteligencia en su artículo 29 creó el Sistema Nacional de Información sin que tenga ningún controlador dentro del sistema institucional del justicia (Ministerio Público, Poder Judicial, Instituto de Acceso a la Información Pública). En esta ley se establece la obligación de las instituciones públicas y privadas a entregar la información requerida por la Dirección Nacional de

134 Honduras "Ley de Portabilidad Numérica, 97-2013" La Gaceta No. 33, 188 (29, julio 2013).

135 Artículo 7: La base de datos de la Central de Portabilidad Numérica es propiedad exclusiva del Estado de Honduras, debe y tiene que estar física y digitalmente en el País, con su respectiva copia de seguridad. En aplicación al Decreto No. 243-2011 de fecha 8 de Diciembre de 2011 reformado, contentivo de la Ley Especial Sobre la Intervención de las Comunicaciones, los Operadores de Telefonía Móvil deben notificar en el término de cuarenta y ocho (48) horas a la Dirección Nacional de Investigación e Inteligencia los cambios que de uno o más números telefónicos se realicen de conformidad a esta ley. Honduras "Ley de Portabilidad Numérica".

136 Artículo 37: Registro de clientes y su identificación. Las empresas y las instituciones que brindan los servicios de comunicación, trátese de operadoras, suboperadoras, o cualquier otra empresa relacionada con esta actividad, deberán llevar un registro completo de todos sus clientes de prepago en general, clientes pos-pago que no tengan su registro completo todos los futuros clientes en general y usuarios de los servicios provistos como parte de sus obligaciones de contribución en especie. Se prohíbe y es constitutivo de sanción conforme a la normativa de multas que opera la Comisión Nacional de Telecomunicaciones (CONATEL), realizar transacciones sin haber efectuado la identificación del cliente, la que deberá realizarse de la forma siguiente: 1) Los hondureños deberán presentar su tarjeta de identidad; debiendo las operadoras y suboperadoras validar esa información con la base de datos del Registro Nacional de las Personas (RNP), o cualquiera otra similar que cumpla este propósito; y, 2) Los extranjeros deberán facilitar su carné de extranjero residente o pasaporte. Estas obligaciones también se aplican a las personas naturales o jurídicas que se dedican a proveer servicios de venta de aparatos celulares, recargas, sim o cualquier otro. Toda la información que obtengan las personas naturales o jurídicas intermediarias del servicio de comunicación o venta de accesorios deberán remitirla dentro de los dos (2) días siguientes a la compañía que les haya concesionado estos servicios. Será responsabilidad de la Comisión Nacional de Telecomunicaciones (CONATEL) llevar un registro de los proveedores y usuarios a quienes se les asigne IP públicas dentro del territorio nacional. Los proveedores y usuarios de internet que tengan asignadas IPS públicas de las cuales derivan IPS privadas, deberán instalar en su negocio un sistema de cámaras que permita identificar en fecha y hora los clientes que hacen uso del servicio, debiendo llevar en sus sistemas un registro de la información por lo menos de los últimos treinta (30) días. La infracción de esta disposición dará lugar al cierre o clausura del establecimiento mercantil. Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas."

Investigación e Inteligencia (DNII), de lo contrario se les sancionará civil, penal y administrativamente. Esta norma no establece qué tipo de información ni la razones que puedan motivar la solicitud de información.[137] Esto es grave porque para que esta Dirección obtenga información no se necesita controlador administrativo ni jurisdiccional.

2.3.1.4. Normativas de acceso a la información o transparencia

El derecho de acceso a la información pública está restringido por dos leyes. La primera de ellas es la Ley de Inteligencia Nacional, que dispone que "las actividades, informaciones y documentos de inteligencia tendrán el carácter de reservados, en vista que su contenido es confidencial o secreto, por ser elementos inherentes a la seguridad y la defensa nacional".[138] La segunda disposición normativa mencionada se blindó en enero de 2014, cuando entró en vigencia una ley especial sobre secretos oficiales en materia de seguridad y defensa.[139] De acuerdo con esta ley,

> pueden ser declaradas Materias Clasificadas los asuntos, actos, contratos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y/o defensa nacional, y el logro de los objetivos en estas materias.[140]

Es decir, que aunque sea declarada inconstitucional la norma sobre inteligencia, la transparencia sobre intervenciones podría verse obstaculizada por la Ley de Secretos Oficiales.

Como un mecanismo de presión para que se mantenga la secretividad en las intervenciones de las comunicaciones, el Congreso Nacional aprobó el delito de "infidencia", mediante el cual se sanciona a las empresas e instituciones que brindan servicios de comunicación por tecnología o cualquier otro ente natural o jurídico que se dedique a esa actividad, a sus funcionarios y funcionarias, empleados y empleadas, directores, propietarios, representantes legales, informar a la persona suscriptora del servicio, sospechosos o imputado que sus comunicaciones o medios están siendo intervenidos.[141]

137 Artículo 6 de la Ley de Inteligencia Nacional: (…) Será obligación de las instituciones públicas brindar la información que le sea requerida por la Dirección Nacional de Investigación e Inteligencia; asimismo, las entidades privadas deberán cooperar brindando la información que les sea requerida a fin de apoyar el esfuerzo de inteligencia. El incumplimiento de esta obligación, dará lugar a sanciones administrativas, civiles y penales. Honduras "Ley de Inteligencia Nacional."

138 Honduras "Ley de Inteligencia Nacional", artículo 18.

139 Honduras "Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional, 418-2013" La Gaceta No. 33, 373 (7, marzo 2014).

140 Honduras "Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional", artículo 3.

141 Artículo 51: (Delito de Infidencia) Se prohíbe a las empresas e instituciones que brindan servicios de comunicación por tecnología o cualquier otro ente natural o jurídico que se dedique a esa actividad, a sus funcionarios, empleados, directores, propietarios, representantes legales, informar al suscriptor del servicio, sospechosos o imputado que sus comunicaciones o medios están siendo intervenidos. Quienes incumplan lo establecido en este artículo incurrirán en el delito de infidencia y serán sancionados con seis (6) a nueve (9) años de reclusión y una multa equivalente de sesenta (60) a ciento veinte (120) salarios mínimos. Honduras "Ley de Intervención de las Comunicaciones Privadas."

Por otra parte, también una norma especial castiga a la persona funcionaria o empleada pública que "revele o facilite la revelación de un hecho del que tenga conocimiento por razón del cargo y que deba permanecer en secreto".[142]

2.3.1.5. Otras normas relacionadas al tema (protección de datos)

El sistema tanto de transparencia como de manejo de información funciona con base en Instituciones Obligadas, de ofrecer información al público y de la custodia de datos; la Ley de Transparencia y Acceso a la Información Pública establece una lista de Instituciones Obligadas:

- El Poder Legislativo, el Poder Judicial, el Poder Ejecutivo, las instituciones autónomas, las municipalidades y los demás órganos e instituciones del Estado;
- Las Organizaciones No Gubernamentales (ONG'S), las Organizaciones Privadas de Desarrollo (OPD's).
- En general todas aquellas personas naturales o jurídicas que a cualquier título reciban o administren fondos públicos, cualquiera que sea su origen, sea nacional o extranjero o sea por sí misma o a nombre del Estado o donde este haya sido garante, y todas aquellas organizaciones gremiales que reciban ingresos por la emisión de timbres, por la retención de bienes o que estén exentos del pago de impuestos.[143]

La Ley de Transparencia establece que "los datos personales serán protegidos siempre".[144] El reglamento de esta ley complementa la declaración de protección al establecer que "los datos personales confidenciales son de carácter personalísimo y, por tanto, irrenunciables, intransferibles e indelegables, por lo que ninguna Institución Obligada deberá proporcionarlos o divulgarlos".[145] La ley define como datos confidenciales

> los relativos al origen étnico o racial, características físicas, morales o emocionales, domicilio particular, número telefónico particular, dirección electrónica particular, participación, afiliación a una organización política, ideología política, creencias religiosas o filosóficas, estados de salud, físicos o mentales, personal o familiar y cualquier otro relativo al honor, la intimidad personal, familiar o la propia imagen.[146]

142 Artículo 349: Será castigado con reclusión de tres (3) a seis (6) años e inhabilitación especial por el doble del tiempo que dure la reclusión, funcionario o empleado público que: (...) 5) Revele o facilite la revelación de un hecho del que tenga conocimiento por razón del cargo y que deba permanecer en secreto. Cuando la revelación no fuere de grave trascendencia, la pena se rebajará en un (1/6) sexto. Honduras "Código Penal".

143 Honduras "Ley de Transparencia y Acceso a la Información Pública" La Gaceta No. 31, 193 (30, diciembre 2006), artículo 3.

144 Artículo 24: Sistematización de archivos personales y su acceso. Los datos personales serán protegidos siempre (…) El acceso a los datos personales únicamente procederá por decreto judicial o a petición de la persona cuyos datos personales se contienen en dicha información o de sus representantes o sucesores. Honduras "Ley de Transparencia y Acceso a la Información Pública."

145 Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública" La Gaceta No. 31, 552 (6, marzo 2008).

146 Honduras "Ley de Transparencia y Acceso a la Información Pública", artículo 3, numeral 7.

El reglamento de la Ley de Transparencia y Acceso a la Información Pública es contundente al establecer que "ninguna persona podrá obligar a otra a proporcionar datos personales que puedan originar discriminación o causar daños o riesgos patrimoniales o morales de las personas".[147] El mismo reglamento dispone que por regla general "sólo los interesados o sus representantes previa acreditación, podrán solicitar a una Institución Obligada que les proporcione los datos personales que obren en un sistema de datos personales";[148] esta norma deja una cláusula abierta que genera inseguridad jurídica: "sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes previa acreditación, podrán solicitar a una Institución Obligada que les proporcione los datos personales".[149]

Además del "derecho a acceder a los datos personales", la ley prevé el derecho para que se modifiquen los datos personales erróneos al decir: "Las personas interesadas o sus representantes (legales) podrán previa acreditación, solicitar a las Instituciones Obligadas correspondientes la modificación de sus datos que obren en cualquier sistema de datos personales".[150]

Reglamentariamente se establecen las responsabilidades de las Instituciones Obligadas sobre la custodia de los datos personales confidenciales y de la información confidencial, siendo las siguientes:[151]

- Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto de Acceso a la Información Pública;

147 Artículo 50: Prohibición de entrega de información. Ninguna persona podrá obligar a otra a proporcionar datos personales que puedan originar discriminación o causar daños o riesgos patrimoniales o morales de las personas. Honduras " Reglamento de la Ley de Transparencia y Acceso a la Información Pública."

148 Artículo 45: Acceso a datos personales. Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes previa acreditación, podrán solicitar a una Institución Obligada que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo hasta diez días hábiles contados desde la presentación de la solicitud en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante. La entrega de los datos personales será gratuita, debiendo él o la solicitante cubrir únicamente los gastos de producción o de envío. Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública."

149 Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública", artículo 45.

150 Artículo 46. Solicitud para que se modifiquen los datos personales erróneos. Las personas interesadas o sus representantes podrán previa acreditación, solicitar a las Instituciones Obligadas correspondientes la modificación de sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado o la interesada deberá entregar una solicitud de modificación a la Institución Obligada, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive y fundamente su petición. La Institución Obligada, en un plazo de 30 días hábiles a contar desde la fecha de la presentación de la solicitud, deberá entregar al o la solicitante una comunicación que haga constar las modificaciones o bien le informe de manera fundada y motivada, las razones por las cuales no procede la modificación. Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública."

151 Artículo 41. Instituciones obligadas responsables de la custodia de los datos personales. Sin perjuicio de lo que dispongan otras leyes sobre la protección de datos y procesos y confidencialidad de datos personales y de información entregada por particulares al Estado bajo reserva, las Instituciones Obligadas serán responsables de los datos personales confidenciales y de la información confidencial y, en relación estos, deberán (…) Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública."

- Tratar datos personales solo cuando estos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

- Poner a disposición del público, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, siguiendo los lineamientos que establezca el Instituto;

- Procurar que los datos personales sean exactos y actualizados;

- Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos en el momento en que tengan conocimiento de esta situación, y,

- Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Sin embargo, se deja abierta la posibilidad que mediante otras leyes sobre protección de datos, procesos y confidencialidad de datos personales se generen otras responsabilidades o se dejen sin valor las anteriores; sobre esto la Ley de Transparencia dispone:

Sin perjuicio de lo que dispongan otras leyes sobre la protección de datos y procesos y confidencialidad de datos personales y de información entregada por particulares al Estado bajo reserva, las Instituciones Obligadas serán responsables de los datos personales confidenciales y de la información confidencial (...)[152]

Por otra parte, se establece en el Reglamento de la Ley de Transparencia la protección de los datos personales confidenciales por tiempo indefinido, salvo consentimiento o resolución judicial y siempre que no impliquen discriminación.[153]

El acceso a los datos únicamente procederá por decreto judicial o a petición de la persona cuyos datos personales se contienen en dicha información o de sus representantes o sucesores".[154]

Hay datos personales que no están protegidos con la confidencialidad, sin embargo, no implica que el dato en sí mismo sea de carácter público; el reglamento de la Ley de Transparencia y Acceso a la Información Pública establece una enumeración de datos no confidenciales aparentemente taxativa,

152 Honduras "Ley de Transparencia y Acceso a la Información Pública".

153 Artículo 47. Plazos indefinidos de restricción del acceso a la información. Los datos personales confidenciales y la información confidencial establecida en los numerales 7) y 9) del artículo 3 de la ley no estarán sujetos a plazos de vencimiento y tendrán ese carácter de manera indefinida, salvo que medie el consentimiento expresa del titular de la información o mandamiento escrito emitido por autoridad competente. Se exceptúa lo relativo a las ofertas selladas en concurso y licitaciones, las cuales serán públicas a partir de su apertura. Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública."

154 Honduras "Ley de Transparencia y Acceso a la Información Pública", artículo 24, párrafo segundo.

pero que el último numeral lo deja abierto al determinar que quedan desprotegidos otros datos personales en otros casos determinada en otras leyes:

- Los necesarios por razones estadísticas, científicas o de interés general previstas en la ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;
- Cuando se transmitan entre Instituciones Obligadas, siempre y cuando los datos se utilicen para el ejercicio de atribuciones y funciones propias de las mismas;
- Cuando exista una orden judicial;
- A terceros, cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquellos para los cuales se le hubieren transmitido, y
- En los demás casos que establezcan las leyes.[155]

La redacción de este último numeral podemos encontrarla en muchas normas de la legislación hondureña, de una aparente taxatividad (*numerus clausus*) se pasa a clausulas abiertas (*numerus apertus*), con las que se terminan limitando los derechos.

El procedimiento establecido, cuando una Institución Obligada reciba una solicitud sobre datos personales, contempla que se puede requerir al titular del dato para que se pronuncie si autoriza la entrega del dato; esto implica que la Institución Obligada no tiene obligación de requerir, por lo que queda a su discreción consultar o no.[156] En caso que la Institución Obligada acceda a la entrega del dato, deberá omitir los datos confidenciales.[157]

155 Artículo 44. Casos en que no es necesaria la autorización para acceder a datos personales. No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos: 1. Los necesarios por razones estadísticas, científicas o de interés general previstas en Ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran; 2. Cuando se transmitan entre Instituciones Obligadas, siempre y cuando los datos se utilicen para el ejercicio de atribuciones y funciones propias de las mismas; 3. Cuando exista una orden judicial; 4. A terceros, cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquellos para los cuales se le hubieren transmitido; y, 5. En los demás casos que establezcan las leyes. Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública."

156 Artículo 49. Requerimiento de acceso a información confidencial. Cuando una Institución Obligada reciba y considere pertinente una solicitud de acceso a un expediente o documento que contengan información confidencial, podrá requerir a la persona titular de la información su autorización para entregarla, quien tendrá diez días hábiles para responder a partir de la notificación correspondiente. El silencio de la persona requerida será considerado como una negativa (…) Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública".

157 Artículo 49. Requerimiento de acceso a información confidencial. Cuando una Institución Obligada reciba y considere pertinente una solicitud de acceso a un expediente o documento que contengan información confidencial (…) La Institución Obligada deberá dar a acceso a las versiones públicas de los expedientes o documento a que se refiere el párrafo que antecede, en las que se omitan los documentos o las partes o secciones de estos que contenga información confidencial aún en los casos que no se haya requerido a la persona titular de la información para que otorgue su consentimiento o bien se obtenga una negativa expresa o tacita del mismo. Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública".

En otra norma de la legislación hondureña existe una restricción a la autodeterminación informativa sobre los datos de funcionarios/as públicos relacionados con el sistema de justicia y persecución del delito. Se prevé que esos datos los manejará la Dirección de Investigación e Inteligencia, la norma refiere

> que se contará con una base de datos que contenga toda la información del personal que labore en los entes a los que les es aplicable la Ley (de pruebas de confianza) para efecto de control y seguimiento. En consecuencia los órganos están obligados a actualizar esta información una vez al año.[158]

Por otra parte la Ley de Transparencia y Acceso a la Información Pública, regula las bases de datos personales y establece que "las personas naturales o jurídicas que por razón de su trabajo elaboren bases de datos personales e información confidencial, no podrán utilizarla sin el previo consentimiento de la persona a que haga referencia la información.[159]

Para tener un control de quienes elaboran o cuentan con bases de datos se establece reglamentariamente que "las Instituciones Obligadas que posean, por cualquier título, sistemas o bases de datos personales, deberán hacerlo del conocimiento de Instituto de Acceso a la Información Pública, que mantendrá un listado actualizado de dichos sistemas o bases".[160]

También se establece la prohibición para las Instituciones Obligadas de difundir, distribuir o comercializar ni permitir el acceso a los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones.[161] El Instituto de Acceso a la Información Pública podrá recibir quejas por abusos en la recolección de información con datos personales o confidenciales. El Instituto impondrá las medidas correctivas y establecerá recomendaciones a quienes atenten contra la divulgación no autorizada de los datos personales y confidenciales.[162]

Se establecen como infracciones administrativas sobre el manejo de datos personales por parte de las personas que laboran para las Instituciones Obligadas:

158 Honduras "Ley General de la Superintendencia para la Aplicación de Pruebas de Evaluación y de Confianza" La Gaceta No. 33, 372 (6, marzo 2014), artículo 7.

159 Artículo 42. Bases de datos personales y de información confidencial. Las personas naturales o jurídicas que por razón de su trabajo elaboren bases de datos personales e información confidencial, no podrán utilizarla sin el previo consentimiento de la persona a que haga referencia la información. En todo caso, nadie estará obligado en suministrar información conteniendo datos personales o información confidencial. Las Instituciones Obligadas que posean, por cualquier título, sistemas o bases de datos personales, deberán hacerlo del conocimiento de Instituto que mantendrá un listado actualizado de dichos sistemas o bases. El Instituto podrá recibir quejas por abusos en la recolección de información con datos personales o confidenciales. El Instituto impondrá las medidas correctivas y establecerá recomendaciones a quienes atenten contra la divulgación no autorizada de los datos personales y confidenciales. Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública."

160 Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública", artículo 42.

161 Artículo 43. Prohibición de difundir y comercializar datos personales. Las Instituciones Obligadas no podrán difundir, distribuir o comercializar ni permitir el acceso a los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso escrito directo o autenticado, de las personas a que haga referencia la información. Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública".

162 Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública", artículo 42.

- En el caso de datos personales, se negare a proporcionarlos a su legítimo titular, sus sucesores o autoridad competente.

- Fuera de los casos previstos en la Ley de Transparencia y Acceso a la Información Pública, recoja, capte, transmita o divulgue datos personales, o se niegue a rectificarlos, actualizarlos o eliminar información falsa en los datos personales confidenciales contenidos en cualquier archivo, registro o base de datos de las Instituciones Obligadas.[163]

Las infracciones anteriores serán sancionadas con amonestación por escrito, suspensión, multa, cesantía o despido. Las multas de entre medio salario hasta cincuenta (50) salarios mínimos mensuales, serán impuestos por el Instituto de Acceso a la Información Pública, (IAIP), dependiendo de la gravedad de la infracción.[164]

A nivel de protección penal, es aplicable la protección establecida en el Código Penal para el derecho a la intimidad, el "delito de revelación de secretos (privados)", que de acuerdo con la configuración normativa se castiga la revelación de cualquier secreto siempre y cuando la persona que lo revela se haya enterado por razón de oficio, empleo, profesión o arte.[165]

Hay una cuestión grave en el país y es la concentración de datos a través de la creación del "Centro Nacional de Información", que es una dependencia técnica de la Dirección Nacional de Investigación e Inteligencia en la que se integran las diferentes bases de datos de las entidades públicas que administran información de interés para la seguridad y la defensa nacional; la norma establece que "para tal fin el Centro Nacional de Información adquirirá la plataforma tecnológica que permita la interconexión con las entidades públicas, quienes facilitaran este proceso.[166]

Por otra parte, derivado de esta ilegalidad en el control de datos, de acuerdo con una resolución del Consejo Nacional de Defensa y Seguridad, este sistema se alimenta de las bases de datos de varias instituciones del Estado: la Corte Suprema de Justicia; la Secretaría de Seguridad y la Policía Nacional; la Dirección Nacional de Investigación e Inteligencia; la Dirección de Información Estratégica de las Fuerzas Armadas; la Secretaría de Relaciones Exteriores y Cooperación Externa; la Unidad

163 Artículo 27. Infracciones administrativas. Sin perjuicio de la responsabilidad civil, incurrirá en infracción a esta Ley, quien: 1) (…) 2. (...) En el caso de datos personales, se negare a proporcionarlos a su legítimo titular, sus sucesores o autoridad competente. 3) (…) 4. Fuera de los casos previstos en esta Ley, recoja, capte, transmita o divulgue datos personales, o se niegue a rectificarlos, actualizarlos o eliminar información falsa en los datos personales confidenciales contenidos en cualquier archivo, registro o base de datos de las Instituciones Obligadas por esta Ley (…) Honduras "Ley de Transparencia y Acceso a la Información Pública."

164 Artículo 28. Sanciones administrativas. Sin perjuicio de la responsabilidad civil, las infracciones no constitutivas de delito, serán sancionadas con amonestación por escrito, suspensión, multa, cesantía o despido. Las multas de entre medio salario hasta cincuenta (50) salarios mínimos mensuales, serán impuestos por el Instituto de Acceso a la Información Pública, (IAIP), dependiendo de la gravedad de la infracción, debiendo ser enterados dichos valores en la Tesorería General de la República. Honduras "Ley de Transparencia y Acceso a la Información Pública."

165 Honduras "Código Penal" Congreso Nacional (1985), artículo 215.

166 Honduras "Ley de Inteligencia Nacional", artículo 29,

de Intervención Financiera; la División de Seguridad Financiera; la Unidad de Intervención de las Comunicaciones; el Instituto de Migración; el Sistema Nacional de Acueductos; la Empresa Nacional de Energía Eléctrica; la Dirección Ejecutiva de Ingresos; el Instituto de la Propiedad; la Dirección de Lucha Contra el Narcotráfico; el Ministerio Público; el Instituto Hondureño de Seguridad Social; la Unidad de Inteligencia de la Comisión Nacional de Bancos y Seguros; la Dirección General de Marina Mercante; el Registro Nacional de las Personas y otras que se puedan incorporar en el futuro[167]. Todo esta información fue declarada en reserva en la misma resolución 69/2014 y con base en la Ley de Secretos Oficiales.[168]

Existe un anteproyecto de ley promovido por el Instituto de Acceso a la Información Pública denominado "Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data de Honduras", que hace mención al concepto de "Autodeterminación Informativa", esta ley es de orden público y tiene por objeto la protección de los datos personales con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.[169] Este proyecto tiene postulados muy importantes como por ejemplo que la protección de datos es un derecho fundamental.[170]

Sin embargo, en el ámbito de aplicación de este anteproyecto se dejan fuera bases de datos muy sensibles que pondrían en serio peligro el derecho a la privacidad de las personas, pues se contempla que la ley no se aplicará a las bases de datos siguientes:

> a) A las bases de datos mantenidas por personas naturales en el ejercicio de actividades exclusivamente personales o domésticas.
>
> b) Las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.
>
> c) Las bases de datos creadas y reguladas por leyes especiales.[171]

---

167 Consejo Nacional de Defensa y Seguridad, Resolución CNDS-069-2014 del 14 de julio 2014.

168 Esta Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional, tiene disposiciones abiertas para decretar secretividad no solo en seguridad y defensa.

169 Instituto de Acceso a Información Pública. *Anteproyecto de Ley de Protección de Datos Personales y Acción de Hábeas Data*. (Honduras: Instituto de Acceso a Información Pública: 2014), artículo 1.

170 Art. 3 Definiciones: Derecho fundamental a la protección de datos: Es el derecho que toda persona tiene a controlar sus datos personales que se encuentran registrados en bases de datos de entidades públicas o privadas, personas naturales o jurídicas. Instituto de Acceso a Información Pública. *Anteproyecto "Ley de Protección de Datos Personales y Acción de Hábeas Data*.

171 Artículo 2 : Ámbito de aplicación. Esta Ley será de aplicación a los datos personales registrados en bases de datos automatizadas o manuales, de organizaciones del sector público como del sector privado, y a toda modalidad de uso posterior de estos datos. El régimen de protección de datos personales que se establece en la presente Ley no será de aplicación: a) A las bases de datos mantenidas por personas naturales en el ejercicio de actividades exclusivamente personales o domésticas; b) Las bases de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito; c) Las bases de datos creadas y reguladas por leyes especiales, y d) Las bases de datos y archivos de información periodística y otros contenidos editoriales. Instituto de Acceso a Información Pública. *Anteproyecto "Ley de Protección de Datos Personales y Acción de Hábeas Data*.

Es decir, que permite la existencia de un sistema paralelo de retención de datos que vulneran el derecho a la autodeterminación informativa, que viola los estándares internacionales de derechos humanos (idoneidad, proporcionalidad, necesidad, sobre todo el de proporcionalidad). En ese sentido, esta disposición restrictiva es mucho mas fuerte que la norma de protección de datos.

2.3.1.6. Otras normas especificas que regulen el cifrado

En relación con normas específicas relacionadas con el cifrado, solo encontramos la definición siguiente: "cifrado es el sistema mediante el cual, con la ayuda de técnicas diversas o programas informáticos, se cifra o codifica determinada información con la finalidad de volverla inaccesible o ininteligible".[172]

También existe una norma protectora de manera general pero que se puede usar en relación al cifrado, pues "ninguna persona [incluyendo agentes estatales] podrá obligar a otra a proporcionar datos personales que puedan originar discriminación o causar daños o riesgos patrimoniales o morales de las personas".[173]

2.3.1.7. Otras normas de debido proceso que expliquen el proceso para revelar la identidad de la persona anónima si existe

No existe ninguna norma particular que obligue a una persona a revelar la identidad anónima *a priori* a la comision de algún delito.

2.3.2. Otras normas que regulen el allanamiento de casas/oficinas, registros y secuestro de computadora

Como consecuencia de la inviolabilidad del domicilio, ningún ingreso o registro podrá verificarse sin el consentimiento de cualquiera de las personas que lo habitan o sin que sea por cumplimiento de orden emanada de autoridad competente, es decir, que como regla general el ingreso a un domicilio debe ser mediando consentimiento de sus moradores y como excepción en virtud de cumplimiento de una orden emitida por autoridad competente o cuando exista una causa de gravedad calificada.[174] Según la Sala de lo Penal de la Corte Suprema de Justicia, de allí se deriva "la diferencia entre un ingreso y/o registro autorizado, un allanamiento como acto investigativo y un allanamiento ante un estado de necesidad o delito flagrante."[175] Nos referiremos aquí solo a dos de las circunstancias de allanamiento: 2.3.2.1. Allanamiento por orden judicial

172 Artículo 3: Definiciones. Para los efectos de aplicación de esta ley se deberá entender por: (…) 7) CIFRADO O CODIFICADO: Es el sistema mediante el cual, con la ayuda de técnicas diversas o programas informáticos, se cifra o codifica determinada información con la finalidad de volverla inaccesible o ininteligible. Honduras "Ley de Intervención de las Comunicaciones Privadas."

173 Honduras "Reglamento de la Ley de Transparencia y Acceso a la Información Pública", artículo 25.

174 Honduras "Constitución de la República", artículo 99,

175 Sala de lo Penal. Sentencia número CP-303-2010, 21-22.

De acuerdo con la Sala de lo Penal de la Corte Suprema de Justicia, el allanamiento por orden judicial es "el acto de investigación consistente en la penetración a un determinado recinto aislado del exterior, sin la autorización de sus moradores, con la finalidad de buscar, identificar y recoger fuentes de investigación y/o a la propia persona del imputado".[176] El artículo 99 constitucional manda que el allanamiento, aún con orden judicial, deberá iniciarse entre las seis de la mañana y las seis de la tarde. La misma Sala Penal de la CSJ establece que,

> el propósito de que la ley determine que únicamente un Órgano Jurisdiccional pueda ordenar el allanamiento de un domicilio es debido a que el Tribunal evaluará la necesidad racional y la proporcionalidad, entre el principio *pro-Societate* de la persecución e investigación de un hecho delictivo y la garantía constitucional a la inviolabilidad del domicilio, para la práctica de estas diligencias.[177]

El Decreto Judicial que ordene la práctica de un allanamiento deberá reunir los requisitos señalados en el artículo 213 del Código Procesal Penal,[178] ordenado por el Órgano Jurisdiccional con competencia en el lugar en donde se lleve a cabo. Aún con orden judicial, el allanamiento que se practique irrespetando el protocolo contemplado para el efecto en los artículos 214[179] y 215[180] del Código Procesal Penal, será calificado como ilegal.

2.3.2.2. Allanamiento por estado de necesidad

En cuanto a los allanamientos por un estado de necesidad o delito flagrante, establece el artículo 99 de la Constitución que

> se exceptúa a lo anterior, es decir que se podrá realizar un allanamiento sin autorización de las personas que lo habitan o sin orden de autoridad competente y aún fuera de las horas establecidas para ello (06:00 a.m. a 06:00 pm), cuando sea con el objeto de impedir

176 Sala de lo Penal. Sentencia número CP-303-2010, 23.

177 Sala de lo Penal. Sentencia número CP-303-2010, 23.

178 Artículo 213: Mandamiento y Contenido de la Orden de Allanamiento. Para practicar un allanamiento, el juez expedirá mandamiento que contendrá los requisitos siguientes: 1) El órgano jurisdiccional que ordena el allanamiento y el asunto con el que se relaciona; 2) La indicación precisa del lugar o lugares que habrán de ser registrados; 3) La indicación de ser registrados; 4) La designación de juez ejecutor, el que en todo caso deberá estar acompañado por agentes de la Dirección General de Investigación Criminal (DGIC) o en su defecto por la Policía Nacional Preventiva; 5) El motivo preciso del allanamiento, con indicación concreta de las personas u objetos buscados, si son conocidos, y de las diligencias por practicar; y, 6) La fecha, la firma y sello del juez. Honduras "Código Procesal Penal."

179 Artículo 214: Procedimiento y Formalidades a que están sujetos los Allanamientos. La orden de allanamiento será notificada a quien habite la casa o lugar en que deba efectuarse. La notificación se hará mediante entrega de una copia del mandamiento. Si quien habita la casa o lugar se encuentra ausente, la notificación se hará al encargado de aquélla y, en su defecto, a cualquier persona mayor de edad que se encuentre en el sitio, particularmente a los parientes del primero. El notificado será invitado a presenciar el registro. Si no se encuentra persona alguna en el lugar o si quien habita la casa se opone al ingreso, éste se hará con el auxilio de la fuerza pública. Practicado el registro, se consignarán en acta los hechos más importantes ocurridos durante el mismo y sus resultados. Se cuidará, en su caso, que el lugar quede cerrado y debidamente protegido hasta el regreso de quienes lo habitan. Honduras "Código Procesal Penal."

180 Artículo 215: Personas que podrán participar en un allanamiento. En el allanamiento solo podrán participar las personas designadas para el efecto, por la autoridad competente. Durante el mismo se evitarán las inspecciones que no guarden relación con los hechos que se investigan y no se perjudicará o importunará al investigado más de lo estrictamente necesario. Se evitará igualmente comprometer su reputación y se respetarán todos los secretos que no interesen a la investigación. Ni los medios de comunicación ni otras personas no autorizadas, tendrán acceso al domicilio durante la práctica del allanamiento. Honduras "Código Procesal Penal."

> la comisión de un delito, para impedir la impunidad de delitos, para impedir daños graves a la persona o para impedir daños graves a la propiedad. [181]

Lo anterior es desarrollado por el Código Procesal Penal que en su artículo 212 establece los supuestos bajo los cuales el Ministerio Público podrá ordenar un allanamiento sin orden judicial y los supuestos bajo los cuales la autoridad policial, sin orden judicial y sin orden del Ministerio Público, puede practicar un allanamiento.[182]

2.3.2.3. Registro de sitios públicos

De acuerdo con el Código Procesal Penal, los registros que no impliquen un allanamiento de morada se podrán efectuar cuando existan motivos para presumir que en un lugar público se ha cometido un delito o que en el mismo existen pruebas relacionadas con el que se está investigando o que en él se encuentra alguna persona fugada o sospechosa de haber participado en la comisión de un delito, se registrará el lugar sin más trámite. Es decir, que una oficina de una organización ya sea de derechos humanos u organización social, puede entrar en la categoría de sitios públicos.[183]

2.4. Supervisión pública

La supervisión y el control de las conductas públicas son componentes indispensables para el funcionamiento del Estado de derecho. Para que la supervisión sea efectiva y legítima deben crearse mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones, estos deben tener la autoridad para acceder a toda la información potencialmente relevante para evaluar el uso legítimo de medidas de vigilancia de comunicaciones.

---

181 Honduras "Constitución de la República", artículo 99,

182 Artículo 212: Requisitos para practicar allanamiento de moradas. El allanamiento de una morada, casa o lugar en que viva una persona, sólo podrá efectuarse previa orden escrita del órgano jurisdiccional competente. Lo dispuesto en el párrafo anterior no será aplicable en caso de flagrancia o cuando la medida sea necesaria para impedir la comisión de un delito, para evitar la fuga de un delincuente o la destrucción, pérdida u ocultamiento de las pruebas o evidencias con miras a lograr la impunidad de los responsables y no sea posible esperar el tiempo necesario para solicitar la autorización judicial. En estos casos, el Ministerio Público, una vez practicado el allanamiento, lo pondrá inmediatamente en conocimiento del juez competente, al que explicará las razones que lo determinaron. El juez, por auto motivado, convalidará o anulará, total o parcialmente, lo actuado. En lo demás, se estará a lo dispuesto por el artículo 99 de la Constitución de la República. Honduras "Código Procesal Penal."

183 Artículo 209: Registro de Sitios Públicos. Cuando existan motivos para presumir que en un lugar público se ha cometido un delito o que en el mismo existen pruebas relacionadas con el que se está investigando o que en él se encuentra alguna persona fugada o sospechosa de haber participado en la comisión de un delito, se registrará el lugar sin más trámite. El registro de templos, edificios públicos, instalaciones militares o, en general, de bienes del Estado, se efectuará con solo hacérsele saber a la persona a cuyo cargo se encuentren. Dicha persona podrá asistir a la diligencia o nombrar a otra para que la represente. La negativa a permitir el registro será constitutiva del delito de desobediencia. Si en cualquiera de los lugares mencionados en los párrafos precedentes existen bienes muebles cerrados o compartimientos también cerrados, en los que se presuma que se encuentran elementos útiles para la investigación de un hecho criminal, podrán ser inspeccionados de conformidad a lo que disponen los artículos 207 y 208, precedentes. El registro se practicará en presencia de quienes se encuentren en el lugar. Los elementos probatorios de la comisión de un delito serán mantenidos en depósito por la Dirección General de Investigación Criminal (DGIC) o de acuerdo con lo que disponga el Fiscal encargado de la investigación del hecho, conforme lo establecido en el artículo 217. De todo lo actuado se dejará constancia en acta, la que deberá reunir los requisitos establecidos en el artículo 207 precedente. Honduras "Código Procesal Penal."

La supervisión de las vigilancias debería efectuarse por el Ministerio Público, el Poder Judicial o el Congreso Nacional, sin embargo, al analizar que en Honduras las vigilancias la lleva a cabo la Unidad de Intervención de las Comunicaciones,[184] que es un órgano de la Dirección Nacional de Investigación e Inteligencia (como ente encargado de ejecutar las políticas públicas en materia de defensa y seguridad),[185] esta a su vez es la plataforma de la operatividad del Consejo Nacional de Defensa y Seguridad (que en el apartado sobre "inteligencia" se estableció que es un ente concentrador de poder que limita los contrapesos institucionales, ya que está conformado por el Ministerio Público y la Corte Suprema de Justicia, entre otros). Por lo que podemos deducir que no existe un controlador independiente en el actual sistema institucional hondureño.

Esta conclusión se ve reforzada con el análisis sobre la secretividad oficial, pues la Ley de Inteligencia Nacional dispone que por el solo hecho de existir "las actividades, informaciones y documentos de inteligencia, tendrán el carácter de reservados" por un término de cinco años,[186] y con la Ley sobre Secretos Oficiales se puede elevar a otro rango de secretividad hasta por veinticinco años. Este es un problema en sí mismo, pero se ve aumentado porque es el CNDS quien establece la secretividad,[187] la prórroga de la secretividad[188] y la publicidad. Solo puede solicitar la desclasificación de un documento el fiscal general de la República y será el mismo CNDS quien resolverá si un documento puede desclasificarse o no.[189]

184 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 33.
185 Honduras "Ley Especial del Consejo Nacional de Defensa y Seguridad" Poder Legislativo, artículo 6,
186 Honduras "Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional" Poder Ejecutivo (2013), artículo 3.
187 Honduras "Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional", artículo 5.
188 Honduras "Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional", artículo 7.
189 Honduras "Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional", artículo 7.

3. Marco legal nacional y su adecuación 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.[190]

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. Ellos sirven como guía para que los Estados, los y las funcionarias públicas o la sociedad civil pueda evaluar si las leyes de vigilancia en Honduras se aplican en el marco de respeto de los derechos humanos.[191]

Los 13 Principios han sido citados en el informe el Grupo de Revisión del presidente de los Estados Unidos sobre Inteligencia y Tecnologías de las Comunicaciones,[192] el informe de la Comisión Interamericana de Derechos Humanos,[193] el Reporte sobre Anonimato y Cifrado del Relator sobre Libertad de Expresión de Naciones Unidas,[194] y el Reporte de Privacidad en la Era Digital del Alto Comisionado de Derechos Humanos de Naciones Unidas,[195] entre otros. Al ser ello así, tanto los tratados como las decisiones judiciales que interpretan los 13 Principios son aplicables a Honduras.

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

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

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

193 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)

194 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)

195 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, www.ohchr.org/EN/HRBodies/HRC/.../Session27/.../A-HRC-27-37_sp.do (consultado: 16 septiembre, 2013)

3.1. Legalidad

En términos de **legalidad**, se aprecia que los límites y requisitos de la intervención de las comunicaciones en el marco de la investigación penal no están bien delimitados. En primer lugar, la Ley de Intervención de la Comunicaciones en su artículo 6 establece que las intervenciones entre "personas presentes realizadas en lugares públicos" podrán efectuarse sin ningún procedimiento ni requisito legal. Esta situación es grave, ya porque no se establece qué debe entenderse por "lugar público", ya porque de acuerdo con la jurisprudencia hondureña se determina como "el espacio físico privado" solo el domicilio, todo lo demás es considerado público. En segundo lugar, la misma norma permite la intervención de las comunicaciones en los domicilios por la mera "sospecha" de la futura comisión de un delito (pero necesita orden judicial).

> Cualquier limitación a los derechos humanos debe ser prescrita por ley. La ley debe ser pública y cumplir un estándar de claridad y precisión suficientes para prever el alcance de las medidas de vigilancia de comunicaciones.

El artículo 3 numeral 11 de la Ley de Intervención a las Comunicaciones define que la intervención a las comunicaciones consiste en:

> el procedimiento a través del cual, se escucha, capta, registra, guarda, graba, u observa [...] una comunicación que se efectúa, mediante cualquier tipo de transmisión, emisión o recepción de signos, símbolos, señales escritas, imágenes, sonidos, correos electrónicos o información de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros medios, sistemas electromagnéticos, telefonía, radiocomunicación, telegrafía, medios informáticos o telemáticos, o de naturaleza similar o análogo, así como la comunicación que se efectúe a través de cualquier medio o tipo de transmisión.[196]

Por otra parte el artículo 10 de la Ley de Intervención a las Comunicaciones establece que la intervención a las comunicaciones "debe recaer sobre las comunicaciones y medios de soporte, físicos o virtuales (…)" y "sobre aparatos de comunicación y otros medios de soporte similar".

Estas normas no son precisas y dejan abierta la puerta para futuros usos de técnicas y tecnologías de vigilancia que pueden llegar a ser desproporcionadas o requerir de estándares más altos de protección, por lo que inhiben una discusión pública en el Congreso sobre la necesidad de esas garantías adicionales.

196 Honduras "Ley de Intervención de las Comunicaciones Privadas", artículo 3, numeral 11.

3.2. Objetivo legítimo

> Las leyes que establezcan medidas de vigilancia de las comunicaciones deben perseguir objetivos legítimos y no ser aplicada de manera discriminatoria.

Este desequilibrio en la rigurosidad del marco legal también se aprecia si se analiza el **legítimo objetivo de las actividades de vigilancia.** La Ley de Intervención de las Comunicaciones se aplica a cualquier delito[197] con el solo requisito que no exista una "medida menos gravosa", pero sin establecer los parámetros para la determinación de esta.

Por otra parte y aún más grave, es que la ley en su artículo 46 permite utilizar "la información recabada mediante la intervención de comunicaciones realizada por orden del órgano jurisdiccional" en "otras investigaciones u ofrecida como medio probatorio en procesos distintos para el cual fue emitido la orden de intervención".

3.3. Necesidad, idoneidad y proporcionalidad

Necesidad: La vigilancia de las comunicaciones solo debe llevarse a cabo cuando la consecución del objetivo legítimo no pueda alcanzarse a través de métodos menos lesivos a los derechos humanos. La carga de demostrar dicha justificación le corresponde al Estado.

Idoneidad: Las medidas de vigilancia de comunicaciones deben ser apropiadas y capaces de conseguir el objetivo legítimo perseguido.

Proporcionalidad: Las medidas de vigilancia solo deben autorizarse por una autoridad judicial independiente cuando exista un alto grado de probabilidad de que un delito grave o una amenaza específica, actual y comprobable a la seguridad nacional, pueda materializarse. Las medidas de vigilancia adoptadas deben ser las menos invasivas posibles, lo cual implica que solamente se obtendrá, retendrá o utilizará la información relevante para la consecución del objetivo legítimo que justifica la autorización y por períodos de tiempo limitados.

Los principios de **necesidad, idoneidad y proporcionalidad** son recogidos en la Ley de Intervenciones en el artículo 5, en similares condiciones. Se exige su razonamiento pero mínimamente. Además las normas no son precisas en cuanto al principio de necesidad para el caso; como único requisito previo para solicitar la intervención, es que exista una investigación abierta y que la misma cuente con un número de registro (artículo 14), exigiendo del peticionario (Fiscalía o Procuradoría de la República) que razone la solicitud (artículo 15), que califique el tipo penal por el que se presenta la solicitud (artículo 15), que se señalen los datos de identificación de los servicios de comunicación a

197 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 1, 5 numeral 2 y 8.

intervenir (artículo 15), y que se identifique a las personas afectadas, sin embargo, se puede omitir este requisito si no se conocen los nombres y apellidos de las personas a vigilar (artículo 15), el período durante el cual se llevará a cabo la vigilancia (artículo 15), pero no se exige la presencia de indicios delictivos suficientes. Algo grave es que la intervención por un delito puede ser utilizada como prueba de la comisión de cualquier otro delito distinto al que sirvió de fundamento para la autorización (artículo 47).

3.4. Autoridad judicial competente

Las medidas de vigilancia de comunicaciones deben ser autorizadas de manera previa, o inmediata con efecto retroactivo en casos de emergencia, por una autoridad judicial competente, independiente e imparcial.

La **autoridad judicial competente** está determinada en la Ley de Intervenciones de las Comunicaciones para autorizar las intervenciones a las comunicaciones, por medio de los Juzgados en Materia Penal (art. 12). El problema esta en la independencia, pues las políticas de seguridad pública son diseñadas por el Consejo Nacional de Defensa y Seguridad, presidido por el presidente de la República y de la cual forma parte el presidente de la Corte Suprema de Justicia, quien a su vez es el presidente del Consejo de la Judicatura que tiene las facultades de nombramiento, remoción y sanción de los jueces y juezas. Luego, el órgano operativo del Consejo Nacional de Defensa y Seguridad es la Fuerza Nacional Interinstitucional (FUSINA), formado por las Fuerzas Armadas, la Policía Nacional, la Dirección Nacional de Defensa y Seguridad y todos los operadores de justicia a nivel nacional. A su vez, la Dirección de Inteligencia tiene bajo su jerarquía a la Unidad de Intervención de las Comunicaciones. Incluso, la Ley de la Policía Militar establece que en los operativos será acompañada de jueces y fiscales asignados a la Policía Militar[198], que luego (en el caso de los jueces o juezas), serán los mismos que resuelvan para el caso una solicitud de intervención de las comunicaciones en una investigación efectuada por la Policía Militar.

3.5. Debido proceso

Las decisiones de autorización de medidas de vigilancia de comunicaciones deben garantizar el debido proceso. Lo anterior implica que, cuando para la consecución del objetivo legítimo, y en particular la protección de la vida de una persona, sea necesaria la secrecía de la medida o su aplicación inmediata, existan otras medidas que garanticen la protección de los intereses del afectado como lo es la designación de una persona o institución que asuma representación general de sus intereses en la audiencia o que la autorización judicial se lleve a cabo con efecto retroactivo.

198 Honduras "Ley de la Policía Militar del Orden Público" La Gaceta No.33, 211 (24, agosto 2013), artículo 8.

Las decisiones de autorización de medidas de vigilancia sobre comunicaciones no garantizan el **debido proceso** en la normativa hondureña, pues no se ha contemplado la publicidad de los expedientes, tanto antes, durante, ni después de realizadas la vigilancia; esto se agrava porque incluso que el acusado o acusada esté detenida (o aunque no lo esté, que ya este personado en el proceso) no se prevé que se le notifique previamente la intervención (en realidad en la investigación no tendría sentido si se notifica previamente), con lo cual se viola lo que establece el Código Procesal Penal (en relación al derecho a la defensa), el derecho a participar en la producción de medios de prueba y a oponerse a la limitación de derechos fundamentales cuando ya está acusado, en caso contrario hay nulidad por indefensión (artículo 19, 20 y 21 de la Ley de Intervención de las Comunicaciones). Es comprensible que en algunos casos la completa publicidad del proceso puede comprometer los objetivos de la investigación; lo que que más preocupa es que la ley no establece obligaciones de hacer públicos dichos expedientes en el futuro. Incluso, distintas disposiciones establecen la reserva absoluta de cualquier funcionario público o privado involucrado en las actividades de intervención de las comunicaciones (art. 19 y 48 de la Ley de Intervención de las Comunicaciones).

3.6. Notificación del usuario

> Las personas afectadas por medidas de vigilancia de comunicaciones deben ser notificadas de ello y tener acceso a las materiales que pretendan ser o hayan sido obtenidos. La notificación podrá diferirse cuando la misma ponga en riesgo la consecución del objetivo legítimo o exista un riesgo inminente de peligro a la vida humana.

Por otra parte, no se establece en la normativa hondureña el derecho a la **notificación del usuario ni previa ni diferida.** El Código Procesal Penal exige la notificación previa de cualquier diligencia investigativa una vez que se ha presentado acusación, no obstante la Ley de Intervención de las Comunicaciones en su artículo 21 establece la "reserva del Expediente" mientras dura la vigilancia y que el mismo deberá incorporarse al expediente principal cuando ya haya finalizado la misma. En cuanto a la vigilancia realizada en etapa administrativa (sin que se llegue a presentar acusación), no se exige la notificación al vigilado/a, tampoco se refiere a qué se hará con la información.[199]

3.7. Transparencia

Para hacer efectivo el Principio de Transparencia, ni en la Ley de Intervención de las Comunicaciones ni en el resto de legislación existen disposiciones normativas legales que obliguen a las entidades que llevan a cabo estas actividades a informar periódicamente del número, tipo y ámbito de las que llevan a cabo. A estas actividades podrían aplicarse las normas de la Ley de Transparencia y

199 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 20.

Transparencia: El Estado debe publicar de manera periódica información estadística sobre las medidas de vigilancia encubierta llevadas a cabo. Como mínimo debe publicar el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad, tipo y propósito.

Acceso a la Información Pública, sin embargo, los datos que se generan en la Unidad de Intervención de las Comunicaciones tienen la categoría de "información de Inteligencia" ya que la Unidad de Intervención de las Comunicaciones es una dependencia de la Dirección Nacional de Investigación e Inteligencia y la Ley de Inteligencia en los artículos 18 y 19 contiene mecanismos de secretividad legal sin procedimientos, al establecer que "las actividades, informaciones y documentos de inteligencia, tendrán el carácter de reservados, en vista que su contenido es confidencial o secreto, por ser elementos inherentes a la seguridad y la defensa nacional" y que "la información reservada, obtenida y manejada por el Sistema Nacional de Inteligencia cuyo conocimiento público vulnere la privacidad de las personas y la seguridad nacional, queda exenta del escrutinio de cualquier organismo o persona natural".

Por lo que no existe podemos afirmar que hay vulneración al principio de transparencia.

3.8. Supervisión pública

Supervisión Pública: Deben establecerse mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones. Dichos mecanismos de supervisión independiente deben tener la autoridad para acceder a toda la información potencialmente relevante para evaluar el uso legítimo de medidas de vigilancia de comunicaciones.

En cuanto a la **supervisión pública,** el estándar se refiere a mecanismos independientes de supervisión, que no existen en la Ley de Intervención de las Comunicaciones y si bien es cierto existe el Instituto de Acceso a la Información Pública, este no tiene facultades para supervisar a la Unidad de Intervención de las Comunicaciones. Si la información manejada por la la Unidad de Intervención de las Comunicaciones es considerada "reservada o secreta" por ser materias de Inteligencia Nacional, y ambas categorías son recogidas por la Ley de Secretos Oficiales,[200] misma que establece como órgano encargado de autorizar la publicidad de la información considerada como reservada o secreta, al Consejo Nacional de Defensa y Seguridad, que es el superior jerárquico tanto de la Dirección de Inteligencia como de la Unidad de Intervención de las Comunicaciones, y tomando en cuenta que del mismo forman parte la Corte Suprema de Justicia y el Ministerio Público, que podrían ser mecanismos de supervisión pública. Con esto podemos decir que no existe una institucionalidad independiente *per se*, ni tampoco los órganos generales de supervisión.

200 Honduras "Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional", artículo 4.

3.9. Integridad de las comunicaciones y sistemas

Integridad de las Comunicaciones y Sistemas: No debe obligarse a proveedores de servicios o desarrolladores de "hardware" o "software" a desarrollar capacidades de vigilancia que comprometan la seguridad de las comunicaciones y los dispositivos. No debe exigirse la retención indiscriminada y masiva de datos de las personas que usan dichos servicios ni debe comprometerse el derecho a la expresión anónima a través del establecimiento de obligaciones de identificación o prohibiciones respecto del uso de herramientas de cifrado y otras para proteger la identidad y la seguridad de las personas, sus comunicaciones y sus dispositivos.

El principio de **integridad de las comunicaciones y sistemas** no se cumple en la legislación hondureña, pues la Ley de Intervención de las Comunicaciones en su artículo 38 establece que

> las empresas y las instituciones que brindan los servicios de comunicación o cualquier otro ente natural o jurídico que se dedique a este tipo de actividad comercial, están obligados a proporcionar al órgano jurisdiccional competente, a UIC y al Ministerio Público o por la Procuraduría General de la República en su caso, todas las facilidades materiales, técnicas y humanas para que las intervenciones sean efectivas, seguras y confidenciales. En ese sentido están en la obligación de adaptar a su sistema los aparatos técnicos y recursos humanos necesarios para la captación y derivación y que se requieran para realizar la intervención de las comunicaciones, indistintamente del tipo de comunicación a intervenir.[201]

Este principio también se refiere a que

> no debe comprometerse el derecho a la expresión anónima a través del establecimiento de obligaciones de identificación o prohibiciones respecto del uso de herramientas de cifrado y otras para proteger la identidad y la seguridad de las personas, sus comunicaciones y sus dispositivos. [202]

Esta parte del estándar internacional tampoco se cumple en las normas hondureñas, pues se obliga a las empresas a

> llevar un registro completo de todos sus clientes" de manera permanente y se les "prohíbe y es constitutivo de sanción conforme a la normativa de multas que opera la Comisión Nacional de Telecomunicaciones (CONATEL), realizar transacciones sin haber efectuado la identificación del cliente"; por otra parte "los proveedores y usuarios de Internet que tengan asignadas Ips (*Protocolo de Internet*) públicas de las cuales derivan IPs privadas, deberán instalar en su negocio un sistema de cámaras que permita identificar en fecha y hora los clientes que hacen uso del servicio, debiendo llevar en sus sistemas un registro de la información por lo menos de los últimos treinta (30) días.[203]

201 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 38.
202 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 38.
203 Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas", artículo 37,

También la Ley de Intervención de las Comunicaciones viola el estándar al "exigirse la retención indiscriminada y masiva de datos de las personas que usan dichos servicios". El artículo 39 de la ley obliga a las empresas que brindan servicios de telefonía a

> guardar los datos de todas las conexiones de cada usuario por el plazo de cinco (5) años. Los datos incluyen los números de teléfono que participan en cada conversación, su duración y la hora de la llamada. En el caso de llamadas con teléfono móvil, deberá guardarse el lugar donde se encuentra un usuario cuando hace la llamada, contesta, o envía un mensaje de texto.

3.10. Garantías para la cooperación internacional

En lo referente a las **garantías para la cooperación internacional,** Honduras cuenta con tratados de asistencia judicial con todos los países centroamericanos, con México y Brasil.

Si para llevar a cabo las medidas de vigilancia es necesaria la cooperación internacional, esta debe llevarse a cabo a través de acuerdos de asistencia judicial recíproca (MLAT en inglés) en los que debe garantizarse que los mismos no sean utilizados para burlar las restricciones internas relacionadas con la vigilancia de las comunicaciones.

Honduras se adhirió a la Convención Interamericana sobre Asistencia Mutua en Materia Penal (MLAT en inglés) en el 2006.[204] El artículo segundo de la Convención es la única disposición de este tratado aplicable a materia de vigilancia. El artículo indica que los Estados partes se prestarán asistencia mutua en investigaciones, juicios y actuaciones en materia penal referentes a delitos cuyo conocimiento sea de competencia del Estado requirente al momento de solicitarse la asistencia. El articulo segundo explica que la Convención se aplica únicamente a la prestación de asistencia mutua entre los Estados partes, y por ende sus disposiciones no otorgan derecho a los particulares para obtener o excluir pruebas, o para impedir la ejecución de cualquier solicitud de asistencia.

3.11. Garantías contra el acceso ilegítimo y recurso efectivo

Garantías contra el Acceso Ilegítimo y Recurso Efectivo: La vigilancia ilegal de comunicaciones por parte de actores públicos o privados debe ser castigada mediante sanciones civiles y penales suficientes y adecuadas. Los denunciantes de información de interés público (*whistleblowers* en inglés) deben ser protegidos por la ley de cualquier repercusión legal por el incumplimiento de su deber de secrecía.

204 OEA. *Convención Interamericana Sobre Asistencia Mutua en Materia Penal*. (1992), http://www.oas.org/juridico/english/treaties/a-55.html [consultado: 22 julio, 2015]

Finalmente, nuestro sistema penal sí contempla **salvaguardas contra el acceso ilegítimo** por parte de actores públicos o particulares. El Código Penal establece el delito de interceptación ilegal de las comunicaciones con una pena hasta de 8 años si se trata de un particular y hasta de 12 años si se trata de un funcionario público.[205]

Sin embargo, la normativa hondureña no cumple con una parte de este principio, el referido a que "los denunciantes de información de interés público (*whistleblowers*) deben ser protegidos por la ley de cualquier repercusión legal por el incumplimiento de su deber de secrecía", esto si lo relacionamos con las vigilancias, la Ley de Intervención de las Comunicaciones establece el delito de infidencia con una pena de hasta 9 años de reclusión.[206] Asimismo, se estableció el delito de "divulgación de la información" con una pena de hasta 8 años de reclusión.[207]

205 Honduras "Código Penal", artículo 2014.

206 Artículo 51: Delito de Infidencia. Se prohíbe a las empresas e instituciones que brindan servicios de comunicación por tecnología o cualquier otro ente natural o jurídico que se dedique a esa actividad, a sus funcionarios, empleados, directores, propietarios, representantes legales, informar al suscriptor del servicio, sospechosos o imputado que sus comunicaciones o medios están siendo intervenidos. Quienes incumplan lo establecido en este artículo incurrirán en el delito de infidencia y serán sancionados con seis (6) a nueve (9) años de reclusión y una multa equivalente de sesenta (60) a ciento veinte (120) salarios mínimos. Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas."

207 Artículo 48: Delito de Divulgación de Información o Utilización de Información. Se castigará, con reclusión de seis (6) a diez (10) años de reclusión al funcionario judicial, policial, del Ministerio Público o Procuraduría General de la República en su caso, o de la empresa generadora de la información, que la divulgue o utilice cuando sea mediante la intervención de comunicaciones, con un propósito diferente del establecido en el ordenamiento jurídico. Honduras "Ley Especial Sobre la Intervención de las Comunicaciones Privadas."

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

El objetivo de este capítulo es presentar 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 Honduras, que surgieron de entrevistas a profundidad y de un grupo focal realizados con personas defensoras de derechos humanos y con técnicas y técnicos en telecomunicaciones e informática comprometidos con la defensa de los derechos humanos.

El presente se subdivide de la siguiente manera: una reseña sobre los aspectos metodológicos utilizados para luego dar paso a las experiencias tanto de defensores y defensoras y técnicos y técnicas relacionadas con vigilancia, anonimato, cifrado, allanamientos y requisas, entre otros. Finalmente, cierra con un sub-acápite que contiene las principales dudas manifestadas por las y los entrevistados sobre el marco legal existente en el país con respecto al anonimato, cifrado, allanamientos, requisas y cualquier otro tipo de legislación relacionada con vigilancia de las telecomunicaciones y/o que pudiera estar encaminado a criminalizar la labor de personas defensoras y técnicas.

4.1. Reseña metodológica

La metodología utilizada fue de carácter cualitativo, a través de herramientas como la entrevista a profundidad, de tipo semi-estructurado, con el objetivo de obtener las percepciones, experiencias y dudas u observaciones sobre el marco legal de defensoras y defensores de derechos humanos, así como de técnicos y técnicas involucrados en la defensa de derechos humanos o que trabajen para organizaciones y/o personas defensoras de derechos humanos en Honduras.

En tal sentido, se realizaron seis entrevistas a personas defensoras de derechos humanos (tres mujeres y tres hombres), vinculadas a distintas áreas de defensa de los derechos humanos: libertad de expresión, defensa de los territorios, derechos de la mujer, privados/as de libertad y prevención de tortura, acompañamiento a defensores/as. Se realizaron dos entrevistas a técnicos, ambos hombres, siendo importante mencionar que se tuvo cierto nivel de dificultad para encontrar el perfil adecuado de las y los técnicos, pues no solo se buscaba su conocimiento y capacidad técnica en las áreas de telecomunicaciones e internet, sino también su compromiso por la defensa de derechos humanos

y/o trabajo con organizaciones defensoras de derechos humanos. No se pudo realizar el grupo focal por cuestiones de seguridad.

La información de este capítulo fue brindada por defensores y defensoras de derechos humanos, quienes se han opuesto públicamente a la vigilancia en las comunicaciones, por lo que los convierte en actores válidos para hablar sobre sus experiencias en cuanto a vigilancia y criminalización por medio de internet y las telecomunicaciones. Por el tipo de metodología utilizada no podemos hacer generalizaciones a partir de sus respuestas, sino más bien plantearlas como experiencias, dudas y percepciones que viven de primera mano las personas en el ejercicio de la defensa de derechos humanos en el país.

4.2. Experiencias (hallazgos y casos paradigmáticos)

4.2.1. Vigilancia

Todas las personas entrevistadas coinciden en que 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. Las y los entrevistados mencionaron con bastante frecuencia algunos elementos que les sirven para sospechar que están siendo o han sido intervenidos telefónicamente, entre los cuales destacan: el eco que se escucha durante sus llamadas telefónicas; las llamadas son cortadas cuando se usan ciertas palabras o términos; se escuchan otras voces durante las llamadas. Por otra parte, también manifiestan haber tenido experiencias como *hackeos* de sus cuentas de correo y redes sociales, así como clonación de las páginas web institucionales a través del envío de solicitudes masivas.

Entre los entes que los y las entrevistadas identifican como las posibles entidades vigilantes se mencionan a la Dirección de Inteligencia a través de la Unidad de Intervención de las Comunicaciones, los departamentos de investigación de la Policía y las empresas telefónicas.

El técnico con más experiencia nos manifestó la situación de la vigilancia en Honduras a partir de sus investigaciones.

Primero se refirió al software de infiltración: “he visto troyanos que clonan la información. Otro comportamiento extraño pero que no se ha comprobado que sea el denominado ataque conocido como día cero, en dos máquinas que clonaban las conexiones de internet”.[208] Luego habló del hardware de interceptación:

> Hay tres tipos de ataques, los más comunes son **el escaneo de puertos**, que es la antesala de la infiltración. Los ejecutan los proveedores de internet directamente. He tenido

208 Técnico No. 1, entrevistado en fecha 29 de julio de 2015, Tegucigalpa. (Destacado del autor.)

> experiencias donde he montado cortafuegos, y han llamado de la empresa proveedora preguntando que qué se había conectado a la red, que ya no podían ver lo que antes podían ver. [209]

Según este técnico, el escaneo de puertos implica que "las computadoras se comunican en base a puertas, por ejemplo Skype tiene una puerta y llega a otra computadora", este ataque es "permanente en el país", con una finalidad de "mantener un inventario de lo que existe en la organización, o equipos, o previo a otros ataques". Otro de los ataques es el *net fishing***,** el cual es "una combinación de varias técnicas, capturar información de las personas en internet [pesca con red], para obtener fechas de nacimiento, correos electrónicos, generalmente para fraudes", con una finalidad de "lucro" y se da de manera "permanente" en Honduras.

Por otra parte el Técnico número 1 manifestó que están los **ataques de denegación de servicios (Ddos),** que "han sido públicos, hacia el Estado y en esos momentos también se han atacado organizaciones de derechos humanos, se ha producido en momentos puntuales durante los meses de (marzo, mayo, septiembre de todos los años)". Otro ataque mencionado por este Técnico No. 1, es la **usurpación de identidad** "se usan los elementos ya existentes en la red y hacer creer que corresponden a la persona que se quiere usurpar. Sirve para difamar, se ha dado en momentos de alto conflicto con organizaciones de derechos territoriales". Por último, el *defasing*, el cual consiste en "tomar el sitio web de un organización, entran a él y cambian las imágenes o dejan mensajes amenazantes", de este "no hay un patrón de comportamiento, es aleatorio"[210]

4.2.2. Anonimato y cifrado

Respecto de estos dos temas, las y los entrevistados hicieron poca referencia pero manifestaron la necesidad del uso de cifrado para poder enfrentar según ellos la grave situación de vigilancia en el país. Manifestaron también que es difícil mantener el anonimato en las telecomunicaciones, pero que existen herramientas para poder minimizar el riesgo. Evidenciaron también que han recibido capacitaciones en estos temas, pero que a veces no hay disciplina en el uso. A continuación se citan dos entrevistas relacionas con estos temas: "Nosotras, nos migramos a Linux, de allí usar herramientas de seguridad como los candados para claves y el uso de kee pass, es una política de la organización. La información la guardamos en TrueCript "[211]. "El resto del equipo, todavía maneja correos normales. Para pocos temas se maneja correos con seguridad".[212]

209 Técnico No. 1, entrevistado en fecha 29 de julio de 2015, Tegucigalpa.
210 Técnico No. 1, entrevistado en fecha 29 de julio de 2015, Tegucigalpa.
211 Defensora No. 1, entrevistada en fecha 03 de agosto de 2015, Tegucigalpa.
212 Periodista No.1, Técnico No. 1, entrevistado en fecha 20 de julio de 2015, Tegucigalpa.

4.2.3. Allanamientos y requisas

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.

4.2.4 Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en Internet y en las telecomunicaciones

Las y los entrevistados manifestaron que ellos y sus conocidos fueron objeto de robos de dispositivos que contenían información y que luego la información fue utilizada para criminalizarlos.

Asimismo, que tenían conocimiento de que la vigilancia se agudizaba en momentos cercanos a las votaciones populares, en discusiones de leyes importantes y en momentos de protestas, contra políticos de oposición y defensores y defensoras de derechos humanos.

Por otra parte, algunos entrevistados y entrevistadas mencionaron que los hackeos a sus cuentas de correo o de redes sociales se han hecho en momentos de visibilidad en la defensa de los derechos humanos.

4.3. Inquietudes

4.3.1 Vigilancia

Las y los entrevistados manifestaron que tienen plena conciencia de la vigilancia en las telecomunicaciones y su preocupación por esta situación, y sobre todo por ser ejercida por el órgano de inteligencia del país. Uno de los entrevistados manifestó que este tipo de medidas tienenrelación con el “control político de la población, la generación de terror y tortura psicológica”. Otra de las entrevistadas se refirió a que, aunque existe la conciencia de una vigilancia fuerte, muchas personas asumen el riesgo de ser vigiladas por difundir información, pero que está el temor latente de ser criminalizados.

La mayoría de las y los entrevistados manifestaron que la ley es demasiado ambigua y abierta; por otra parte, que aunque existe un procedimiento formal para poder intervenir las comunicaciones, en el país actualmente no hay independencia judicial para poder garantizar un efectivo control judicial de las solicitudes de intervención y con ello la protección del derecho a la privacidad.

4.3.2. Anonimato y cifrado

Sobre anonimato y cifrado surgieron dudas generales sobre su regulación y si es prohibido o permitido su uso.

> A mí en el aeropuerto me dijeron que encendiera la computadora. Yo para encenderla, lo primero que salen son que necesito las claves. El militar estaba necio que quería ver el contenido de mi computadora. Mi inquietud es ¿si están facultados para hacer eso? ¿Qué pasaría si nosotros promovemos en los talleres de seguridad digital la encriptación, para hacer llamadas seguras, qué pasa si nos denuncian?[213]

Los técnicos manifestaron su preocupación por la criminalización que pueda generarse desde el Estado por "cifrar e intercambiar información cifrada" y por la "facilitación de conocimientos con el fundamento de que se atenta contra la seguridad del Estado".

4.3.3. Allanamientos y requisas

Las dudas sobre allanamientos y requisas estuvieron principalmente relacionadas con qué información pueden quitar o pedir las autoridades, y qué normas pueden utilizarse para que no les despojen de información de manera arbitraria.

4.3.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones

Los técnicos manifestaron que les preocupaba la interpretación que puedan hacer las y los fiscales y los jueces de algunos tipos penales establecidos en la Ley de Intervención de las Comunicaciones y la Ley de Financiamiento del Terrorismo, ley que penaliza a las personas que presten cualquier colaboración material o conocimientos que faciliten la comisión de los delitos de terrorismo[214]. Esto se agrava pues además se puede sancionar como facilitación del terrorismo aun cuando el delito de terrorismo no se cometa.

Por otra parte, manifestaron preocupación por la retención de datos en las empresas de telefonía e internet y que no hay protocolos para la destrucción de los mismos una vez cumplido el plazo.

213 Defensora No. 1, entrevistada en fecha 03 de agosto de 2015, Tegucigalpa.

214 Hay una tendencia en el país a acusar de terroristas a personas del movimiento social que participan en manifestaciones públicas.

5. Conclusiones nacionales

1. El tema del derecho a la privacidad relacionado con la privacidad digital ha sido muy poco tratado en el país, de igual manera que el tema de las vigilancias en el internet y en las telecomunicaciones. Ha sido hasta el mes de octubre y noviembre que se puesto en discusión porque se filtraron a los medios de comunicación unas conversaciones entre le presidente de la Sala de lo Constitucional y el vicepresidente del Consejo de la Judicatura, y que se ha manejado diatónicamente que están relacionadas con supuestos actos de corrupción y tráfico de influencias; a partir de ese momento es que han salido varios sectores no relacionados a la defensa de los derechos humanos (este sector ha denunciado la vigilancias desde el golpe de Estado de 2009), que han manifestado que las vigilancias en el país se están efectuando de manera ilegal.

2. La brecha digital es menor en el acceso a telefonía, así como el uso del internet a través de celulares, esto es importante en cuanto al derecho a la comunicación, pero también es un terreno fértil para las vigilancias, sobre todo a partir que el Estado eliminó el derecho al anonimato mediante la exigencia de que las personas que usan telefonía celular estén registradas y estos datos llegan al organismo de inteligencia que también se ocupa de las vigilancias.

3. En Honduras la criminalización de defensores y defensoras de derechos humanos por parte del Estado continua siendo un grave problema, ya sea a través del sistema de persecución penal con el uso de figuras delictivas que en otros momentos no se utilizaban, como las figuras de daños a la propiedad, las calumnias, injurias y difamación. Asimismo, la estigmatización por su labor y amenazas por parte del Estado. Por otra lado, la criminalización hacia personas defensoras y otras relacionadas con la política mediante las vigilancias en internet y las telecomunicaciones se han hecho notorias después del golpe de Estado y agravadas en las cercanías a las elecciones de 2012 y 2013. Resulta preocupante las publicaciones mencionadas en esta investigación, que refieren a Honduras como un consumidor de servicios de espionaje y como centro de espionaje mundial.

4. La vigilancia en internet y en las telecomunicaciones en Honduras forma parte de una política en materia de seguridad pública mediante la cual fueron fusionados temas relativos a seguridad, defensa e inteligencia, y que se ha venido implementando con el postulado de que, para lograr una sociedad segura, es necesario crear las herramientas jurídicas e institucionales para el combate a la violencia y la delincuencia organizada, donde quien no está a favor de la medidas restrictivas, está a favor de la “delincuencia”; en otras palabras, se plantea una falsa disyuntiva entre libertades fundamentales y seguridad.

5. El 05 de diciembre de 2011 se estableció un estado de excepción en seguridad por motivos de violencia, a través del decreto ejecutivo número PCM-075-2011, esto dio paso a una reorganización legal e institucional del Estado en materia de seguridad, defensa e inteligencia, entre lo cual se incluyó la aprobación de la Ley Especial de Intervención a las Comunicaciones Privadas el 26 de enero de 2012 y la creación de la Unidad de Intervención de las Comunicaciones.

6. La fusión de los conceptos seguridad, defensa e inteligencia llevó además a amalgamar a los entes encargados del sistema de justicia, de persecución penal, defensa e inteligencia, con lo cual se ha ido eliminando el equilibrio de poderes, los contrapesos jurídicos, los mecanismos de contradicción necesarios para valorar la necesidad de la restricción al derecho, con lo cual en este momento no se cuenta con una supervisión pública independiente, entre otras cosas, de las vigilancias en internet y las telecomunicaciones, que redunda tanto en la violación al derecho al debido proceso como en la restricción ilegítima del derecho a la privacidad.

7. 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 por meras sospechas con lo cual se viola el principio internacional de objetivo legítimo; 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.

8. La vigilancia en internet y en las telecomunicaciones es realizada por el Estado a través del sistema de inteligencia y mediante la utilización de las empresas de telefonía e internet.

9. En la legislación hondureña existe normativa idónea sobre el derecho de acceso a la información pública a través de la Ley de Transparencia y Acceso a la Información Pública y por otra parte normas que establecen un sistema paralelo de secretividad demasiado amplio a través de la Ley de Secretos Oficiales en Materia de Defensa y Seguridad, que prácticamente establece la inaplicabilidad de las normas sobre transparencia y acceso a la información pública. Todo esto permite la no rendición de cuentas por parte del vigilante. No sabemos cuántas personas están

siendo vigiladas en el país, tampoco si las vigilancias están relacionadas con la persecución de delitos de criminalidad organizada; lo que sí sabemos es que existen varias denuncias de opositores y opositoras políticos y defensores y defensoras de derechos humanos que creen que están siendo vigilados arbitrariamente por el Estado.

10. Las personas que fueron entrevistadas, tanto técnicas como defensoras, manifestaron que les preocupa la ambigüedad y apertura de las normas para autorizar las vigilancias, así como la ambigüedad de normas sancionatorias que pueden ser utilizadas en cualquier momento para criminalizar a las personas que prestan su colaboración técnica en anonimato y cifrado de las comunicaciones.

11. Unas cuantas normas relacionadas con el derecho a la privacidad son disposiciones de protección, la mayoría permiten la restricción contra constitucional y contra convencional. Ni la Constitución de la República ni las leyes secundarias han incluido aún el derecho a la privacidad digital en internet y en las telecomunicaciones, sin embargo sí se ha desarrollado a través de la jurisprudencia en casos penales.

Bibliografía

Libros

Basterra I., Marcela. *Protección de Datos Personales.* México: Universidad Nacional Autónoma de México, UNAM, 2008.

Comisión Interamericana de Derechos Humanos. *Observaciones Preliminares sobre la situación de los derechos humanos en Honduras*. Washington, D.C.: CIDH, 2014. https://www.oas.org/es/cidh/prensa/comunicados/2014/146A.asp (consultado: 14 junio, 2015)

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

Comisión Nacional de Telecomunicaciones. *Desempeño del sector telecomunicaciones. Informe Trimestral, cuarto trimestre 2014.* Tegucigalpa, M.D.C.: CONATEL, 2015. http://www.conatel.gob.hn/doc/indicadores/2015/Desempe%C3%B1o_del_Sector_De_Telecomunicaciones_4to_Trimestre_2014.pdf (consultado: 12 julio, 2015)

Comité por la Libre Expresión. *Informe Libertad de expresión 2013.* Tegucigalpa, M.D.C.: C LIBRE, 2013. http://www.clibrehonduras.com/content/informe-libertad-de-expresi%C3%B3n-2013 (consultado: 4 de noviembre, 2015)

Hernández Alcerro, Jorge Ramón. *Comentarios a la Constitución de la República de Honduras de 1982 (Los Tratados en la Constitución).* Tegucigalpa: Editorial Universitaria, 1982.

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, David Kaye, Resolución A/HRC/29/32 del 22 de mayo de 2015.* Ginebra: Naciones Unidas, 2015. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc (consultado: 4 de noviembre, 2015)

Naciones Unidas. Consejo de Derechos Humanos. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue, resolución A/HRC/23/40, 17 de abril de 2013.* Ginebra: Naciones Unidas, 2013. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40 (consultado: 4 de noviembre, 2015)

Naciones Unidas. Consejo de Derechos Humanos. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, resolución A/HRC/17/27, 16 de mayo de 2011.* Ginebra: Naciones Unidas, 2011. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G11/132/04/PDF/G1113204.pdf?OpenElement (consultado: 4 de noviembre, 2015)

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.* Ginebra: Naciones Unidas, 2015. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc (consultado: 4 de noviembre, 2015)

Naciones Unidas. Asamblea General, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. *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.* New York: Naciones Unidas. Asamblea General, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2015. www.ohchr.org/EN/HRBodies/HRC/.../Session27/.../A-HRC-27-37_sp.do (consultado: 4 de noviembre, 2015)

Mata Tobar, Víctor Hugo. *La aplicabilidad del derecho internacional de los derechos humanos en el orden jurídico de los Estados de Centroamérica.* San José, Costa Rica: CODEHUCA, 1998.

Mejía, Joaquín. *Honduras y los sistemas internacionales de protección de derechos humanos.* Tegucigalpa, Honduras: Editorial Casa San Ignacio, 2010.

Mejía, Joaquín. *Una mirada a la Justicia Constitucional hondureña, desde la óptica de los Derechos Humanos.* Tegucigalpa, Honduras: Editorial Casa San Ignacio, 2012.

Organización de Estados Americanos. *Convención Interamericana sobre Asistencia Mutua en Materia Penal*. Washington, Organización de Estados Americanos, 1992. http://www.oas.org/juridico/english/treaties/a-55.html (consultado: 22 julio, 2015)

Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI). *Informe de la Encuesta latinoamericana de hábitos y prácticas culturales 2013.* Madrid: Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura, 2013. http://oei.es/xxivcie/encuestalatinoamericana2013.pdf (consultado: 17 mayo, 2015)

Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Necessary and Proportionate, s.f. https://es.necessaryandproportionate.org/text (consultado: el 15 de agosto de 2015)

Rodríguez, Katitza. *Anonimato y Cifrado: Comentarios enviados a la Relatoría Especial de la Comisión de Derechos Humanos sobre la promoción y protección del derecho a la libertad de opinión y de expresión*. San Francisco, EUA: Electronic Frotntier Foundation, 2015. https://www.eff.org/files/2015/03/18/anonimatoycifrado-eff-11.pdf (consultado: 20 octubre, 2015)

Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN). *Agenda Digital de Honduras, 2014-2018.* Tegucigalpa, M.D.C.: Secretaría Técnica de Planificación y Cooperación Externa de Honduras (SEPLAN), 2013.

Villagrán Kramer, Francisco. *Derecho de los tratados.* Guatemala: F&G Editores, 2002.

Tesis

Sierra Castro, Hedme. *"Aplicación de los derechos humanos a la intervención de las comunicaciones; Internet libre y comunicaciones seguras en la labor de promoción y defensa de los derechos humanos."* Tesis de maestría, Centro Internacional de Estudios Políticos, Universidad Nacional de San Martín. http://www.unsam.edu.ar/ciep/wp-content/uploads/2014/11/Hedme-Sierra-Castro.pdf (consultado: 4 de noviembre, 2015)

Legislación nacional

Honduras. "Anteproyecto "Ley de Protección de Datos Personales y Acción de Habeas Data de honduras". Instituto de Acceso a la Información Pública (2014).

Honduras. "Código Penal". Congreso Nacional (1985).

Honduras. "Código Procesal Penal". Congreso Nacional (2002).

Honduras. "Constitución de la República". Asamblea Nacional Constituyente (1982).

Honduras. "Ley de Alfabetización en Tecnologías de Información y Comunicación". Congreso Nacional (2013).

Honduras. "Ley de Compras Eficientes Transparentes a través de Medios Electrónicos". Congreso Nacional (2014).

Honduras. "Ley Contra el Financiamiento del Terrorismo". Congreso Nacional (2010).

Honduras. "Ley Especial del Consejo Nacional de Defensa y Seguridad". Congreso Nacional (2011).

Honduras. "Ley Especial Sobre la Intervención de las Comunicaciones Privadas". Congreso Nacional (2012).

Honduras. "Ley de Firmas Electrónicas". Congreso Nacional (2013).

Honduras. "Ley General de la Superintendencia para la Aplicación de Pruebas de Evaluación y de Confianza". Congreso Nacional (2014).

Honduras. "Ley de Inteligencia Nacional". Congreso Nacional (2013).

Honduras. "Ley Marco del Sector de Telecomunicaciones". Congreso Nacional (1995).

Honduras. "Ley Orgánica del Poder Legislativo". Congreso Nacional (2014).

Honduras. "Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional". Congreso Nacional (2014).

Honduras. “Ley de la Policía Militar del Orden Público”. Congreso Nacional (2013).

Honduras. “Ley de Portabilidad Numérica”. Congreso Nacional (2013).

Honduras. “Ley de Transparencia y Acceso a la Información Pública”. Congreso Nacional (2006).

Honduras. “Reforma a la Constitución de la República”. Congreso Nacional (2013).

Honduras. “Ley Sobre Justicia Constitucional”. Congreso Nacional (2004).

Reglamentos

Honduras. “Reglamento de la Ley Marco del Sector de Telecomunicaciones”. Secretaría de Estado en el Despacho de Gobernación y Justicia (2002).

Honduras “Reglamento del Servicio de Internet o Acceso a Redes Informáticas”. Comisión Nacional de Telecomunicaciones (CONATEL) (2011).

Honduras “Reglamento de la Ley de Transparencia y Acceso a la Información Pública”. Instituto de Acceso a la Información Pública (2007).

Decretos ejecutivos

Honduras. “Decreto Ejecutivo PCM- 053-2014”. Consejo de Ministros (2014).

Honduras. “Resolución CNDS-069-2014”. Consejo Nacional de Defensa y Seguridad (2014).

Jurisprudencia Interna

Sala de lo Constitucional. Corte Suprema de Justicia de Honduras. Recurso de Amparo número AA 406-13 del 28 de junio de 2013.

Sala de lo Penal. Corte Suprema de Justicia de Honduras. Sentencia número CP-48-2011, de fecha 11 de junio de 2013.

Sala de lo Penal. Corte Suprema de Justicia de Honduras. Sentencia número CP-303-2010, de fecha 11 de junio de 2013.

Páginas web

Comité por la Libre Expresión (C-LIBRE). “Informes anuales sobre Libertad de Expresión en Honduras”. Comité por la Libre Expresión. http://www.clibrehonduras.com/publicaciones (consultado: el 04 de mayo de 2015)

Comité de Familiares Desaparecidos de Honduras (COFADEH). http://www.cofadeh.hn/ (consultado: el 04 de mayo de 2015)

Noticias de Periódico

"Honduras: Gobierno paga L.8 millones en software de espionaje telefónico". *Conexihon, 6 de julio de 2015, bajo Sección Libertad de Expresión.* http://conexihon.hn/site/noticia/libertad-de-expresi%C3%B3n/honduras-gobierno-paga-l8-millones-en-software-de-espionaje-telef%C3%B3nico (consultado: el 15 de agosto de 2015)

lqVRomqgghOAGr2Ov9VxK/Eb

r79b8K3hVurUKZnLI8ag

RXlyjpbQioxwxvU1jeZpj86Z/sIDhll vy5WvrrskJ4A1dbQioxwx

CPRXlyjpbQioxwxvU1jeZpj86Z/sIDhll vy5

oxwxv**Nicaragua**//fs

sCPRXlyjpbQioxwxvU1jeZpj86Z/sIDhll vy5WvrrskJ4A1dbQiox

Mireya Zepeda Rivera

1. Antecedentes

1.1. Estado de la discusión nacional

La vigilancia, censura, sanción y control del derecho a la privacidad de defensores y defensoras de derechos humanos violenta cualquier orden constitucional y jurídico de un país. Las y los funcionarios públicos y quienes persiguen un fin económico optan por criminalizar, evadiendo el origen del conflicto. En un Estado de derecho y democrático, el ideal es desarrollar acciones y políticas para enfrentar los problemas sociales, sin embargo, actualmente se emprenden acciones de persecución, judicializacion y sanción penal, al convertir toda acción política en un delito. O bien, ante acciones efectivas de defensores y defensoras de derechos humanos, se crean respuestas más "intimidantes" tales como agresión, amenaza, o inclusive asesinato.

Para la elaboración del presente estado del arte y para alcanzar los objetivos de investigación, se procedió a recolectar la información mediante la indagación, identificación y análisis de fuentes bibliográficas en forma física, recurriendo a los marcos legales nacionales e internacionales que protegen el derecho a la privacidad o propician la criminalización, vigilancia y/o censura digital, en internet y en las telecomunicaciones, de defensoras y defensores de derechos humanos en Nicaragua.

También se consultaron los principales informes nacionales e internacionales relacionados a la libertad de expresión, libre movilización, libertad de prensa, prohibición de la censura, derecho a la privacidad y libre ejercicio de la profesión, así como dos tesis nacionales de la Universidad Centroamericana.

Posteriormente, se elaboraron fichas bibliográficas por cada documento consultado con el fin de facilitar la clasificación y el análisis de los datos recolectados; se designaron descriptores que facilitaron la búsqueda de información entre los documentos que se tuvieron acceso, entre los que figuran: privacidad, seguridad de la información, seguridad informática, seguridad de la comunicación, encriptación, allanamiento, ciberseguridad, seguridad digital, telecomunicación, tecnologías de información y comunicación, criminalización, defensor/a de derechos humanos. Finalmente, con la información recogida se procedió a elaborar el presente estado de arte.

Las dos tesis monográficas a nivel nacional abordan la importancia del recurso de *habeas data* como mecanismo de protección, actualización y rectificación de información personal almacenada en ficheros de cualquier tipo, incluyendo los digitales.

Tabla 1 – Tesis nacionales

Nombre de la tesis	Año	Universidad	Autor/a/es
Los ataques de la informática y la protección de datos personales en Nicaragua	2005	Universidad Centroamericana	Jovanka Ñancahuazú Durón Chow,
El Habeas Data como Mecanismo de defensa de los Derechos Humanos	2010	Universidad Centroamericana	Adriana María Obando Quezada

1.1.1. Protección de datos personales y habeas data

Las y los ciudadanos proporcionamos diariamente mucha información personal sin saber para qué será utilizada y sin creer que esto pueda afectarnos. En Nicaragua, a raíz del Caso Infornet 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 Personales[2], la 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.[3]

Posteriormente, y para garantizar el resguardo y protección de los datos personales, en el año 2013 se reforma la Ley de Amparo[4] 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.[5]

2 Nicaragua "Ley de Protección de Datos Personales" La Gaceta No. 61 (2012).
3 Nicaragua "Ley de protección de datos personales", artículo 1.
4 Nicaragua "Ley de Amparo"La Gaceta No (08, abril 2013).
5 Nicaragua "Ley de Amparo" artículo 6.

El recurso de *habeas data* hace referencia al derecho legítimo del individuo a "la libre disposición de los datos personales"[6]. 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 informativa[7] (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).

Para el autor Alberto Cerda Silva, el consentimiento en el tratamiento de datos personales es un tema de análisis, debido a que ello implica visualizar el riesgo de los datos en manos de prestadores de servicio en línea, la apropiada extensión del concepto dato personal, el consentir como legitimación para el tratamiento de datos y la protección de los datos personales como derecho autónomo.[8]

1.1.2. La autodeterminación informativa

El derecho de autodeterminación informativa es el derecho al control personal de la información que circula sobre el propio individuo[9]. El ejercicio de dicho derecho se encuentra limitado en la esfera digital, debido a que nunca se llega a conocer de groso modo la cantidad de información personal que circula en la red. Además, para Alberto Cerda, la rectificación y retiro de información personal depende tanto de la *"*...plataforma web a la que se ha subido dicha información [...], como del país en el que está alojada la empresa que proporciona el servicio"[10]. En ese sentido, el recurso de *habeas data*, se podrá o no ejercer dependiendo del límite de cada jurisdicción nacional.

De acuerdo a la jurisdicción, para el caso de Nicaragua, el recurso de *habeas data* sirve como mecanismo jurisdiccional de protección de los derechos a la autodeterminación informativa, por lo que se recurrirá a dicho recurso para la protección de datos personales asentados en archivos,

6 Osvalo Alfredo Gozaíni, "Hábeas Data. Protección de los datos personales. Doctrina y Jurisprudencia". (Argentina: Rubinzal Culzoni Editores, 2011), 67.

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

8 Alberto J, Cerda Silva. "Protección de datos personales y prestación de servicios en línea en América Latina" en "Hacia una internet libre de censura: propuestas para América Latina". Coord. Eduardo Andrés Bertoni (Buenos Aires: Universidad de Palermo - UP, 2012), 165-180,

9 Lorena Cano Orón. "La privacidad en el escenario digital. Análisis de la política de la Unión Europea para la protección de datos de la ciudadanía". (Bellaterra: Universidad Autónoma de Barcelona, 2014), 57,

10 Alberto J, Cerda Silva. "Protección de datos personales y prestación de servicios en línea en América Latina" en "Hacia una internet libre de censura: propuestas para América Latina". (Buenos Aires: Universidad de Palermo - UP, 2012), 170.

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[11].

En este sentido, la tesis de Adriana Obando explica cómo el *habeas data* proporciona un mecanismo de resguardo para la protección de los datos personales, que también está implícito en la Ley No 621:

La legitimación para ejercer la acción de protección de datos personales o Habeas Data puede ser activa o pasiva, es activa cuando la acción es interpuesta por el afectado, sus tutores y sucesores, por si o por medio de apoderado y cuando sea interpuesta por personas jurídicas se tiene que realizar por medio de sus representantes legales o apoderados. La legitimación es pasiva cuando la acción es ejercida por los responsables y usuarios de ficheros de datos públicos y privados.[12]

Los argumentos implícitos para la defensa son los mencionados, en este sentido la ley explicita que podemos obtener esta información pero también menciona que no se puede utilizar sin previo aviso.

1.1.3. Documentos e informes

Por otro lado, se indagaron otras fuentes de información que aportan al análisis y que, a pesar de ser un tema con poco abordaje a nivel nacional, es complementado por medio de estudios internacionales que permiten dar un enfoque comparado.

Tabla 2 – Informes nacionales

Nombre de la obra	Año	Autor/a/es
El derecho a la vida privada en la Constitución de Nicaragua	1999	María Asunción Moreno Castillo
La intervención de las comunicaciones telefónicas y la interceptación de las comunicaciones escritas, telegráficas y electrónicas como medios de prueba en el nuevo proceso penal	2012	María Asunción Moreno Castillo
Estado de la Libertad de Expresión en Nicaragua 2013-2014	2014	Guillermo Rothschuh Villanueva
Las telecomunicaciones y el ente regulador	2010	Guillermo Rothschuh Villanueva

11 Nicaragua "Ley de Amparo", artículo 6.

12 Adriana Obando Quezada, "El Habeas Data como mecanismo de Defensa de los Derechos Humanos". (tesis de Licenciatura, Universidad Centroamérica, 2010), 92.

Informe sobre el estado de la libertad de expresión en Nicaragua conforme al artículo 13 de la Convención Americana sobre Derechos Humanos.	2003	Sofía Montenegro
Novena reforma constitucional. El cambio de las reglas del juego democrático en Nicaragua.	2014	Alejandro Aguilar, Adelmo Sandino, Mireya Zepeda, Ada Esperanza Silva.

Fuente: Elaboración Propia

El derecho universal a la privacidad, incorporado en las normas internacionales de derechos humanos, cada vez está mas relacionado a la seguridad digital; en este sentido, el propio significado de "derecho a la privacidad" tiene diferencias. Por un lado, aquel relacionado con la prohibición de que una persona sea objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, así como de ataques a su honra o a su reputación, contando con la protección de la ley contra tales injerencias o ataques[13]. Por otro lado, encontramos el significado de derecho a la privacidad que es considerado como un derecho no absoluto, puesto que involucra otros derechos fundamentales como la libertad de expresión, de opinión, asociación, intimidad. En ese sentido, es necesario cuestionarse ¿Qué entendemos por derecho a la privacidad digital, en internet y en las telecomunicaciones? ¿Cuál es la importancia de analizar el derecho a la privacidad digital desde un contexto de vigilancia de interceptación de las comunicaciones digitales? ¿Cómo se relaciona el derecho a la privacidad digital con el ejercicio de defensa de los derechos humanos de los defensores y defensoras de derechos humanos en Nicaragua?

En Nicaragua, el derecho a la vida privada está reconocido en el *artículo* 26 de la Constitución Política, ello aplica no solo para los y las ciudadanas nicaragüenses sino también para las personas extranjeras, pues se trata de un derecho estrictamente vinculado a la propia persona. El mismo artículo constitucional, inciso 2, establece que el respeto a la vida privada no abarca únicamente la sustracción de determinados datos, sino también el que las comunicaciones no sean interceptadas, lo que evidencia que el derecho a la privacidad es extensivo al derecho a la privacidad digital.

Por lo tanto, podemos decir que la privacidad digital como un derecho abarca el ámbito de protección a los derechos del honor y la intimidad también recogidos en la Constitución Política, por lo tanto debe dársele la atención debida. En cuanto al derecho al honor, este está recogido y protegido por las normas penales estableciendo los delitos de difamación o injurias para casos que hagan referencias a personas naturales.

13 Asamblea General de las Naciones Unidas. "Declaración Universal de los Derechos Humanos". (París: Naciones Unidas, 1948), artículo 12.

El concepto de intimidad se ha definido de varias formas. Desde ese derecho a "ser dejados solos" hasta el más actual enfoque que insiste en definir el derecho a la intimidad como control de informaciones[14]. Para el autor Alfonso Parejo[15], el derecho a la intimidad se presenta como el derecho de una persona a reservar un ámbito de su vida como secreto e intangible, así como a ostentar la capacidad y los medios para evitar la manipulación de su intimidad por parte de otras personas. Dicha posición facilita la extensión de la protección de la intimidad a los datos que se encuentren en archivos o registros no automatizados, así como a cualquier otro tipo de tecnología que permita recoger, almacenar y resguardar la información de las personas.

El *artículo* 26 constitucional no establece la posibilidad de una limitación del derecho por vía judicial. Sin embargo, establece restricciones respecto a la inviolabilidad del domicilio y la apertura de la correspondencia extraída ilegalmente.[16]

Según Moreno, las limitaciones del derecho a la privacidad operan como excepciones a las facultades de exclusión y al control que el titular del derecho ostenta *erga homnes*. Por consiguiente, tanto los limites voluntarios, los cuales consisten en consentir, como los que provienen del interés público, constituyen causas de justificación legitimadoras de las intromisiones en el ámbito íntimo y privado de las personas.[17] Es decir, nadie debe ni puede hacer uso de información que es parte de la vida privada, puesto que la norma que esté vigente ha sido aceptada.

1.2. Brecha digital

Nicaragua es el país más extenso de América Central con una superficie de 130.373,47 km2, constituida por una proyección hasta el 2013 de 6,035,748.2 habitantes[18], de los cuales el 50,4 % son mujeres y el 54 % tiene menos de 30 años de edad. El 57 % vive en zonas urbanas y el 43 % en el área rural. Está dividido en quince departamentos, dos regiones autónomas de la Costa Caribe y 154 municipios. El desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) ha traído consigo cambios estructurales en todos los ámbitos: económico, laboral, social, educativo, y hasta en el manejo de las relaciones interpersonales. En Nicaragua, existen ciertas particularidades que deben ser tomadas en cuenta cuando se habla de las TIC y una de ellas es la brecha digital existente. La coexistencia de la pobreza, la marginalidad y la desigualdad en medio de la abundancia incrementa las desigualdades, dificultando el que este parte de la ciudadanía nicaragüense se beneficie del uso de herramientas tecnológicas.

14 María Moreno Castillo. "El derecho a la vida privada en la Constitución de Nicaragua". *Revista Encuentro*, 30(49), 1999, 25.
15 Alfonso Parejo. "El derecho fundamental a la intimidad y sus restricciones". (Madrid: Cuaderno de Derecho Judicial No. XXII, 1996), 300.
16 Nicaragua "Ley de reforma parcial a la Constitución Política de Nicaragua" La Gaceta No. 26 (2014), artículo 26, Inc. 4.
17 María Moreno Castillo. "El derecho a la vida privada en la Constitución de Nicaragua", 29.
18 Instituto Nicaragüense de Telecomunicaciones y Correos. Estadísticas del sector de las telecomunicaciones de Nicaragua. (Nicaragua, TELCOR, 2014).

Para el Sistema de Información de Tendencias Educativas en América Latina (SITEAL)[19], la brecha digital no es más que la distancia en términos de la posible inclusión social de aquel conjunto de personas que accede a internet con cierta asiduidad y por lo tanto conoce su funcionamiento, respecto de aquella parte de la población que no tiene acceso a este recurso. La brecha digital en Nicaragua depende de dos factores. En primer lugar, las disparidades en servicios y en el grado de desarrollo económico son grandes entre las zonas urbanas y las rurales y, en segundo lugar, las y los trabajadores no calificados son los más numerosos y los que quedan más rezagados para la utilización de las TIC.

En torno a las estadísticas del sector de las telecomunicaciones de Nicaragua, es importante resaltar la disponibilidad y relativa actualización de las mismas. Entre los años 2011 y 2013 la cantidad de teléfonos móviles o celulares en Nicaragua aumentó de 4.8 a 6.8 millones de usuarios, es decir, creció un 42 % lo que equivaldría a decir que al menos, cada habitante del país posee un teléfono móvil, con esto se deduce que existe un crecimiento anual de aproximadamente un 19 %.[20]

Durante el año 2013, según el Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR), 207,275 ciudadanos y ciudadanas nicaragüenses disponían de conexión de acceso a internet, lo que corresponde al 3.43 por ciento de la población total. La desagregación de conexión móvil o fija no está disponible para el año 2013, sin embargo, durante el año 2011 el 64 % de las conexiones eran fijas, es decir, 91,776 ciudadanos y ciudadanas nicaragüenses se conectaban de manera alámbrica en contraste con el 36 % que se conectaba inalámbricamente.[21]

Por otro lado, TELCOR reporta que para 2013 existían 6,808,930 líneas celulares asignadas a nivel nacional, lo que equivale a decir que un ciudadano/a nicaragüense utiliza más de un teléfono móvil. Según las estadísticas de TELCOR, del 2010 al 2013 se aprecia un crecimiento anual de aproximadamente un 8 % en la utilización del servicio móvil. De acuerdo a la clasificación de usuarios de telefonía celular por tipo de plan, sobresale el plan prepago con 6,344,451 asignaciones durante el 2013, seguido del plan pospago (396,701) y en menor cantidad las unidades fijas celulares con 1,643 asignaciones.[22] Según el informe de Foro Económico Mundial titulado "Global Information Technology Report 2014"[23], Nicaragua aparece como el país latinoamericano con tarifas celulares más caras; el estudio explica que en Nicaragua se padece de importantes debilidades en infraestructura de telecomunicaciones, así como falta de innovación e impulsar al sector. Por otro lado, se hace mención que el minuto de teléfono celular prepago podría llegar a costar cerca de U$0,91.

19 SITEAL. “La brecha digital en América Latina”. http://www.siteal.iipe-oei.org/sites/default/files/siteal_datodestacado25_20121205.pdf (consultado: 11 noviembre, 2015)

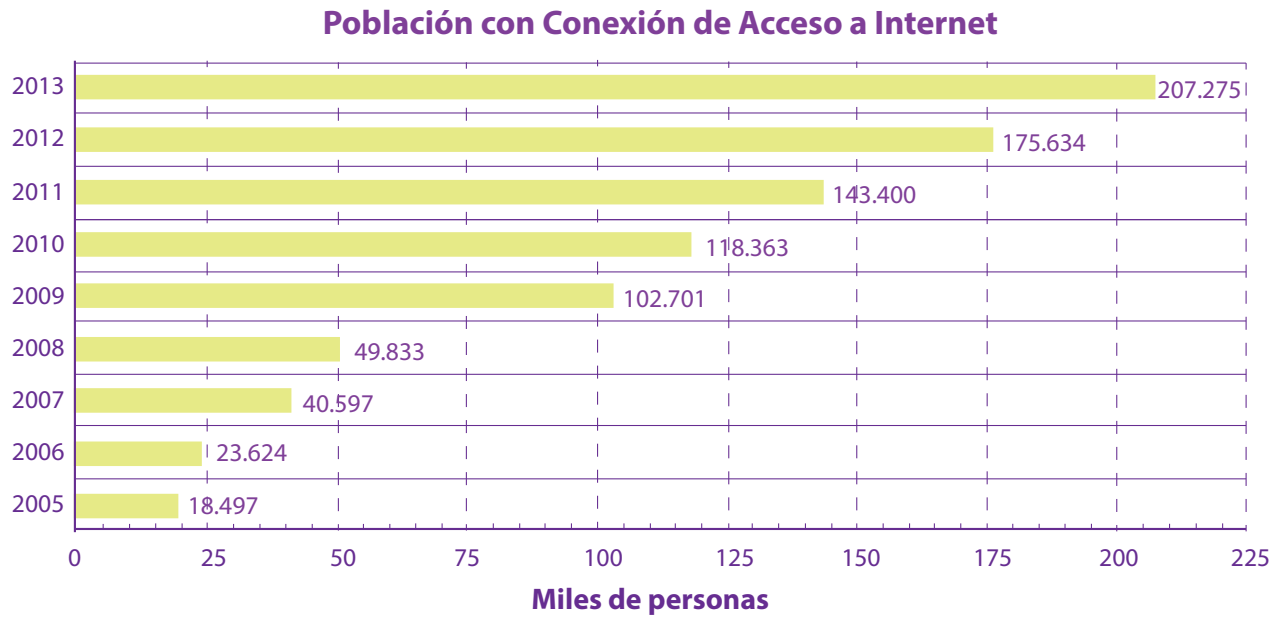
20 Instituto Nicaragüense de Telecomunicaciones y Correos. Estadísticas del sector de las telecomunicaciones de Nicaragua.

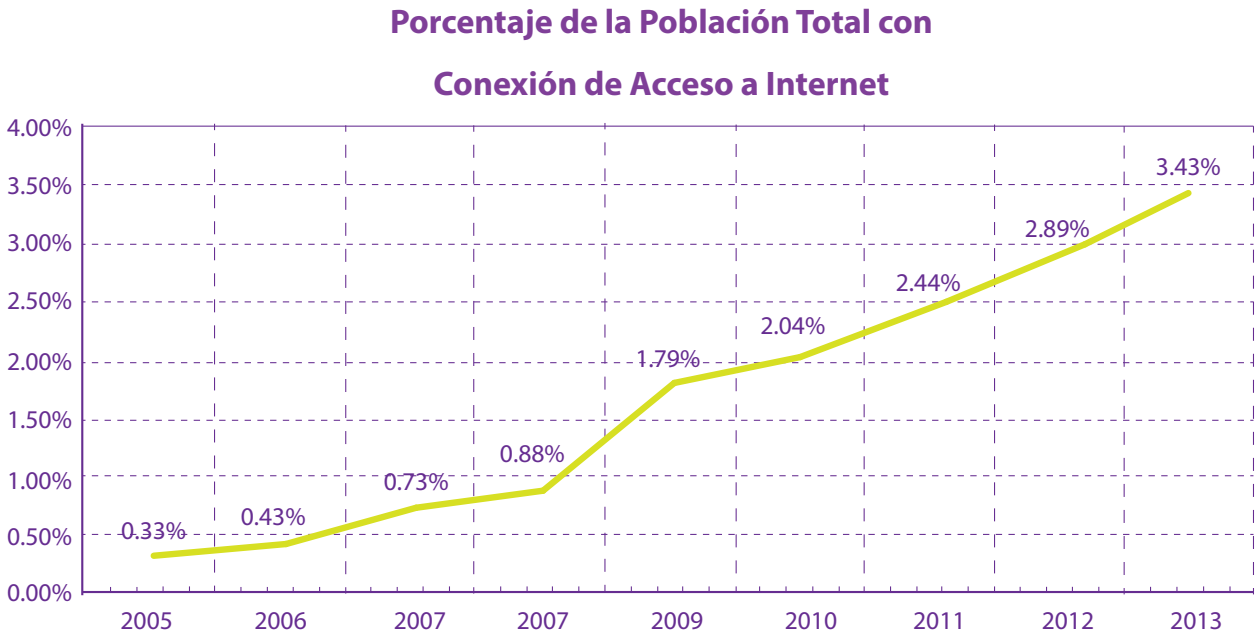
21 TELCOR. “Conexiones del servicio de acceso al internet”. http://www.telcor.gob.ni/Desplegar.asp?PAG_ID=50 (consultado: 12 agosto, 2015)

22 TELCOR. “Telefonía celular”. http://www.telcor.gob.ni/Desplegar.asp?PAG_ID=47 (consultado: 12 agosto, 2015)

23 World Economic Forum. “The Global Information Technology Report 2014”. http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf (consultado: 11 mayo, 2015)

Por otro lado y según un estudio de la plataforma virtual "Guía Local", el ranking de países que mayor crecimiento mostraron en el uso de dispositivos móviles es liderado por Nicaragua; el informe registra un crecimiento anual del 123 %, después que el país no figuraba en la medición hoy se posiciona como el de mayor crecimiento a la par de países como Argentina, Brasil y México.[24]





24 Guía Local Blog. http://guialocal.com/blog/es/2014/09/15/cayo-un-12-el-uso-de-computadoras-para-conectarse-a-internet/?utm_source=press&utm_medium=mail&utm_campaign=invasion (consultado: 12 agosto, 2015)

Año	Población Total	Población con Conexión de Acceso a Internet[4]	Relación
2005	5551,000[1]	18,497	0.33%
2006	5522,606[2]	23,624	0.43%
2007	5595,541[2]	40,597	0.73%
2008	5668,866[3]	49,833	0.88%
2009	5739,387[4]	102,701	1.79%
2010	5815,526[4]	118,363	2.04%
2011	5886,475[4]	143,400	2.44%
2012	6071,045[5]	175,634	2.89%
2013	6035,748[4]	207,275	3.43%

Fuentes:
1. INEC, N"Censo 2005".
2. INIDE, “Estimaciones y Proyecciones de Población”, Período 1950-2050. Revisión Octubre 2004.
3. INIDE, “Estimaciones y Proyecciones de Población”, Período 1950-2050. Revisión 2007.
4. Telcor: www.telcor.com.ni, Estadísticas, Acceso a Internet.
5. INIDE: "Población Total, estimada al 30 de Junio del año 2012".

1.3. Criminalización de defensoras y defensores de derechos humanos

1.3.1. Institucionalidad democrática

Nicaragua, en los últimos años, se ha caracterizado por un acelerado proceso de agudización de la crisis de gobernabilidad democrática; durante el segundo período de gobierno de Daniel Ortega, las denuncias por fraudes electorales y los constantes cuestionamientos de su legitimidad y legalidad alimentan tal situación.

La aprobación de reformas al Código Militar, la nueva Ley de la Policía Nacional, las reformas en materia tributaria y financiera, las reformas a la Ley Integral Contra la Violencia Hacia las Mujeres, la Ley de Concesión Canalera y las reformas parciales a la Constitución Política en febrero de 2014, han implicado cambios al régimen jurídico del país que define con claridad cómo el régimen político ha logrado institucionalizar su modelo autoritario y hegemónico, estructurado para controlar todo y por ende crear un clima de inseguridad jurídica para la ciudadanía en general.

En Nicaragua, el Centro Nicaragüense de Derechos Humanos (CENIDH) anualmente da a conocer sobre la situación de defensores y defensoras de derechos humanos. Si bien no han registrado específicamente casos por violaciones al derecho a la privacidad digital, sí han informado sobre actos de hostigamiento contra sus colaboradores/as y directores mediante la publicación en medios oficiales de más de 45 artículos que tuvieron lugar entre los meses de enero y agosto de 2013[25], en los que se intenta denigrar su labor así como las injerencias y daños a la propiedad de la presidenta del CENIDH, sin que estos acontecimientos surtan un efecto investigativo y judicial de parte de las autoridades competentes.

El abuso de poder, los actos de corrupción, la impunidad y las constantes violaciones a los derechos humanos no solo afectan al fortalecimiento del Estado de derecho, sino que son obstáculos para que cualquier país avance en materia de equidad social, desarrollo humano, justicia, seguridad y progreso económico. La criminalización "es una de las respuestas por parte de funcionarios y poderes económicos a la acción de la defensa de Derechos Humanos"[26], la cual consiste en utilizar cualquier herramienta o sistema para deslegitimar y desmovilizar la actuación del individuo que defiende y pone de manifiesto algún acto de violación a los derechos humanos.

1.3.2. Control de medios de comunicación

Es de conocimiento público que en Nicaragua existe una concentración del poder y de los medios de comunicación en manos de la familia presidencial, los que incluyen medios de comunicación televisivo, radial y prensa escrita, limitando de esta manera el acceso a la información pública escrita y el acceso a entrevistas oficiales que, a pesar de contar con la Ley de Acceso a la Información Pública aprobada en el año 2007, no se cumple.

La reciente reforma al Código Militar de Nicaragua establece en su artículo 2 inciso 15 que el Ejército de Nicaragua tendrá el control de las comunicaciones y de los puntos de comunicación, así como el espectro radio eléctrico y satelital que, además de ser regulados, serán propiedad del Estado, reafirmando el nuevo rol de seguridad nacional del Ejército y remarcando un modelo autoritario y dictatorial que utiliza la ley y la institucionalidad para fortalecer sus intereses ideológico y económicos.

Según el Instituto de Estudios Estratégicos y Políticas Públicas, tal reforma no abandona el riesgo de control sobre el espacio digital.[27]

25 Centro Nicaragüense de Derechos Humanos, *Nicaragua ante la segunda revisión del Examen Periódico Universal 2014* (Nicaragua: Centro Nicaragüense de Derechos Humanos, 2014), 20.

26 Unidad de protección a Defensoras y Defensores de Derechos Humanos en Guatemala, *Criminalización en contra de Defensores y Defensoras de Derechos Humanos Reflexión sobre Mecanismos de Protección 2009* (Guatemala: Unidad de protección a Defensoras y Defensores de Derechos Humanos en Guatemala, 2009), 7.

27 Irving Davila. *Análisis jurídico comparado del Código Militar vigente y la iniciativa de reformas propuestas por la presidencia de la República a la Asamblea Nacional*, (Managua: Ieepp, 2014), 9.

1.3.3. Amenazas, intimidación y criminalización

A nivel nacional se identifican niveles, formas y mecanismos para la intimidación, amenazas e intentos de criminalización en la labor por la defensa de los derechos humanos o como generadores de opinión pública, en el caso de quienes lideran y coordinan programas o proyectos de promoción de pensamiento crítico y el ejercicio de los derechos de la participación ciudadana activa.

En una primera escala se ubican aquellas organizaciones que realizan denuncias o acompañamiento de personas que han sido sujetos de violación de derechos humanos, entre ellas figuran el Centro Nicaragüense de Derechos Humanos y el Movimiento de Mujeres María Elena Cuadra, organizaciones reconocidas por su labor de promoción y defensa activa en la demanda de igualdad, equidad, libre de violencia y respecto a los derechos humanos.

En esta misma escala están aquellos y aquellas periodistas o comunidadores sociales que están en medios o programas independientes, y con mayor riesgo los que se atreven a realizar periodismo investigativo. En este sentido se señala que las voces más críticas son las que se quieren callar y por ello son quienes enfrentan persecución política de manera directa y sistemática.

En una segunda escala se encuentran las organizaciones y personas que realizan activismo de derechos humanos a través de otras formas alternativas como el arte, la cultura o ciberactivismo, donde los ataques o actos de intimidación se califican como indirectos. Se señala que los métodos que se utilizan son más sutiles, menos visibles y que están encaminados a ocasionar miedo o provocar la autocensura. Este tipo de ataques se valoran como más efectivos por que no causan daño inmediato, pero que se van estructurando a mediano o largo plazo hasta causar un efecto que en la mayoría de los casos es acallar voces.

2. Marco legal nacional

Uno de los derechos fundamentales de la persona más afectado en las sociedades modernas es el derecho a la privacidad. Ello se debe al desarrollo experimentado en el campo de la tecnología, razón que ha conllevado la transformación de un bien jurídico en el olvido en uno de los hitos del derecho actual.

El derecho a la privacidad se ha visto seriamente afectado, ello como resultado de los adelantos tecnológicos. Esta situación ha creado una preocupación en la doctrina científica jurídica que vela por una mayor protección de la privacidad debido a su estrecha relación con la dignidad humana y el desarrollo de la personalidad.

Como parte de este trabajo, nos referiremos al derecho a la privacidad como un todo que involucra el derecho a la vida privada y su familia, la inviolabilidad del domicilio, correspondencia y comunicaciones de todo tipo, el derecho a la intimidad, el derecho a la autodeterminación informativa y protección de datos personales, en otras palabras, el derecho a controlar la recolección, uso y transferencia de nuestros datos personales en manos de terceros.

2.1. Tratados internacionales

La protección y garantía del derecho a la privacidad lo encontramos en los tratados internacionales suscritos por Nicaragua, los cuales ejercen su fuerza vinculante tanto en el ámbito de las relaciones entre Estados como en las relaciones internas. El artículo 138 constitucional de Nicaragua[28] establece que los instrumentos internacionales aprobados por la Asamblea Nacional confieren efectos legales, dentro y fuera del país, una vez que hayan entrado en vigencia internacionalmente. Es decir, los tratados, convenios y/o instrumentos ratificados y aprobados por Nicaragua forman parte del derecho vigente, por consiguiente, las leyes que a nivel nacional se debatan y aprueben deberán ir en consonancia con el derecho internacional y de lo que el derecho a la privacidad en todos sus ámbitos refiera.

Además de lo regulado por la Constitución Política de Nicaragua, el control de convencionalidad que realiza la Corte Interamericana de Derechos Humanos (Corte IDH) es de vital importancia, pues dicho control es el cumplimiento de la función principal que fue otorgada por la Convención Americana mediante su artículo 62 a la Corte IDH. Es un control de carácter complementario de las obligaciones convencionales (Constitución) de los Estados de respetar y garantizar derechos humanos.

28 Nicaragua "Constitución Política de la República de Nicaragua" La Gaceta No. 176 (16, septiembre 2010), artículo 138, Inc, 12.

Dos casos nicaragüense ante la CorteIDH han hecho alusión al control de convencionalidad. El primero[29] sostenía, en abstracto, que era improcedente la revisión de las legislaciones nacionales. Sin embargo, diez años después, en la sentencia del caso *Yatama vs. Nicaragua* del 23 de junio de 2005, la CorteIDH mencionó que:

> [...] el deber general del Estado de adecuar su derecho interno a las disposiciones de [la CADH] para garantizar los derechos en ella consagrados, establecido en el artículo 2, incluye la expedición de normas y el desarrollo de prácticas conducentes a la observancia efectiva de los derechos y libertades consagrados en la misma, así como la adopción de medidas para suprimir las normas y prácticas de cualquier naturaleza que entrañen una violación a las garantías previstas en la Convención. Este deber general del Estado parte implica que las medidas de derecho interno han de ser efectivas (principio del *effet utile*), para lo cual el Estado debe adaptar su actuación a la normativa de protección de la Convención.[30]

En ese sentido, los Estados tienen el deber de asegurar que cualquier limitación del derecho a la privacidad esté de acuerdo a lo regulado en las normas de derechos humanos del sistema interamericano. En otras palabras, el derecho a la privacidad puede limitarse siempre y cuando esta limitación sea prescrita por ley, necesaria, idónea y proporcional para obtener un objetivo legitimo. Este examen de limitaciones permisibles ha sido desarrollado por el derecho internacional de los derechos humanos, y se aplica por igual al derecho a la privacidad, libertad de expresión y libertad de asociación.[31]

2.2. Constitución Política de Nicaragua

Nicaragua, en su Constitución Política de 1987, Titulo IV, Capítulo I, reconoce una serie de derechos fundamentales, entre ellos los llamados “derechos de la personalidad”, entendidos como aquellos derechos subjetivos y absolutos que posee toda persona y que garantizan la tutela y protección de los bienes jurídicos inmersos en el ser humano como la vida, la privacidad, el domicilio, la integridad física y la correspondencia, entre otros.

29 Corte Interamericana de Derechos Humanos, Caso Genie Lacayo Vs. Nicaragua, Excepciones Preliminares, Serie C No. 21 del 27 de enero de 1995. párr. 50.

30 Corte Interamericano de Derechos Humanos, Caso Yatama Vs. Nicaragua, Sentencia de 23 de junio de 2005, Serie C No. 127, párr. 7.

31 Necessary and Proportionate. “Análisis Jurídico Internacional de Apoyo y Antecedentes a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones”, https://es.necessaryandproportionate.org/content/explicaci%C3%B3n-principio-por-principio (consultado: 4, septiembre 2015).

2.2.1. Vigilancia

2.2.1.1. Salvaguardas constitucionales del derecho a la privacidad en el contexto de la vigilancia de las comunicaciones

1. El artículo 26 constitucional[32] dispone que toda persona tiene derecho:
2. A su vida privada y a la de su familia.
3. Al respeto de su honra y reputación.
4. A conocer toda información 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 esa información.
5. A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo.

El contenido normativo de este precepto constitucional aborda el derecho a la vida privada desde un punto de vista más amplio a aquel tradicional, en el que las libertades públicas para crear un espacio libre de injerencias no solo aplica para las que provienen desde particulares (como lo establecía la Constitución Política de 1987), sino también de aquellas injerencias desde el Estado. De ahí que, en su apartado 3 introducido con la reforma constitucional de 1995, se reconoce el derecho a la información sobre registros de datos personales.

Los derechos humanos son derechos individuales en sentido propio. El derecho a la vida privada, reconocido en el artículo 26 de la Constitución Política de Nicaragua, protege la autonomía del individuo en su ámbito privado y aplica tanto para los y las ciudadanas nicaragüenses como también para las personas extranjeras, pues se trata de un derecho estrictamente vinculado a la propia persona, imponiendo como única restricción el ejercicio de los derechos políticos[33].

Respecto a la titularidad del derecho por parte de las personas jurídicas, no existe referencia constitucional pues el derecho a la privacidad está concebido como un derecho de la personalidad, por ende lo ostentan personas físicas y no jurídicas.

Como consecuencia del desarrollo técnico jurídico, la protección material del derecho a la vida privada presenta en el contexto constitucional de Nicaragua un contenido amplio y complejo: el reconocimiento de la vida privada personal, vida privada familiar, inviolabilidad del domicilio y del secreto de las comunicaciones. Sin embargo, también cuenta con otras manifestaciones que no

32 Nicaragua "Ley de Reforma Parcial a la Constitución Política de Nicaragua" La Gaceta, No. 26 (2014), artículo 26.
33 Nicaragua "Constitución Política", artículo 27.

necesariamente suponen derechos protegidos y reconocidos como se verá a continuación.

a) Vida privada personal y familiar

La vida privada es entendida bajo un concepto que está relacionado con la prohibición de que una persona sea objeto de injerencias arbitrarias hacia ella misma o la de su familia, su domicilio o su correspondencia, así como de ataques a su honra o a su reputación, contando con la protección de la ley contra tales injerencias o ataques. En Nicaragua, aunado a lo contenido en precepto constitucional, la Ley de Acceso a la Información Pública[34] y su reglamento[35] y la Ley de Protección de Datos Personales[36] hacen referencia a los aspectos que se consideraran como información privada y/o sensible, entendiendo aquellos referidos a la salud o vida sexual, raza, etnia, preferencia política o religiosa, situación económica, social o familiar, o a su honra y reputación, antecedentes penales o faltas administrativas, información crediticia y financiera o cualquier otra que pueda ser motivo de discriminación.

b) Protección de datos personales

La protección de datos personales emerge de la garantía constitucional establecida en el artículo 26.3 de la Constitución Política, la que establece 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.

La Ley de Protección de Datos Personales define la autodeterminación informativa como el derecho que tiene toda persona a saber quién, cuándo, con qué fines y en qué circunstancias toman contacto con sus datos personales[37], entendidos los datos como toda información sobre una persona natural o jurídica que la identifica o la hace identificable, sean estos medios electrónicos o automatizados.[38]

Hasta el año 2013, Nicaragua velaba por el cumplimiento de dicho precepto constitucional a través del recurso de amparo, el cual era admisible contra el funcionario, autoridad o agente que por su acción u omisión violara o tratara de violar los derechos y garantías consagrados en la Constitución Política. Posteriormente y para garantizar el resguardo y protección de los datos personales, en el año 2013 se reforma la Ley de Amparo[39] en la que se adiciona el recurso de *habeas data* con el objetivo de evitar la publicidad ilícita de los mismos, la reforma establece que el recurso de *habeas data,*

34 Nicaragua "Ley de Acceso a la Información Pública" La Gaceta No. 118 (22, junio 2007), artículo , artículo 4, inciso b., párr. segundo.
35 Nicaragua "Reglamento de la Ley de Acceso a la Información Pública" Asamblea Nacional de la República de Nicaragua, Decreto No. 81-2007 (17, agosto 2007)
36 Nicaragua "Ley de Protección de Datos Personales" La Gaceta No. 61 (2012), artículo 2, inciso g.
37 Nicaragua "Ley de Protección de Datos Personales" La Gaceta No. 61(2012), artículo 3 inciso a).
38 Nicaragua "Ley de Protección de Datos Personales", artículo 3 incisos e) y f).
39 Nicaragua "Ley de Amparo" La Gaceta No 61 (08, abril 2013).

> [...] 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".[40]

El criterio de la Sala Penal del Tribunal de Apelaciones, Circunscripción León de la Corte Suprema de Justicia de Nicaragua, antes de la reforma a la Ley de Amparo respecto al recurso de *habeas data*, era que "el Recurso de Amparo al igual que el Recurso por Inconstitucionalidad, el Recurso de Exhibición Personal, el Recurso por Inconstitucionalidad, entre otros recursos…"[41] constituían los únicos mecanismos jurídicos mediante los cuales se garantizan la supremacía de la Constitución Política frente a las acciones y omisiones de los funcionarios públicos.

Al respecto, la Sala de lo Constitucional fue enfática en aclarar que la valoración de fondo realizada por la Sala Penal le corresponde de manera exclusiva a la Sala Constitucional;

> ...así en reiteradas sentencias esta Sala de lo Constitucional ha sido categórica en señalar que 'todos los principios, disposiciones y garantías contenidas en la Constitución Política vinculan sin exclusión a todos los poderes del Estado en su actuar' [...] II). En consecuencia, mientras no se regule de manera autónoma, y con procedimiento especial el Recurso de Hábeas Data, éste debe tramitarse conforme los cauces del Recurso de Amparo...[42]

c) Secreto de las comunicaciones

En el artículo 26.4 del texto constitucional nicaragüense se reconoce de forma concisa el derecho a la inviolabilidad del domicilio y al secreto de las comunicaciones, correspondencia, los papeles privados y las manifestaciones privadas contenidas en cualquier soporte, y se establece como único límite la autorización judicial.

Nicaragua, a diferencia de otros países de la región, no cuenta con una ley especifica de escucha o de interceptación de comunicaciones. Sin embargo, ampliando los supuestos establecidos en la Constitución Política, bajo los cuales se podría interceptar una comunicación, la Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados[43], establece que se interceptarán las comunicaciones a solicitud expresa y fundada del Fiscal General de la República o de la Directora General de la Policía Nacional. El juez penal podrá no solo interceptar una comunicación telefónica, sino también grabar e interrumpir cualquier tipo de comunicación: electrónica, radioeléctrica, fijas o móviles, inalámbricas, digitales o de cualquier otra naturaleza, siempre y cuando sea para fines de investigación penal.

40 Nicaragua "Ley de Amparo" La Gaceta No 61 (08, abril 2013), artículo 6.

41 Sala Penal del Tribunal de Apelaciones. Corte Suprema de Justicia de Nicaragua, Sentencia No. 60 del 18 de enero de 2007.

42 Sala de lo Constitucional. Corte Suprema de Justicia de Nicaragua, Sentencia No. 108 del 20 de mayo de 2003.

43 Nicaragua "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados" La Gaceta No. 199 y 200 (19-20, octubre 2010), capítulo VIII, artículo 62.

Dicha interceptación aplica únicamente para la investigación de los delitos previstos en la misma ley: financiamiento ilícito de estupefacientes, psicotrópicos y sustancias controladas, lavado de dinero, crimen organizado, terrorismo, asesinato, trata de personas, tráfico de migrantes, tráfico y extracción de órganos, delitos contra el sistema bancario, cohecho cometido por autoridad, uso de información reservada, entre otros.[44]

Por otro lado, los artículos 213 y 214 del Código Procesal Penal hacen una selección de los delitos graves que pueden dar lugar a una intervención telefónica y solo por un tiempo determinado, así como el procedimiento de las intervenciones de otro tipo de comunicaciones sean estas escritas, telegráficas y electrónicas respectivamente.

Es importante destacar que dentro del proceso penal, la intervención de las comunicaciones telefónicas y la interceptación de comunicaciones escritas o telegráficas, constituyen una intromisión permisible de los órganos de persecución penal del Estado en el libre ejercicio del derecho fundamental de las personas reconocido en el artículo 26.4 de la Constitución Política, cuya finalidad consiste en averiguar la verdad por su relación con un hecho delictivo.

d) Dimensiones constitucionales

El precepto constitucional número 26 respecto a la privacidad de todo ciudadano y ciudadana nicaragüense presenta un doble contenido: aquel entendido positivamente que impide la intromisión e injerencias ajena a nuestra información y uno negativo que refiere al control privado que ejercen terceros sobre nuestra información soportada en archivos informáticos. Desde esta visión el derecho a la autodeterminación informativa se presenta como el derecho de una persona a reservar un ámbito de su vida como intangible y secreto para los demás, así como el derecho a controlar la recolección, uso y tratamiento de sus datos personales en manos de terceros.

Positivamente, es a partir del precepto constitucional donde se encuentra, de forma implícita, la protección de los datos personales de los ciudadanos nicaragüenses, y el planteamiento de un limite legal a la Administración Pública, la que se encuentra en el deber de informar, a petición del ciudadano, qué datos personales tiene registrados, el por qué y la finalidad de ello.

e) Otros derechos

En el contexto de vigilancia por parte del Estado, la afectación del derecho a la privacidad también conlleva a la vulneración de otros derechos humanos como la libertad de expresión, asociación, la seguridad personal, la libertad personal e integridad psicológica.

44 Nicaragua "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados", artículo 3.

La Constitución Política no hace alusión de la relación del derecho a la privacidad con otros derechos expresamente, sin embargo la Ley de Protección de Datos Personales deja claro que la autodeterminación informativa puede conjugar con otros bienes jurídicos de la persona, destacando:

- La intimidad física e informativa. Esta última bajo el entendido de difundir información personal de parte del titular del derecho con terceros.
- La seguridad personal
- La libertad personal

Por otro lado, el artículo 17 de la Ley de Protección de Datos Personales hace mención a algunos derechos implícitos que la libertad informática supone, a saber:

- El derecho a acceder y controlar las informaciones que se le atribuyen como persona, procesadas en base de datos, a través de vías administrativas y procesales.
- El derecho a demandar la corrección, rectificación, supresión, complementación y actualización de datos personales contenidos en bases de datos públicos y privada que no correspondan, sean inapropiados o se consideren irrelevantes, así como aquellos obtenidos por procedimientos ilegales.
- El derecho a que se tomen todas las medidas de confidencialidad en relación a los datos personales que asienten en ficheros o bases de datos públicos y privadas.
- El derecho a exigir que se evite la difusión y transmisión de datos personales a personas e instituciones (publico privadas) no autorizadas para conocer de información privada.

En cuanto al derecho a la privacidad y la libertad de expresión, el artículo 13.3 de la Convención Americana de Derechos Humanos establece que “no se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares [...]”. En el caso de Nicaragua, los mecanismos indirectos de restricción se ocultan detrás de acciones aparentemente legítimas que, sin embargo, son adelantadas con el propósito de condicionar el ejercicio de la libertad de expresión de los individuos. Para los nicaragüenses, el saber que sus comunicaciones están siendo constantemente vigiladas por parte del Estado en complicidad con los proveedores de servicio, vulnera el principio de libertad de expresión, en cuanto las personas estarán menos dispuestas a hablar sobre temas que consideren podrían conllevar a una imputación de un delito o verse envuelto o envuelta en un caso de injerencia a su vida privada, situación que se configura en una violación del artículo 13.3 de la Convención. Como lo ha sostenido la Corte Interamericana de Derechos Humanos, resulta violatorio de la libertad de expresión “todo acto del poder público que implique una restricción al

derecho de buscar, recibir y difundir informaciones e ideas, en mayor medida o por medios distintos de los autorizados por la misma Convención."[45]

Para el caso de Nicaragua, es importante señalar que las consecuencias de expansión de los poderes y prácticas de vigilancia de los Estados frente a la interferencia de los derechos a la intimidad y la libertad de expresión, y la interdependencia de los dos derechos, aún no han sido considerado ampliamente por los tribunales nicaragüenses.

2.2.1.2 Limitaciones constitucionales al derecho a la privacidad en el contexto de la vigilancia de las comunicaciones

El derecho a la privacidad no es un derecho absoluto. Nicaragua conforme al control de constitucionalidad puede limitar el derecho a la privacidad como medida de protección de la seguridad nacional y seguridad pública de las y los nicaragüenses. La Constitución establece que el Estado puede restringir este derecho, siempre y cuando la vigilancia de las comunicaciones este prescrita por ley, sea necesaria, adecuada y proporcional al objetivo perseguido[46].

Respecto a las limitaciones, el Estado nicaragüense ha establecido en el Código Procesal Penal de Nicaragua[47], medidas de espionaje e intervenciones telefónicas y en las comunicaciones que interfieren directa e indirectamente con el derecho a la privacidad. Los artículos 213 y 214 establecen las "intervenciones telefónicas" y la "interceptación de comunicaciones escritas, telegráficas y electrónicas", cuando se trate de delitos graves como el 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 los casos de investigación de los delitos antes mencionados, aunado a lo establecido en la Ley de Crimen Organizado[48], que requieren de intervención de comunicaciones a solicitud expresa y fundada del Fiscal General de la República o del Director General de la Policía Nacional, los jueces de Distrito de lo Penal podrán autorizar a este el impedir, interrumpir, interceptar o grabar comunicaciones, correspondencia electrónica, otros medios radioeléctricos e informáticos de comunicaciones, fijas, móviles, inalámbricas y digitales o de cualquier otra naturaleza[49] por un plazo máximo de seis meses, salvo en los casos de extrema gravedad o de difícil investigación, en

45 Corte Interamericana de Derechos Humanos, La colegiación obligatoria de periodistas . Opinión Consultiva OC-5/85 del 13 de noviembre de 1985, Serie A No. 5, párr. 55.

46 Nicaragua "Ley de reforma parcial a la Constitución Política de Nicaragua" artículo 26.

47 Nicaragua "Código Procesal Penal de la República de Nicaragua" La Gaceta No. 243 y 244 (24, diciembre 2001).

48 Nicaragua "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados".

49 Nicaragua "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados", capítulo VIII, artículo 62.

los que el juez, mediante resolución fundada, disponga una prorroga de hasta seis meses más.[50]

Por otra parte, se puede llegar a vulnerar el derecho a la privacidad en el contexto de vigilancia e interceptación de las comunicaciones bajo el supuesto de un delito flagrante[51]. La norma confiere la facultad al Ministerio Público para investigar a las personas, no estando obligada a notificar a la persona – a investigar - de la decisión que autoriza las diligencias de su investigación[52], lo que pone en desventaja a las personas para que puedan impugnar la decisión, todo ello sin contar las amplias facultades que la Fiscalía confiere a la Policía de requisar, de inspeccionar e investigar corporalmente a las personas y registrar documentación "con o sin consentimiento de estas que por sospechas se piense que hayan cometido un delito [...]"[53].

2.2.1.3. Mecanismos de acceso a la justicia en el contexto de la vigilancia

En el contexto de la protección de datos personales, la reforma a la Ley de Amparo[54] en la que se adiciona el recurso de *hábeas data*, establece que el presente recurso tendrá por objetivo evitar la publicidad ilícita de los datos personales; se contempla el derecho a 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.

Por otro lado, la reforma a la Ley de Amparo establece que el recurso,

> [...] 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.[55]

Por otro lado, el recurso de *habeas data* no es extensivo a los cuatro numerales del precepto constitucional, excluyendo la interposición del mismo cuando se presuma violación a la honra y reputación de una persona. El recurso procede en defensa de los derechos constitucionales reconocidos en el artículo 26 numerales 1, 3 y 4 de la Constitución Política, en consecuencia toda persona puede utilizar dicho recurso para:

50 Nicaragua "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados", capítulo VIII, artículo 62.

51 Comete flagrante delito toda aquella personas que después de haber cometido un hecho punible es descubierto inmediatamente o cuando es sorprendido con objetos o huellas que revelan que acaba de cometer un acto delictivo.

52 Nicaragua "Código Procesal Penal de la República de Nicaragua" La Gaceta No. 243 y 244. 24, (diciembre 2001), artículo 249.

53 Nicaragua "Código Procesal Penal de la República de Nicaragua", artículo 236 y 239.

54 Nicaragua "Ley de Amparo".

55 Nicaragua "Ley de Amparo", artículo 6.

1. Acceder a información personal que se encuentre en poder de cualquier entidad pública y privada de la que generen, produzcan, procesen o posean, información personal, en expedientes, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier documento que tengan en su poder.

2. Exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización, de datos personales sensibles independientemente que sean físicos o electrónicos almacenados en ficheros de datos, o registro de entidades públicas o instituciones privadas que brinden servicio o acceso a terceros, cuando se presuma la falsedad, inexactitud, desactualización, omisión total o parcial o la ilicitud de la información de que se trate.

3. Exigir la oposición, modificación, supresión, bloqueo, inclusión, complementación, rectificación o cancelación y actualización de cualquier publicidad de datos personales sensibles que lesionen los derechos constitucionales.[56]

El recurso de *habeas data* se interpondrá agotada la vía administrativa contemplada en la Ley de Protección de Datos Personales[57], dentro de un plazo de treinta días posteriores a la notificación de la autoridad administrativa competente, y podrá conocer del mismo la Sala de lo Constitucional de la Corte Suprema de Justicia. Lo podrá interponer: persona natural afectada, tutores y sucesores o apoderados de las personas naturales afectadas y personas jurídicas afectadas por medio de representante legal.[58]

Una vez admitido el recurso, la Sala de lo Constitucional ordenará al administrador del fichero del cual se supone la vulneración del precepto constitucional, que aporte la información objeto del recurso cuando se trate de información confidencial, la Sala tomará las medidas cautelares pertinentes a fin de que el contenido no trascienda las partes. Finalmente, la sentencia que declare con lugar el recurso de *habeas data* ordenará modificar al recurrente (administrador del fichero) el pleno goce del derecho constitucional vulnerado, así como la eliminación o supresión inmediata de la información o el dato impugnado.[59]

El recurso de *habeas data* hace referencia al derecho legítimo de las personas a "la libre disposición de los datos personales"[60]. 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 explicita e individualmente la captación y el tratamiento de los datos por terceros y, por otro lado, por

56 Nicaragua "Ley de Amparo", artículo 87.
57 Nicaragua "Ley de protección de datos personales", artículo 48.
58 Nicaragua "Ley de Amparo", artículos 88, 89 y 90.
59 Nicaragua "Ley de Amparo", artículo 95 y 97.
60 Osvalo Alfredo Gozaíni, "Hábeas Data. Protección de los datos personales. Doctrina y Jurisprudencia". (Argentina: Rubinzal Culzoni Editores, 2011), 67.

aquella autorización regida por ley. Sin embargo, ni el consentimiento ni la habilitación legal suponen la pérdida del poder sobre los datos, ya que existen una serie de derechos que complementan la autodeterminación informativa[61] (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).

La Ley de Protección de Datos Personales legitima al ciudadano afectado permitiéndole ejercer la acción de protección de datos personales, o *habeas data*, mismo que como se ha mencionado protege contra las injerencia y vulneraciones informáticas al igual que atentados ocasionados a la intimidad personal. Es el derecho que asiste a toda persona, identificada o identificable, sobre la base de los supuestos siguientes:

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

2. De 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.

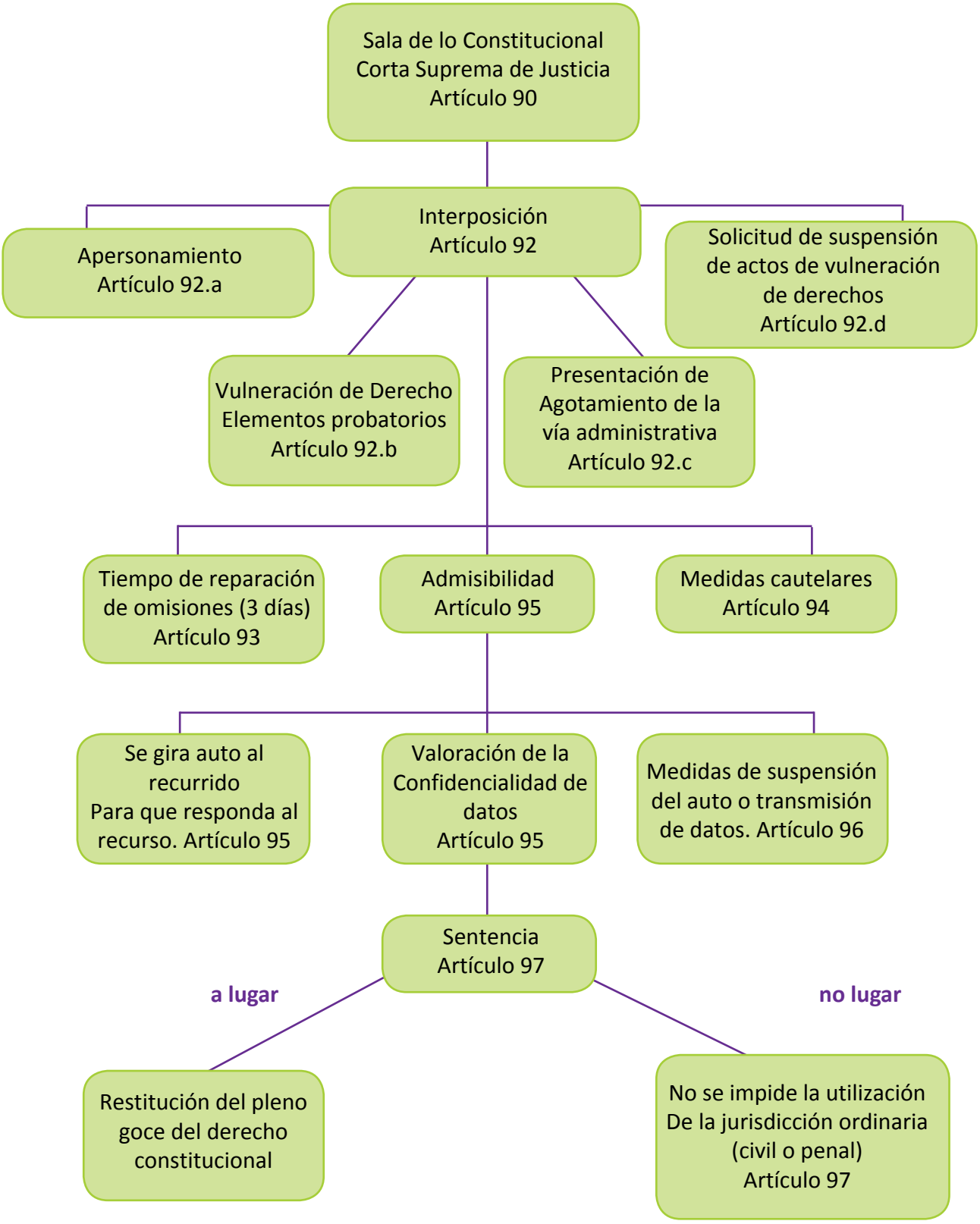
3. Cuando el responsable del fichero de datos se niegue a proveer al ciudadano el derecho de oponerse a figurar en ficheros de datos, aun cuando los datos hayan sido recabados de fuentes accesibles al público[62].

En Nicaragua, el derecho a la protección de la privacidad en el contexto de la seguridad digital enfrenta un reto en cuanto al ejercicio de cumplimiento del mismo. El recurso constitucional del *habeas data* como mecanismo procesal de la acción de protección de datos personales presupone un equilibrio a favor del ciudadano frente a los propietarios de los ficheros de datos. Sin embargo, la pasividad de las y los usuarios frente al cumplimiento de su derecho no creará precedente normativo de dicho mecanismo proteccionista.

61 Pablo Lucas Murillo de la Cueva, "Perspectivas del derecho a la autodeterminación informativa". *Revista de Internet, Derecho y Política*, 5 (2007), 18-32.

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

Flujograma No. 1



Fuente: Elaboración Propia, a partir de la Ley No. 49, Ley de la Amparo con reformas incorporadas. Artículos 90-97.

2.2.2. Anonimato y cifrado

El anonimato puede definirse como la comunicación mediante la cual se utilizan métodos sin usar o presentar la identidad propia. A través del anonimato se protege la determinación del nombre o identidad propios, utilizando un nombre ficticio que no necesariamente se asocia con la identidad legal o habitual de una persona[63].

Por otro lado, el cifrado se define como el proceso matemático de utilizar códigos y claves para comunicarnos de forma privada. A lo largo de la historia, las personas han utilizado métodos cada vez más sofisticados de cifrado.[64]

El siguiente acápite aproxima la protección del anonimato y cifrado en Nicaragua, determinando aquellas salvaguardas, limitaciones y mecanismos judiciales para la protección del cifrado y el anonimato.

2.2.2.1. Salvaguardas constitucionales para la protección del cifrado y el anonimato

El precepto constitucional 26, como ya se ha mencionado, procura la protección a la privacidad y resguardo del derecho a la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo; tal precepto aunado al artículo 34 constitucional[65] establece que toda persona en un proceso tiene derecho, en igualdad de condiciones, al debido proceso y a la tutela judicial efectiva y, como parte de ellas, a diversas garantías, entre ellas la de no ser procesado ni condenado por acto u omisión que, al tiempo de cometerse, no esté previamente calificado en la ley de manera expresa e inequívoca como punible, ni sancionado con pena no prevista en la ley[66].

En Nicaragua, la legislación no profundiza sobre la protección del cifrado y el anonimato, excepto aquel cifrado y/o encriptado referido al comercio electrónico. Sin embargo, tanto el anonimato como el cifrado pueden estar protegidos bajo lo establecido en el precepto constitucional numero 26.

a) Anonimato

La relación y compatibilidad en el uso de mecanismos de cifrado y anonimato en la era digital con la lucha contra el terrorismo y la seguridad nacional es un debate que a pesar de haberse desarrollado sustancialmente en otros países del mundo, ha tenido poco protagonismo a nivel nacional. El interés de regular y promover el uso racional de dichos mecanismos como defensa de derechos humanos ha propiciado la emisión de diversos informes al respecto, publicándose recientemente uno de Naciones Unidas muy interesante por cuanto analiza específicamente si los derechos a la privacidad y la libertad

63 Electronic Frontier Foundation. *Anonimato y cifrado.*(EFF, 2015), 3.
64 Electronic Frontier Foundation. *Anonimato y cifrado,* 37.
65 Nicaragua ""Ley de reforma parcial a la Constitución Política de Nicaragua", artículo 34.
66 Nicaragua "Ley de reforma parcial a la Constitución Política de Nicaragua", artículo 34, inciso 11.

de opinión y expresión[67] alcanzan a garantizar el derecho al uso de comunicaciones en línea seguras a través de mecanismos de cifrado y de garantía de anonimato.

El contenido se basa en una premisa importante de la que ya se había advertido desde una multitud de sectores que "el derecho a la privacidad a menudo se entiende como un requisito esencial para la realización del derecho a la libertad de expresión. La injerencia indebida en la vida privada de los individuos puede limitar tanto directa como indirectamente el libre intercambio y evolución de ideas".[68]

El artículo 30 de la Constitución Política establece que "los nicaragüenses tienen derecho a expresar libremente su pensamiento en público o en privado, individual o colectivamente, en forma oral, escrita o por cualquier otro medio" haciendo permisible el anonimato de lo que se desee expresar en privado. Al respecto, la Relatoría Especial de Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) deja claro que "en todos los casos, los usuarios deben tener derecho a permanecer bajo anonimato y cualquier disputa sobre este punto debe ser resuelta exclusivamente en sede judicial".[69]

Por su lado, los artículos 29, 66 y 67 reconocen los derechos a la libertad de expresión, pensamiento e información, así como un marco jurídico que garantiza el derecho de los y las ciudadanos a saber y demandar un ejercicio responsable de la comunicación social como garantía de resguardo al derecho a la privacidad en el contexto de la libre autodeterminación informativa, lo que aunado a lo establecido en el Informe de la Relatoría de Libertad de Expresión de Naciones Unidas, reporte de Frank La Rue, respecto a que los Estados deben "...abstenerse de requerir la identificación de los usuarios, como condición previa para el acceso a las comunicaciones, incluidos los servicios en línea, los cibercafés o la telefonía móvil"[70], dan validez al anonimato en Nicaragua.

El informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue, relaciona el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos referido a la protección— de injerencias en su "correspondencia", con el efecto intimidatorio que las restricciones del anonimato podrían llegar a producir. Como hemos señalado anteriormente, el artículo 26 de la Constitución Política de Nicaragua hace referencia a la prohibición de toda

67 Organización de las Naciones Unidas. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión" (29º período de sesiones del Consejo de Derechos Humanos, resolución A/HRC/29/32 del 22 de mayo, 2015).

68 Organización de las Naciones Unidas. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión" (23º período de sesiones del Consejo de Derechos Humanos, resolución A/HRC/23/40 del 17 de abril, 2013), párr. 24.

69 Organización de las Naciones Unidas. "Informe anual de la Relatoría Especial para la libertad de expresión 2013" (resolución OEA/Ser.L/V.II. del 31 de diciembre, 2013)

70 Organización de las Naciones Unidas. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión" (17º período de sesiones del Consejo de Derechos Humanos, resolución A/HRC/17/27 del 16 de mayo, 2011), párr. 84.

injerencia a la correspondencia de todo tipo y como lo ha sostenido el Relator Especial, el derecho a la correspondencia privada genera una amplia obligación del Estado de velar porque el correo electrónico y otras formas de comunicación en línea lleguen a su destinatario previsto sin injerencia o inspección por parte de órganos estatales o de terceros.[71]

b) Cifrado

No existe precepto constitucional que haga mención al cifrado. Sin embargo, y al igual que el anonimato se puede relacionar con otros derechos regulados constitucionalmente, por ejemplo la libertad de expresión como derecho fundamental reconocido en el artículo 30 de la Constitución Política. Relacionando este derecho y considerando la no existencia del cifrado en nuestro ordenamiento, el artículo 32 constitucional permite indirectamente el cifrado, estableciendo que ningún ciudadano o ciudadana nicaragüense esta obligado a hacer lo que la ley no mande, ni impedida de hacer lo que ella no prohíbe.

El Relator de Libertad de Expresión de Naciones Unidas, David Kaye, ha expresado que

> ...el Cifrado y el Anonimato son los principales vehículos para la seguridad en línea, proporcionando a los individuos un medio para proteger su privacidad, dándoles el poder de navegar, leer, desarrollar y compartir opiniones e información sin interferencias y apoyando a los periodistas, organizaciones de la sociedad civil, miembros de las minorías étnicas o grupos religiosos, a los perseguidos [...] por su orientación sexual o identidad de género, activistas, académicos, artistas y a otros los derechos a la libertad de expresión y opinión.[72]

2.2.2.2. Limitaciones constitucionales a la protección del cifrado y el anonimato

En vista del poco estudio en materia legislativa del anonimato y cifrado, no se encontraron limitaciones constitucionales que puedan analizarse y estudiarse para la presente investigación.

2.2.2.3. Mecanismos de acceso a la justicia en el contexto del cifrado y el anonimato a nivel constitucional

Según el criterio de la Sala Penal del Tribunal de Apelaciones, Circunscripción León de la Corte Suprema de Justicia de Nicaragua, antes de la reforma a la Ley de Amparo los recursos que constituían los mecanismos jurídicos mediante los cuales se garantizaba la supremacía de la Constitución Política frente a las acciones y omisiones de los funcionarios públicos eran: el recurso de amparo, recurso por inconstitucionalidad, recurso de exhibición personal, recurso por inconstitucionalidad, el recurso de conflicto de competencia y constitucionalidad entre poderes del Estado y el conflicto de

71 Organización de las Naciones Unidas. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión",párr. 24.

72 Organización de las Naciones Unidas. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión", párr. 1.

constitucionalidad entre el Gobierno central y los Gobiernos Municipales y de las Regiones Autónomas de la Costa Caribe[73]. En la reforma a la Ley 49 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.

En ese sentido, es posible asegurar mecanismos de acceso a la justicia respecto al cifrado y anonimato a nivel constitucional a través de tres recursos: en primer lugar, el recurso de amparo, interpuesto en contra del funcionario o autoridad que ordene el acto que se presume violatorio de la Constitución Política;[74] el recurso por inconstitucionalidad, mismo que podrá ser interpuesto por cualquier ciudadano o ciudadanos, cuando una ley, decreto o reglamento, se oponga a lo prescrito en la Constitución[75] y, en tercer lugar, el recurso de exhibición personal, el cual procede en favor de aquellas personas cuya libertad, integridad física y seguridad sean violadas o estén en peligro de serlo por funcionario o autoridad, entidad o institución estatal autónoma o no, o por actos restrictivos de la libertad personal de cualquier habitante realizado por particulares[76].

El Relator de Libertad de Expresión, Frank La Rue, ha dejado claro que "el anonimato de las comunicaciones es uno de los avances más importantes habilitados por Internet, y permite a las personas expresarse libremente sin temor a represalias o condenas"[77], lo que en conjunto con recursos y mecanismos de defensa conllevan a la protección del derechos fundamentales como la privacidad en el contexto digital.

2.3. Leyes, reglamentos y jurisprudencia

2.3.1. Vigilancia, cifrado y anonimato en leyes y reglamentos

El Código Penal, Código Procesal Penal, Código de la Niñez y Adolescencia, Código Militar, Ley Orgánica del Poder Judicial, Ley de Amparo, Ley de Acceso a la Información Pública, Ley de Crimen Organizado, Ley de Protección de Datos Personales y su Reglamento, Ley de Firma Electrónica, Ley General de Telecomunicaciones y Servicios Postales, Ley de Defensa de los Consumidores, Ley de Participación Ciudadana, Ley Creadora del Colegio de Periodistas de Nicaragua, Ley de Promoción de los Derechos Humanos y de la Enseñanza de la Constitución Política y el anteproyecto de ley de banda ancha, son solo algunos instrumentos legales nacionales que regulan el derecho a la privacidad en el contexto digital en Nicaragua.

73 Sala Penal del Tribunal de Apelaciones, Sentencia No. 60 del 18 de enero de 2007.
74 Nicaragua "Ley de Amparo", artículo 27.
75 Nicaragua "Ley de Amparo", artículo 9.
76 Nicaragua "Ley de Amparo", artículo 4.
77 Organización de las Naciones Unidas. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión", párr. 23.

El presente apartado hace referencia a la normativa jurídica secundaria y reglamentaciones sobre la privacidad en el contexto de la vigilancia de las comunicaciones por la autoridad y protección de cifrado y anonimato.

2.3.1.1. Normas en materia penal

El Código Penal nicaragüense, que tipifica y penaliza aquellas acciones que constituyen delito, dedica un capítulo a los delitos contra la vida privada y contra las intromisiones ilegitimas en la privacidad:

- Sustracción, desvío o destrucción de comunicaciones: será penado con prisión de seis meses a un año, quien sin enterarse de su contenido, se apodere ilegalmente, destruya o desvié de su destino una comunicación que no le esté dirigida. Y será penado con prisión de uno a dos años, quien conociendo o presuponiendo el contenido de la comunicación se apodere ilegalmente, destruya o desvíe la comunicación que no le pertenece.[78]

- Captación indebida de comunicaciones ajenas: será penado con prisión de uno a dos años, quien ilegítimamente grabe las palabras o conversaciones ajenas, no destinadas al público, o el que mediante procedimientos técnicos escuche comunicaciones privadas o telefónicas que no le estén dirigidas.[79]

- Acceso y uso no autorizado de información: será penado con prisión de uno a dos años, y de doscientos a quinientos días multa, quien sin la debida autorización utilice los registros informáticos de otro, o ingrese, por cualquier medio, a su banco o archivos electrónicos.[80]

El capítulo IV del Código Penal contempla como delitos la negación a brindar información publica y la divulgación de información privada por parte de una autoridad o funcionario/a público/a:

- Denegación de acceso a la información pública: la autoridad, funcionario o empleado público que fuera de los casos establecidos por ley, deniegue o impida el acceso a la información pública requerida, será sancionado con pena de seis a dos años de prisión, e inhabilitación de uno a dos años para ejercicio de empleo o cargo público.[81]

- Violación a la autodeterminación informativa: la autoridad, funcionario o empleado público que divulgue información privada o se niegue a rectificar, actualizar, eliminar, información falsa sobre una persona contenida en archivos, ficheros, banco de datos, o

78 Nicaragua "Código Penal" La Gaceta No. 232. 3 (diciembre, 2007), artículo 193.
79 Nicaragua "Código Penal", artículo 194.
80 Nicaragua "Código Penal", artículo 198.
81 Nicaragua "Código Penal", artículo 443.

> registros públicos, será sancionado con prisión de seis meses a dos años, e inhabilitación de uno a dos años para ejercer empleo o cargo público.[82]

En cuanto a las intervenciones telefónicas, el artículo 213 del Código Procesal Penal regula los supuestos en los que resulta procedente la intervención telefónica, mismos que recaen contra delitos pertenecientes a la criminalidad organizada; el artículo establece que

> ...la interceptación de telecomunicaciones sólo procede a solicitud expresa y fundada del Fiscal General de la República o del Director General de la Policía Nacional, quienes deben hacer constar que han valorado los antecedentes y que la intervención se justifica en su criterio, e indicarán también la duración por la que solicita la medida, así como las personas que tendrán acceso a las comunicaciones...

El o la juez, por su lado, determinará la procedencia de la medida y señalará la fecha en que debe cesar la intervención, la cual no puede durar mas de treinta días y en caso de ampliación, el mismo solo puede prorrogarse puna única vez y por un plazo igual[83].

En cuanto a las intervenciones de otro tipo de comunicaciones, el mismo Código Procesal Penal en su artículo 214[84] prevé:

> Procederá la interceptación de comunicaciones escritas, telegráficas y electrónicas, cuando se trate de los delitos a los que se refiere el artículo anterior, previa solicitud ante juez competente con clara indicación de las razones que la justifican y de la información que se espera encontrar en ellas. La resolución judicial mediante la cual se autoriza esta disposición deberá ser debidamente motivada.

La apertura de comunicación será realizada por el juez y se incorporará a la investigación aquellos contenidos relacionados con el delito.

La intervención de las comunicaciones telefónicas y la interceptación de comunicaciones escritas o telegráficas, constituyen una intromisión de los órganos de persecución penal del Estado en el libre ejercicio del derecho fundamental de las personas reconocido en el artículo 26 de la Constitución Política, cuya finalidad consiste en averiguar la verdad, por su relación con un hecho delictivo[85]. Se puede hablar de ilicitud de la intervención de las comunicaciones cuando no se hayan respetado las disposiciones que los artículos 213 y 214 establecen; en caso contrario, se estaría incurriendo en prácticas que el mismo Código Penal considera como delitos.

82 Nicaragua "Código Penal", artículo 444.

83Nicaragua "Código Procesal Penal", artículo 213.

84 Nicaragua "Código Procesal Penal", artículo 213.

85 María Moreno Castillo. "La intervención de las comunicaciones telefónicas y la interceptación de comunicaciones escritas, telegráficas y electrónicas como medios de prueba en el nuevo proceso penal". *Revista de Derecho* (2012), 180.

Por otro lado, la libre autodeterminación informativa, aparte de estar ligada al derecho a la privacidad, tiene sus riesgos en cuanto a la libertad de crear aquellos espacios de difusión de nuestra información, complementándolo con la creación de nuevas herramientas que contribuyan a mantener el anonimato de nuestra información. Los artículos 245 y 246 del Código Penal tipifican los delitos de destrucción de registros informáticos sin especificar si esto podría llevarse a cabo previo o durante un proceso judicial, así como el uso de programas destructivos que podrían ser utilizados en perjuicio de todo aquel o aquella ciudadana que adquiera o ponga en circulación programas o instrucciones informáticas que a discrecionalidad del operador de justicia se pueden considerar como "destructivos" que puedan causar perjuicio a los registros, programas o a los equipos de computación, lo que se incurre en una pena de uno a tres años de prisión.

Una interpretación errada de esta disposición puede conllevar a limitar o restringir el uso de herramientas de privacidad en el contexto de la privacidad digital; en una posible injerencia a las comunicaciones o privacidad, el uso de alguna herramienta que se validara como "destructiva", se podría incurrir en delito según lo establecido en el artículo 246 del Código Penal. Sin embargo, y como se mencionaba anteriormente, lo que no está impedido de hacer no está prohibido, y mas aún están indirectamente protegidos bajo el derecho a la libertad de expresión y la privacidad.

2.3.1.2. Normas sobre inteligencia y contrainteligencia

Los ataques cibernéticos están dando lugar a nuevos tipos de conflicto, no solo entre atacantes y una nación, sino también entre el Estado que persigue controlar la infraestructura electrónica e informática, así como las redes de comunicación de sus propios ciudadanos.

La reforma al Código Militar de Nicaragua establece en su artículo 2 inciso 15 que el Ejército de Nicaragua tendrá el control de las comunicaciones y de los puntos de comunicación, así como el espectro radio eléctrico y satelital, que además serán propiedad del Estado, reafirmando el nuevo rol de seguridad nacional del Ejército. En un análisis previo a la reforma al Código Militar, realizado por el Instituto de Estudios Estratégicos y Políticas Públicas, se expresaba que el espacio digital en manos del Ejercito de Nicaragua no abandona el control que en su momento dicha institución pueda realizar en torno a la privacidad de los y las ciudadanos nicaragüenses.[86]

El reciente anteproyecto de Ley de Promoción y Desarrollo de la Red Nacional de Servicios de Telecomunicaciones de Banda Ancha, define la ciberseguridad como el conjunto de herramientas, políticas, conceptos, medidas de seguridad, directrices, enfoques de gestión de riesgos, acciones, formación, aseguramiento y tecnologías que pueden utilizarse para proteger el entorno cibernético,

86 Irving Dávila. "Análisis jurídico comparado del código militar vigente y la iniciativa de reformas propuestas por la presidencia de la república a la Asamblea Nacional". (Managua: Ieepp, 2014), 9.

la organización y los activos de los usuarios, incluyendo los dispositivos: informáticos, personales, infraestructura, aplicaciones, servicios, sistemas de telecomunicaciones y la totalidad de la información transmitida y/o almacenada en el entorno cibernético.[87]

Por otro lado, el anteproyecto citado anteriormente establece que los operadores de servicios de banda ancha implementarán las medidas de seguridad y protección de la información del tráfico que aseguren la privacidad e inviolabilidad de las comunicaciones de los usuarios[88], cumpliendo con lo establecido en el Principio de Integridad de las Comunicaciones y Sistemas[89], el cual establece que no debe obligarse a proveedores de servicios o desarrolladores de "hardware" o "software" a desarrollar capacidades de vigilancia que comprometan la seguridad de las comunicaciones y los dispositivos. Sin embargo, esta función positiva se contrapone con lo establecido en el mismo anteproyecto de ley, donde se establece que el control de navegación en internet será ejercido por el mismo Estado a través de entidades que no son autónomas, ejerciendo vigilancia nacional a través de instituciones de control (TELCOR y Ejército de Nicaragua).

Por su lado, la Ley de Protección de Datos Personales exige el consentimiento previo del titular del derecho para recopilar datos, someterlos a tratamiento automatizado y cederlos, aunque con excepciones. Una de ellas es la que tiene que ver con el tratamiento de datos personales con fines de defensa o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia.[90]

De acuerdo a la ley, los datos personales tienen un uso excepcional. En primer lugar, los datos recolectados para fines administrativos tienen un periodo máximo de cinco años de almacenamiento y están sujetos al régimen general de dicha norma. Sin embargo, los datos colectados y el tratamiento de los mismo con fines de defensa nacional y seguridad pública a cargo de órganos de inteligencia del Ejército de Nicaragua y la Policía Nacional, queda limitado a lo necesario para el estricto cumplimiento de las misiones legalmente establecidas por la Constitución Política y las leyes en la materia.[91]

2.3.1.3. Normas en el sector de telecomunicaciones

La Ley General de Telecomunicaciones y Servicios Postales tiene por objeto la regulación de los servicios de telecomunicaciones y servicios postales, así como el establecimiento de derechos y deberes de los usuarios y de las operadoras, en condiciones de calidad, equidad, seguridad y el desarrollo planificado

87 Anteproyecto de Ley. "Ley de Promoción y Desarrollo de la Red Nacional de Servicios de Telecomunicaciones de Banda Ancha". (Nicaragua: Mayo, 2015),artículo 4.

88 Anteproyecto de Ley. "Ley de Promoción y Desarrollo de la Red Nacional de Servicios de Telecomunicaciones de Banda Ancha". (Nicaragua: Mayo, 2015), artículo 24.

89 Necessary and Proportionate, "Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones", https://es.necessaryandproportionate.org/text (consultado: 20 agosto, de 2015).

90 Nicaragua "Ley de Protección de Datos Personales", artículo 24.

91 Nicaragua "Ley de Protección de Datos Personales", artículo 24.

y sostenido de las telecomunicaciones. La ley garantiza y protege la privacidad y la inviolabilidad de la correspondencia y las comunicaciones y la seguridad de la información transmitida.[92]

Por su lado, el artículo 68 de la Ley General de Telecomunicaciones considera como infracción muy grave quien interfiera o intercepte intencionalmente los servicios de telecomunicaciones, afecte su funcionamiento e incumpla las leyes, reglamentos, tratados, convenios o acuerdos internacionales de telecomunicaciones en los cuales Nicaragua es parte.[93]

2.3.1.4. Normativas de acceso a la información o transparencia

Además de los convenios internacionales firmados y ratificados por Nicaragua, la legislación interna se ha ido adecuando lentamente a dichos instrumentos, las intenciones legislativas de protección y tutela efectiva del derecho a la privacidad emprendidas desde el año 2007, no han sido suficientes para la protección y regulación del derecho. En junio de ese mismo año se aprueba la Ley de Acceso a la Información Pública[94], la cual se crea para fortalecer el ejercicio de la democracia, visto desde la promoción de la participación ciudadana activa. Algunos de los principales alcances que esta ley reforzó son: 1) El *habeas data*; 2) El principio de transparencia, y 3) El principio de acceso a la información pública.

La Ley 621 regula el principio de transparencia bajo el entendido que las entidades sometidas al imperio de la ley, a través de sus oficiales gubernamentales, funcionarios y servidores públicos, están en el deber de exponer y someter al escrutinio de los ciudadanos la información relativa a la gestión pública y al manejo de los recursos públicos que se les confían.

2.3.1.5. Otras normas relacionadas al tema

La Ley de Protección de Datos Personales, en su artículo 8, determina cuatro categorías de datos: datos personales sensibles, datos personales relativos a la salud, datos personales informáticos y datos personales comerciales, las que tendrán diferentes características y su recolección y procesamiento girará en dependencia del caso. Las personas o instituciones responsables de los ficheros donde se almacenen estas cuatro categorías deberán implementar medidas de seguridad para el resguardo de la información, así como medidas técnicas y organizativas para un mejor control con el fin de evitar filtración de información, adulteración, pérdida y demás riesgos a que se encuentre expuesta la información almacenada en los ficheros[95], lo que va en apego al precepto constitucional de no ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia.

92 Nicaragua "Ley General de Telecomunicaciones y Servicios Postales" La Gaceta No. 154 (18 agosto, 1995), artículo 2.
93 Nicaragua "Ley General de Telecomunicaciones y Servicios Postales", artículo 68.
94 Nicaragua "Ley de Acceso a la Información Pública" La Gaceta No 118 (22, junio 2007).
95 Nicaragua "Ley de Protección de Datos Personales", artículo 9.

El contenido del capitulo V de la Ley 787 hace referencia al control institucional, creado para la aplicabilidad y cumplimiento legislativo de dicha ley. Se crea la Dirección de Protección de Datos Personales adscrita al Ministerio de Hacienda y Crédito Público, que tiene como función principal crear el registro de ficheros de datos personales, manteniendo la información actualizada y completa de los responsables con rango de confidencialidad, como medida de protección de las garantías individuales de las y los ciudadanos consagrados en la Constitución Política.[96]

Administrativamente, la Ley de Protección de Datos Personales establece un procedimiento de inspección, el cual estará en función de inspectores previamente autorizados y acreditados por la Dirección de Protección de Datos Personales que la misma ley establece.

La acción de protección de datos personales deberá presentarse ante la Dirección de Protección de Datos Personales (DIPRODAP). Recibida la solicitud de acción de protección de datos, se dará traslado de la misma al responsable del fichero de datos para que, en el plazo de quince días hábiles, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que tenga a bien.

Como todo proceso administrativo, posterior a la admisibilidad de la solicitud de acción de protección de datos la DIPRODAP, citará a las partes a un proceso de conciliación entre el titular de los datos y el responsable del fichero de datos. De llegarse a un acuerdo de conciliación entre las partes, este se hará constar por escrito y tendrá efectos vinculantes. La solicitud de acción de protección de datos personales quedará sin efectos y la DIPRODAP verificará el cumplimiento del acuerdo respectivo.[97]

La Ley de Firma Electrónica, a pesar de ser una Ley referida al comercio electrónico, se retoma para fines del presente estudio en vista que es el único instrumento jurídico nicaragüense que define la encriptación como el acto de utilizar una clave única antes de intercambiar información,[98] opera siempre en relación con soportes informáticos y el fin que persigue es primordialmente el de cualificar o incrementar la eficacia probatoria de los soportes electrónicos, al vincular directamente al firmante con el documento que se emite, haciendo constar que el contenido ha sido transmitido voluntariamente, y por lo tanto da la seguridad de que quien envía el mensaje es el autor del mismo, permitiendo así que se dé la identificación de las partes y la integridad en el documento.

96 Nicaragua “Ley de Protección de Datos Personales”, artículo 29 y 30.
97 Nicaragua “Reglamento a la Ley de Protección de Datos Personales” La Gaceta No. 200 (2012), artículo 40 y 41.
98 Nicaragua “Ley de firma electrónica” La Gaceta No. 165(2010), artículo 3.

2.3.2. Sobre allanamientos y registros

2.3.2.1. Plazo de las intervenciones

La diligencia de allanamiento deberá practicarse entre las seis de la mañana y las seis de la tarde. Podrá procederse a cualquier hora cuando el morador o su representante consienta o en los caso sumamente graves y urgentes, en los que los jueces resolverán en un plazo máximo‡ de una hora las solicitudes planteadas por el fiscal o el jefe de la unidad policial a cargo de la investigación. Deberá dejarse constancia de la situación de urgencia en la resolución que acuerda el allanamiento.[99] La solicitud de allanamiento, secuestro o detención contendrá‡ la indicación de las razones que la justifican, el lugar en que se realizará y la indicación de los objetos, sustancias o personas que se espera encontrar en dicho lugar.[100]

2.3.2.2. Allanamiento por orden judicial

1. La resolución judicial que autoriza el allanamiento, secuestro o detención deberá contener:
2. El nombre del juez y la identificación de la investigación o, si corresponde, del proceso;
3. La dirección exacta del inmueble y la determinación concreta del lugar o los lugares que habrán de ser registrados;
4. El nombre de la autoridad que habrá‡ de practicar el registro;
5. La hora y la fecha en que deba practicarse la diligencia;
6. El motivo del allanamiento, secuestro o detención, que sea‡ razonado adecuadamente expresando con exactitud el objeto u objetos, o personas que se pretenden buscar o detener, y,
7. En su caso, del ingreso nocturno.

Si durante la búsqueda del objeto, sustancia o persona para la cual fue autorizado el allanamiento, se encuentran en lugares apropiados para la búsqueda autorizada, otros objetos, sustancias o personas relacionados con esa u otra actividad delictiva investigada, estos podrán ser secuestrados o detenidos según corresponda sin necesidad de ampliación de la motivación de la autorización.[101]

Respecto a las formalidades de allanamiento, se requiere una copia de la resolución judicial que

99 Nicaragua "Código Procesal Penal", artículo 217.
100 Nicaragua "Código Procesal Penal", artículo 218.
101 Nicaragua "Código Procesal Penal", artículo 219.

autoriza el allanamiento y el secuestro, la cual será entregada a quien habite o posea el lugar donde se efectúe o, cuando esté ausente, a su encargado, y a falta de este, a cualquier persona mayor de edad que se halle en el lugar. Se preferirá a los familiares del morador. Respecto a la intimidad de las personas, la diligencia se practicará procurando afectar lo menos posible este derecho.

De dicha diligencia de allanamiento se levantará un acta para hacer constar la observancia de las regulaciones legales. Cuando no se encuentre a nadie, ello se hará constar en el acta. Practicando el registro, en el acta se consignará el resultado.[102]

2.3.3. Supervisión pública

La interceptación de telecomunicaciones solo procede a solicitud expresa y fundada del Fiscal General de la República o del Director General de la Policía Nacional, quienes deben hacer constar que han valorado los antecedentes y que la intervención se justifica en su criterio, e indicarán también la duración por la que solicita la medida, así como las personas que tendrán acceso a las comunicaciones.[103]

Por su lado, el juez determinará la procedencia de la medida, por resolución fundada, y señalará en forma expresa la fecha en que debe cesar la interceptación, la cual no puede durar más de seis meses, salvo en los casos de extrema gravedad que la ley no da a conocer en los que el juez, mediante resolución fundada, disponga una prórroga por una sola vez por un plazo igual.[104]

Todas las actuaciones para la intervención, así como la instalación y remoción de los medios técnicos necesarios, deberán hacerse con pleno conocimiento del fiscal encargado, levantándose un acta de lo actuado que deberá entregarse al Ministerio Público.

De acuerdo al esclarecimiento de la verdad, la Policía Nacional podrá delegar a uno de sus miembros para que perciba las comunicaciones directamente en el lugar de la intervención e informe lo que corresponda a sus superiores y al Ministerio Público.

El levantamiento de la intervención se llevará cabo por resolución judicial, a solicitud del fiscal o de la Policía Nacional, aún antes del vencimiento del plazo originalmente ordenado, cuando se cumplieran los propósitos de investigación previstos.

El juez ordenará la destrucción del material grabado una vez que se haya dictado con firmeza el sobreseimiento o sentencia de no culpabilidad. En caso de desestimación, falta de merito o archivo de

102 Nicaragua “Código Procesal Penal”, artículo 220.
103 Nicaragua “Código Procesal Penal”, artículo 213.
104 Nicaragua “Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados”, capítulo VIII, artículo 62.

la causa, el Fiscal General de la República y el Director General de la Policía Nacional deberán explicar y justificar fehacientemente al juez las razones por la cual no se utilizó la información obtenida y el juez ordenará su destrucción definitiva.[105]

105 Nicaragua "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados", capítulo VIII, artículo 64.

3. Marco legal nacional y su adecuación a los estándares internacionales

Desde antes de los ataques del 11 de septiembre de 2001 en los Estados Unidos de Norteamérica, la mayoría de los gobiernos del mundo emprendieron un proceso de transición en el manejo y uso de las comunicaciones digitales y en la modernización de las tecnologías y técnicas de vigilancia. Ahora es mas sencillo, por un lado, almacenar y analizar grandes cantidades de información rápidamente y a bajo costo, y por otro lado, la mayoría de nuestras comunicaciones se transmiten a través de terceros que pueden tener acceso a la misma. Además, cada vez que usamos el teléfono celular o internet revelamos voluntariamente una gran cantidad de información que agregada revela con quiénes nos comunicamos, por cuánto tiempo y desde dónde. Esta información, también conocida como "metadatos" o "datos sobres nuestras comunicaciones", puede llegar a revelar nuestras asociaciones políticas y sociales, condición médica, orientación sexual, información tan sensible como el contenido mismo de las comunicaciones. Estos cambios tecnológicos afectan profundamente nuestro derecho a la vida privada y, sin los controles necesarios, violentarían diversas libertades básicas. Muchos Estados están buscando la aprobación de legislaciones que norman y regulan las actividades de vigilancia de forma desproporcionada e innecesaria en una sociedad democrática y que, al mismo tiempo, justifican y alientan estas prácticas para aumentar aún más la persecución y el sufrimiento de defensores y defensoras de derechos humanos y debilitar su legítimo trabajo, reduciendo así su capacidad para proteger los derechos de otras personas.

Actualmente, las fronteras físicas han sido sustituidas por una gigantesca red de comunicación virtual, lo que nos permite ampliar la posibilidad de comunicarnos y transmitir información con dos o más personas en puntos geográficos diferentes y a bajo costo. Según el Consejo de Derechos Humanos de la Organización de las Naciones Unidas, mediante resolución A/HRC/20/L.13[106] adoptada el 29 de junio de 2012 sobre la promoción, protección y disfrute de los derechos humanos en internet; tener acceso a internet y estar conectado es un derecho humano, así como también es parte de la cultura informática de esta era; sin embargo, no debemos menospreciar que estos servicios y posibilidades técnicas son suministradas y soportadas por empresas público y/o privadas y, que el acceso a dichos servicios de comunicación virtual demanda los datos personales del usuario.

106 Organización de las Naciones Unidas. "Promoción, Protección y Disfrute de los Derechos Humanos en Internet" (20º período de sesiones del Consejo de Derechos Humanos, resolución A/HRC/20/L.13 del 29 de junio, 2012), 2.

Los recientes avances de la Oficina del Alto Comisionado para los Derechos Humanos sobre la protección y promoción del derecho a la privacidad en las comunicaciones digitales[107], así como los avances del sistema interamericano de derechos humanos,[108] demuestran el interés de los países de la región latinoamericana en "revertir" lo acontecido a inicios de los años dos mil, adecuando sus legislaciones al derecho internacional de los derechos humanos, protegiendo principalmente el derecho a la intimidad y a la libertad de expresión, y Nicaragua no ha sido la excepción. Sin embargo, estos esfuerzos no resultan suficientes para evitar la criminalización de organizaciones sociales, periodistas, comunicadoras y comunicadores, técnicos y técnicas en comunicaciones digitales y defensores y defensoras de derechos humanos en el ejercicio de sus funciones; al contrario, se presenta una dilación de la justicia en casos de violaciones a los derechos humanos o injerencias a la vida privada, entre otras.

En el ámbito internacional, diversos instrumentos regulan y reconocen el derecho a la privacidad. Al respecto, la Declaración Americana de los Derechos y Deberes del Hombre de 1948[109] establece, en su artículo V, que "toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar."

Por su parte, la Declaración Universal de Derechos Humanos[110] norma, en su numeral 12, el derecho a la privacidad estableciendo que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ...Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."

A raíz de las dos declaraciones mencionadas, se produjo la adopción de tres tratados internacionales: El Pacto Internacional de Derechos Civiles y Políticos (PIDCP)[111], el Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC)[112],de 1966; y la Convención Americana sobre Derechos Humanos[113] de 1969, siendo el PIDESC el instrumento que Nicaragua no ha firmado ni ratificado.

Tanto el PIDCP como la Convención, en sus artículos 17 y 11 respectivamente, reconocen como derecho fundamental la privacidad, referida como el respeto a la honra y el reconocimiento de la dignidad humana.

107 Organización de las Naciones Unidas. "El Derecho a la Privacidad en la era digital" (27º período de sesiones del Consejo de Derechos Humanos, resolución A/HRC/27/37 del 30 de junio, 2014).

108 Inter-American Commission on Human Rights. "Annual Report of the Office Of the Special Rapporteur for Freedom Of Expression" (Organization of American States, 2013), 477-530.

109 Organización de Estados Americanos, *Declaración Americana de los Derechos y Deberes del Hombre 1948*. (Colombia: OEA, 1948), artículo V.

110 Asamblea General de las Naciones Unidas, *Declaración Universal de Derechos Humanos 1948*. (París: Naciones Unidas, 1948).

111 Asamblea General de las Naciones Unidas, *Pacto Internacional de Derechos Civiles y Políticos 1966*. (Estados Unidos de Norteamérica: Naciones Unidas, 1966).

112 Asamblea General de las Naciones Unidas, *Pacto Internacional de Derechos Económicos, Sociales y Culturales 1966*.

113 Organización de Estados Americanos, *Convención Americana sobre Derechos Humanos 1969*.

Artículo 17.[114]

1. 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.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Artículo 11.[115]

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Como se mencionó en el capitulo anterior, el artículo 138 constitucional de Nicaragua[116], establece que los instrumentos internacionales aprobados por el Congreso Nacional confieren efectos legales, dentro y fuera del país, una vez que hayan entrado en vigencia internacionalmente. En otras palabras, los tratados, convenios y/o instrumentos ratificados y aprobados por Nicaragua a nivel internacional, forman parte del derecho vigente.

El artículo 13.3 de la Convención Americana de Derechos Humanos establece que:

> No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

Los mecanismos indirectos de restricción se ocultan detrás de acciones aparentemente legítimas que, sin embargo, son adelantadas con el propósito de condicionar el ejercicio de la libertad de expresión de los individuos. Cuando eso sucede, se configura una violación del artículo 13.3 de la Convención. Como lo ha sostenido la Corte Interamericana de Derechos Humanos, resulta violatorio de la libertad de expresión "todo acto del poder público que implique una restricción al derecho de buscar, recibir y difundir informaciones e ideas, en mayor medida o por medios distintos de los autorizados por la misma Convención"[117].

114 Asamblea General de las Naciones Unidas, *Pacto Internacional de Derechos Civiles y Políticos 1966*. (Estados Unidos de Norteamérica: Naciones Unidas, 1966),artículo 17.

115 Organización de Estados Americanos, *Convención Americana sobre Derechos Humanos 1969*, artículo 11.

116 Nicaragua "Constitución Política", artículo 138, Inc. 12.

117 Corte Interamericana de Derechos Humanos, La Colegiación obligatoria de periodistas, párr. 55.

Interpretando el artículo 13.3 citado, la Declaración de Principios sobre Libertad de Expresión, o mejor conocidos como los principios de Chapultepec, establecen en su principio número 5 que:

> [l]a censura previa, interferencia o presión directa o indirecta sobre cualquier expresión, opinión o información difundida a través de cualquier medio de comunicación oral, escrito, artístico, visual o electrónico, debe estar prohibida por la ley. Las restricciones en la circulación libre de ideas y opiniones, como así también la imposición arbitraria de información y la creación de obstáculos al libre flujo informativo, violan el derecho a la libertad de expresión". Y en su principio 13 indica que "la utilización del poder del Estado y los recursos de la hacienda pública; la concesión de prebendas arancelarias; la asignación arbitraria y discriminatoria de publicidad oficial y créditos oficiales; el otorgamiento de frecuencias de radio y televisión, entre otros, con el objetivo de presionar y castigar, o premiar y privilegiar a los comunicadores sociales y a los medios de comunicación en función de sus líneas informativas, atentan contra la libertad de expresión y deben estar expresamente prohibidos por la ley.

En este sentido, la Corte Interamericana ha afirmado que el artículo 13.3 impone a los Estados una obligación de garantía frente a las relaciones entre particulares que puedan derivar en limitaciones indirectas de la libertad de expresión: "el artículo 13.3 de la Convención Americana impone al Estado obligaciones de garantía, aún en el ámbito de las relaciones entre particulares, pues no sólo abarca restricciones gubernamentales indirectas, sino también 'controles […] particulares' que produzcan el mismo resultado". Leído en conjunto con el artículo 1.1 de la Convención Americana, ello implica, en criterio del tribunal, que se viola dicho instrumento no solo cuando el Estado impone a través de sus agentes restricciones indirectas sobre la circulación de ideas u opiniones, sino también cuando ha permitido que el establecimiento de controles particulares genere una restricción de la libertad de expresión[118].

Con el objetivo que los Estados emprendan acciones sistemáticamente de cumplimiento efectivo respecto a las obligaciones contraídas en la firma de una diversidad de instrumentos internacionales en materia de protección de derechos humanos, principalmente aquellos correspondiente a la privacidad y la libertad de expresión, es que nacen los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Los 13 Principios están firmemente enraizados en el derecho internacional de los derechos humanos y la jurisprudencia comparada[119]. Al ser ello así, los tratados, normativa jurídica y decisiones judiciales que interpretan los 13 Principios son aplicables a Nicaragua, constituyéndose en una fuente de doctrina relevante para analizar las prácticas de vigilancia a nivel nacional.

118 Corte Interamericana de Derechos Humanos, La Colegiación obligatoria de periodistas, párr. 48.

119 Necessary and Proportionate, "Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones".

Los 13 Principios han sido citados en el informe del Grupo de Revisión del Presidente sobre Inteligencia y Tecnologías de las Comunicaciones de los Estados Unidos, el informe de la Comisión Interamericana de Derechos Humanos,[120] el reporte sobre anonimato y cifrado del Relator de Libertad de Expresión de Naciones Unidas,[121] el reporte de privacidad en la era digital del Alto Comisionado de Derechos Humanos de Naciones Unidas,[122] entre otros. A continuación se dan a conocer dos principios sobre los que Nicaragua deberá ahondar con respecto a la aplicación y futuro cumplimiento de acuerdo a su contenido. Posteriormente se analizan a profundidad once principios de acuerdo a lo normado por Nicaragua.

No debe obligarse a proveedores de servicios o desarrolladores de "hardware" o "software" a desarrollar capacidades de vigilancia que comprometan la seguridad de las comunicaciones y los dispositivos. No debe exigirse la retención indiscriminada y masiva de datos de las personas que usan dichos servicios ni debe comprometerse el derecho a la expresión anónima a través del establecimiento de obligaciones de identificación o prohibiciones respecto del uso de herramientas de cifrado y otras para proteger la identidad y la seguridad de las personas, sus comunicaciones y sus dispositivos.

Garantías contra el acceso ilegítimo y recurso efectivo: La vigilancia ilegal de comunicaciones por parte de actores públicos o privados debe ser castigada mediante sanciones civiles y penales suficientes y adecuadas. Los denunciantes de información de interés público (*whistleblowers*) deben ser protegidos por la ley de cualquier repercusión legal por el incumplimiento de su deber de secrecía.

3.1. Legalidad

Legalidad: Cualquier limitación a los derechos humanos debe ser prescrita por ley. La ley debe ser pública y cumplir un estándar de claridad y precisión suficientes para prever el alcance de las medidas de vigilancia de comunicaciones.

De acuerdo a este principio, cualquier injerencia a un derecho fundamental, para fines de este estudio, a la vida privada y libertad de expresión debe estar avalada por una norma constitucional o legal para que tenga validez como prueba dentro del proceso penal. En ese sentido, conforme a lo descrito en el capítulo anterior, la norma nicaragüense que autorice las vigilancias de las comunicaciones esta prescrita por ley, es pública y cumple con un estándar de claridad y precisión suficiente para prever el alcance de las medidas de vigilancia de comunicaciones.

120 Inter-American Commission on Human Rights. "Annual Report of the Office Of the Special Rapporteur for Freedom Of Expression".

121 Organización de las Naciones Unidas. "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión".

122 Organización de las Naciones Unidas. "El Derecho a la Privacidad en la era digital" .

En 1987, el constituyente nicaragüense consciente de las facilidades que existen en las sociedades modernas de atentar contra la vida privada de las personas, da una respuesta jurídica a través del reconocimiento constitucional del derecho en el Titulo IV, correspondiente a los "Derechos, deberes y garantías del pueblo nicaragüense", Capítulo I, en el que se establece una serie de derechos humanos entre los que se encuentran los denominados "derechos de la personalidad" entendidos como "aquellos que conceden un poder a las personas para proteger la esencia del ser humano y sus mas importantes cualidades"[123]. Así pues, el artículo 26 de la Constitución Política de Nicaragua establece este derecho humano; reconocido como la inviolabilidad del domicilio, su correspondencia y sus comunicaciones de cualquier tipo, nos conlleva a evaluar y analizar tal principio con escrupulosidad legal a las intervenciones telefónicas, en la que queda claro que los derechos de la personalidad si bien son derecho innato, personalísimo, extrapatrimonial, irrenunciable e inalienable, no son absolutos.

Por ello, ante la interrogante ¿es o no inconstitucional la intervención telefónica o interceptación de comunicaciones de cualquier tipo?, es importante aclarar que dada la naturaleza de los derechos humanos y con la característica no absolutista del derecho, el artículo 24 constitucional establece una restricción a favor del bien común y la seguridad de todos y todas las nicaragüenses, misma que deberá cumplir con el Principio de Legalidad, es decir, las normas que autoriza la vigilancia debe estar prescrita por ley.

3.2. Objetivo legítimo

Objetivo legitimo: Las leyes que establezcan medidas de vigilancia de las comunicaciones deben perseguir objetivos legítimos y no ser aplicada de manera discriminatoria.

La motivación de toda resolución en virtud de la cual se lleva a cabo una injerencia al derecho de la vida privada e inviolabilidad de domicilio debería ser una exigencia constitucional. La Constitución de Nicaragua no establece lo referido, lo que podría conllevar a una interpretación de la norma. Sin embargo, y ante una injerencia, el destinatario de la medida tiene el derecho a conocer cuáles son las razones por las que su derecho está siendo limitado y ademas en virtud de qué otros intereses se llevo a cabo dicha intervención.

El artículo 213 del Código Procesal Penal regula los supuestos en los que resulta procedente la intervención telefónica, lo que en su mayoría son delitos correspondientes al crimen organizado, del mismo modo indica quiénes están facultados para pedir la intervención – Fiscalía General de la República o del Director General de la Policía – los que deberán hacer constar que se han valorado

123 María Moreno Castillo. "La intervención de las comunicaciones telefónicas y la interceptación de comunicaciones escritas, telegráficas y electrónicas como medios de prueba en el nuevo proceso penal", 182.

los antecedentes y que la intervención se justifica. Por otro lado, la constancia deberá indicar la duración de la intervención y los nombres de las personas que tendrán acceso a las comunicaciones intervenidas.

Al juez corresponde determinar la procedencia de la medida a través de resolución fundada, es decir, explicando el proceso que conllevó tal medida. Señalará en forma expresa la fecha que debe cesar la interceptación, la que no debe sobrepasar los treinta días que podrán ser prorrogables por una sola ocasión con el mismo plazo de tiempo, según lo manda el artículo 213. Para los delitos contenidos en la Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados, la interceptación de comunicaciones se autorizará hasta por un plazo máximo de seis meses, salvo en los casos de extrema gravedad o de difícil investigación en los que el juez, mediante resolución fundada, disponga una prorroga de hasta seis meses mas[124]. Al respecto la Ley de Crimen Organizado, a diferencia del Código Procesal Penal, no indica que dicha prórroga podrá ser por una sola ocasión, dejando abierta la interpretación legal para los operadores de justicia, mismo que podría incurrir en violación a derechos humanos del procesado o imputado de hechos contenidos en la normativa antes mencionada.

3.3. Necesidad e idoneidad

Según el proceso penal nicaragüense, a los procesos solo se introducirán como medio de prueba las grabaciones de las conversaciones o parte de ellas, que, a solicitud del fiscal se estimen útiles para el descubrimiento de algún hecho delictivo. Como parte del proceso de defensa, el artículo 213 del Código Procesal Penal indica que el acusado puede solicitar se incluyan otras partes de las conversaciones que han sido excluidas como medida de defensa. Finalmente y posterior a la culminación del proceso, el juez ordenará la destrucción de las conversaciones que no fueron pertinentes al proceso.

Necesidad: Las vigilancias de las comunicaciones solo debe llevarse a cabo cuando la consecución del objetivo legítimo no pueda alcanzarse a través de métodos menos lesivos a los derechos humanos. La carga de demostrar dicha justificación le corresponde al Estado.

Idoneidad: Las medidas de vigilancia de comunicaciones deben ser apropiadas y capaces de conseguir el objetivo legítimo perseguido.

La Policía Nacional como institución a cargo de la interceptación de las comunicaciones, deberá remitir al órgano judicial que autorizó la medida todas las grabaciones originales, el cual tendrá que realizar un examen privadamente y después, con citación de la persona afectada, procederá a destruir

124 Nicaragua "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados", capítulo VIII, artículo 62.

o entregar a la Policía las grabaciones que no tengan relación con la causa, uniéndose las demás al expediente del proceso. El filtro de información es una función exclusiva del juez.

3.4. Proporcionalidad

En palabras mas simples, la proporcionalidad consiste en que la motivación de una resolución de interceptación de comunicación debe consagrarse en un juicio proporcional/ racional entre la limitación del derecho a la privacidad y el fin de investigación que se persigue.

Proporcionalidad: Las medidas de vigilancia solo deben autorizarse por una autoridad judicial independiente cuando exista un alto grado de probabilidad de que un delito grave o una amenaza específica, actual y comprobable a la seguridad nacional pueda materializarse. Las medidas de vigilancia adoptadas deben ser las menos invasivas posibles, lo cual implica que solamente se obtendrá, retendrá o utilizará la información relevante para la consecución del objetivo legítimo que justifica la autorización y por periodos de tiempo limitados.

Según el artículo 213 del Código Procesal Penal, la interceptación de comunicaciones, sean estas telefónicas o de cualquier otro tipo, tienen validez legal como medio de prueba únicamente para los delitos 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. Aunado a lo establecido en el ordenamiento de procedimiento penal, el artículo 3 de la Ley de Crimen Organizado enumera los delitos, sujetos a intervención telefónica.

Es importante destacar que el inciso 23 del artículo 3 de la ley hace referencia a los delitos cometidos tanto de funcionarios públicos como de particulares, por lo que las sanciones contenidas en el Código Penal referidas a aquellos delitos que tienen que ver con el uso de información reservada, fraude o la aceptación de ventaja por un acto cumplido u omisión podrán imponerse a un particular, evidencia la vulnerabilidad y contrariedad del principio de proporcionalidad. Pues la oportunidad de intervención, según lo establece la ley, se podrá otorgar cuando exista una amenaza grave a la seguridad del país y no necesariamente cuando un particular omita cierta información personal que él considera reservada, por lo que lo establecido en la ley es opuesto al fin de la misma.

Otro elemento que debe tomarse en consideración es la del sujeto pasivo de las intervenciones, pues se entiende que las mismas deben ser la de un procesado o imputado en el procedimiento penal por lo delitos antes mencionados, sin embargo, la intervención puede versar sobre personas no imputadas, siempre y cuando existan elementos de juicio suficientes para concluir que puede ser utilizado como medio de prueba en el proceso, menoscabando la esencia del derecho a la privacidad y de las libertades fundamentales de un tercero no directo del proceso.

3.5. Autoridad judicial competente

Autoridad judicial competente: las medidas de vigilancia de comunicaciones deben ser autorizadas de manera previa, o inmediata con efecto retroactivo en casos de emergencia, por una autoridad judicial competente, independiente e imparcial.

Según los principios, las decisiones relacionadas con la vigilancia de las comunicaciones deben ser realizadas por una autoridad judicial competente que sea imparcial e independiente. Al respecto, es quizás el principio que Nicaragua no cumple a cabalidad puesto que la misma autoridad que solicita la intervención a la autoridad judicial es la que interviene las comunicaciones.

En los casos de investigación de delitos que requieren de intervención de comunicaciones a solicitud expresa y fundada del Fiscal General de la República o del Director General de la Policía Nacional, los jueces de distrito de lo penal podrán autorizar a este el impedir, interrumpir, interceptar o grabar comunicaciones, correspondencia electrónica; otros medios radioeléctricos e informáticos de comunicaciones, fijas, móviles, inalámbricas y digitales o de cualquier otra naturaleza[125]. El juez de distrito de lo penal podrá ordenar la captación y grabación de las comunicaciones e imágenes entre presentes dentro del proceso penal.

Siendo el juez penal el encargado de autorizar las intervenciones, la resolución que autorice, deberá contener:

1. la indicación expresa del hecho que se pretende esclarecer,
2. el nombre del dueño o del usuario del equipo de comunicación por intervenir o del destinatario de la comunicación y su vínculo con los hechos,
3. el período durante el cual tendrá vigencia la medida ordenada, que no podrá ser mayor de seis meses y,
4. el nombre de la oficina y de los funcionarios responsables autorizados para realizar la intervención[126].

Lo contradictorio en torno a este principio, y según lo establece el artículo 214 del Código de Procedimiento Penal, la apertura de la comunicación o la interceptación de la comunicación debe

125 Nicaragua "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados", capítulo VIII, artículo 62.

126 Nicaragua "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados", capítulo VIII, artículo 63.

ser realizada por el juez competente; sin embargo, en la práctica la autoridad que tiene la capacidad humana y técnica para llevar a cabo dicha función es la Policía Nacional, a través de su unidad de investigaciones criminales. En este sentido, podríamos decir que la Policía Nacional, además de ser la institución que solicita al juez la interceptación, es la autoridad que la lleva a cabo, función que no versa sobre lo establecido en los principios internacional sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones.

3.6. Debido proceso

Según la Constitución Política de Nicaragua, todo procesado tiene derecho, en igualdad de condiciones, a ser juzgado sin dilaciones por tribunal competente establecido por ley, a ser sometido al juicio oral y público y por jurado en los casos determinados por la ley, a que se le dicte sentencia dentro de los términos legales y a no ser procesado ni condenado por acto u omisión que, al tiempo de cometerse, no esté previamente calificado en la ley de manera expresa e inequívoca como punible, ni sancionado con pena no prevista en la ley[127].

Debido proceso: Las decisiones de autorización de medidas de vigilancia de comunicaciones deben garantizar el debido proceso. Lo anterior implica que, cuando para la consecución del objetivo legítimo, y en particular, la protección de la vida de una persona, sea necesaria la secrecía de la medida o su aplicación inmediata, existan otras medidas que garanticen la protección de los intereses del afectado como lo es la designación de una persona o institución que asuma representación general de sus intereses en la audiencia o que la autorización judicial se lleve a cabo con efecto retroactivo.

3.7. Notificación del usuario

En base a este principio es importante destacar que los artículos 213 y 214 del Código de Procedimiento Penal y 62 y 63 de la Ley de Crimen Ogranizado, no indican en sus enunciados la notificación que deberían hacerle al usuario de que se le interceptara la comunicación, sin embargo, y según lo establecido en el artículo 141 y 142 de la normativa de procedimiento penal, las notificaciones se realizan a todo aquel acto delictivo contenido en dichas normas.

Notificación del usuario: Las personas afectadas por medidas de vigilancia de comunicaciones deben ser notificadas de ello y tener acceso a los materiales que pretendan ser o hayan sido obtenidos. La notificación podrá diferirse cuando la misma ponga en riesgo la consecución del objetivo legítimo o exista un riesgo inminente de peligro a la vida humana.

127 Nicaragua "Constitución Política", artículo 34, incisos: 2, 3, 11.

Respecto a la responsabilidad de los proveedores de servicios, la Ley de Crimen Organizado establece que

> las empresas privadas o públicas prestadoras de los servicios de comunicación telefónica, informática o de otra naturaleza electrónica [...] deberán prestar todas las condiciones y facilidades materiales y técnicas necesarias para que las intervenciones sean efectivas, seguras y confidenciales y estarán obligadas a permitir que se usen sus equipos e instalaciones para la práctica de las diligencias de investigación antes previstas[128].

3.8. Transparencia y supervisión pública

Transparencia: El Estado debe publicar de manera periódica información estadística sobre las medidas de vigilancia encubierta llevadas a cabo. Como mínimo debe publicar el número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad, tipo y propósito.

Supervisión pública: Deben establecerse mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones. Dichos mecanismos de supervisión independiente deben tener la autoridad para acceder a toda la información potencialmente relevante para evaluar el uso legítimo de medidas de vigilancia de comunicaciones.

En materia de vigilancia de las comunicaciones, el ordenamiento jurídico nicaragüense no especifica el principio de transparencia. En la práctica tal principio es invisible, puesto que el numero de intervenciones telefónicas y el desglose de las solicitudes son inexistentes.

Respecto a la interferencia de los proveedores de servicios, el artículo 65, parte de la Ley de Crimen Organizado, regula que las empresas que prestan los servicios deben llevar un registro oficial de los usuarios o clientes que utilicen los servicios, los que podrán ser requeridos por autoridad competente para fines de investigación, persecución y proceso penal. Es importante dar a conocer que ningún ordenamiento jurídico nacional establece un tiempo determinado de recopilación y almacenamiento de información de parte de las empresas prestadoras de servicios, lo regulado indica que todo tratamiento de datos personales estará sujeto al consentimiento de su titular, ello conlleva a no proporcionar a las instituciones públicas y privadas mayor información o datos personales que aquellos que sean adecuados, proporcionales y necesarios para la prestación de los mismos[129].

En Nicaragua, la autoridad para conducir vigilancia por parte del Estado esta normado y procede únicamente en casos excepcionales, es decir, cuando exista un peligro inminente para la seguridad de los ciudadanos nicaragüense, entendidos estos como aquellos delitos que forman parte de la

128 Nicaragua "Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados", capítulo VIII, artículo 65.

129 Nicaragua "Ley de Protección de Datos Personales", artículos 9-10.

criminalidad organizada. Es necesario revisar y adecuar la normativa nacional a lo establecido a nivel internacional, principalmente lo referido a los principios de transparencia, supervisión publica y notificación del usuario, pues las debilidades a pesar de ser pocas podrían traer riesgos y desafíos por la inexistencia o mal aplicabilidad de la norma. La interpretación de parte de los órganos judiciales siempre es un reto para Nicaragua pues la profesionalización en temas tan técnicos como la vigilancia de la comunicaciones no es quizás un tema de interés para el sistema.

3.9. Garantías para la Cooperación Internacional

Garantías para la Cooperación Internacional: Si para llevar a cabo las medidas de vigilancia es necesaria la cooperación internacional, esta debe llevarse a cabo a través de acuerdos de asistencia judicial recíproca (MLAT) en los que debe garantizarse que los mismos no sean utilizados para burlar las restricciones internas relacionadas con la vigilancia de las comunicaciones.

Nicaragua ha firmado y ratificado la Convención Interamericana sobre Asistencia Mutua en Materia Penal (MLAT en inglés).[130] El artículo segundo de la Convención es la única disposición de este tratado aplicable a materia de vigilancia. El artículo indica que los Estados parte *se* prestarán asistencia mutua en investigaciones, juicios y actuaciones en materia penal referentes a delitos cuyo conocimiento sea de competencia del Estado requiriente al momento de solicitarse la asistencia. Esta Convención se aplica únicamente a la prestación de asistencia mutua entre los Estados partes; sus disposiciones no otorgan derecho a los particulares para obtener o excluir pruebas, o para impedir la ejecución de cualquier solicitud de asistencia.

3.10. Conclusiones preliminares

En Nicaragua, el derecho a la vida privada está entendida bajo un concepto que se encuentra relacionado con la prohibición de que una persona sea objeto de injerencias arbitrarias hacia ella misma o la de su familia, su domicilio o su correspondencia, así como de ataques a su honra o a su reputación, contando con la protección de la ley contra tales injerencias o ataques, lo que supone un reconocimiento positivo del artículo 26 de la Constitución Política de Nicaragua que protege la autonomía del individuo en su ámbito privado.

En cuanto al mecanismo constitucional para hacer efectivo el derecho a la vida privada, el recurso de *habeas data* enfrenta un reto en cuanto al ejercicio de cumplimiento del mismo. Dicho recurso constitucional como configuración procesal de la acción de protección de datos personales presupone

130 OEA, "Inter-American Convention on Mutual Assistance in Criminal Matters" (1992), http://www.oas.org/juridico/english/treaties/a-55.html (consultado: 14 octubre, 2015)

un equilibrio a favor del ciudadano frente a las y los propietarios de los ficheros de datos, donde se almacena información personal. Sin embargo, la pasividad de los usuarios frente al cumplimiento de su derecho no creará precedente normativo de dicho mecanismo proteccionista.

A pesar que en Nicaragua la legislación no profundiza sobre la protección del cifrado y el anonimato, exceptuando aquel referido al comercio electrónico, estos pueden estar protegidos bajo lo establecido en el precepto constitucional numero 32, el cual establece que ningún ciudadano o ciudadana nicaragüense está obligado a hacer lo que la ley no mande, ni impedida de hacer lo que ella no prohíbe.

Por otro lado, el artículo 213 y 214 del Código Procesal Penal regulan los supuestos en los que resulta procedente la intervención telefónica, mismos que recaen contra delitos pertenecientes a la criminalidad organizada, así como el procedimiento para llevar a cabo la intervención. Sin embargo, podrían llegar a constituirse una intromisión de los órganos de persecución penal del Estado en el libre ejercicio del derecho fundamental de las personas reconocido en el artículo 26 de la Constitución Política si no se respetan las disposiciones que dichos artículos establecen.

En el año 2014, el Consejo de Derechos Humanos de Naciones Unidas aceptó aprobar la resolución A/HRC/27/37 sobre "El Derecho a la privacidad en la era Digital"[131] propuesta por Alemania, Brasil y México, en la que se identifica un reto: el rápido crecimiento de las tecnologías, aunado al Estado como ente de control frente a los ciudadanos lleva a la vigilancia y la recopilación de datos, sin respetar el derecho a la privacidad de las personas. Con esto se da un paso para el resguardo de la privacidad y la no vulneración de derechos humanos y se insta a los Estados a respetar las normativas internacionales respecto a la no vigilancia de sus ciudadanos y ciudadanas. El siglo XXI crea nuevos desafíos para los Estados y para todos/as los/las ciudadanos, las exigencias y contexto actual en Nicaragua demanda un mayor control y, en vista de ello, se necesita una ciudadanía informada que no tenga restricción de información ni sea perseguida por los propios gobiernos.

131 Alto Comisionado de las Naciones Unidas para los Derechos Humanos. "El derecho a la privacidad en la era digital". (Washington: Naciones Unidas, 2014)

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

El presente apartado recoge las principales experiencias e inquietudes del sector técnico y de defensa de derechos humanos de Nicaragua relacionadas con el derecho a la privacidad digital, en internet y en las telecomunicaciones, mismo que esta dividido en tres apartados referidos a: los aspectos metodológicos e instrumentos utilizados para la recopilación de información de las personas entrevistadas; las experiencias de técnicos y técnicas, defensores y defensora de derechos humanos sobre la vigilancia en las comunicaciones, anonimato, cifrado, allanamientos, entre otros; y las principales dudas, desafíos y desconocimiento sobre el marco jurídico existente en el país en materia de privacidad digital en el contexto de internet y las telecomunicaciones que pudiesen encaminar a criminalizar la labor que realiza dicho sector.

4.1. Metodología

En torno a este capitulo, la metodología utilizada fue de carácter cualitativo y su alcance fue exploratorio considerando la poca información manejada por las y los entrevistados sobre el marco legal y jurídico existente en Nicaragua sobre el derecho a la privacidad digital, en internet y en las telecomunicaciones en el país.

Se diseñó un instrumento de entrevista de tipo semi-estructurado, el cual se aplicó a cuatros técnicas y técnicos comprometidos con la defensa de derechos humanos, tres de ellos pertenecientes a organizaciones de sociedad civil, activistas y en algunos de los casos integrantes y ex integrantes de la comunidad de software libre, una comunidad conformada por usuarios y desarrolladores informales que promueven el uso de aplicaciones digitales de libre adaptación a las necesidades del usuario.

Por otro lado, se realizaron cuatro entrevistas a defensores y defensoras de derechos humanos con amplia trayectoria en la defensa de los derechos de las mujeres, LGBTI, promoción de la democracia y acceso a la justicia a nivel nacional, las que permitieron valorar las experiencias, percepciones y desafíos en torno a la criminalización de su labor como defensores.

Otra herramienta de investigación empleada en el presente estudio consistió en la realización de un grupo focal que contó con una guía de preguntas generadoras de información previamente elaborada, con el objetivo de obtener información grupal, diversa y comparable al momento del análisis. Otra

herramienta de investigación empleada en el presente estudio consistió en la realización de un grupo focal que contó con la participación de cuatro personas, dos de las cuales eran de la misma organización, lo que dificultó la reflexión grupal, diversa y comparable.

Finalmente, la investigación contó con una etapa de validación, la que tuvo por objetivo validar, retroalimentar, presentar y complementar el proceso investigativo. En una sesión de un día los y las participantes, entre ellos técnicos, técnicas, defensores y defensoras de derechos humanos, así como conocedores del derecho, tuvieron la oportunidad de analizar por grupos los diferentes capítulos del estudio, alimentando y eliminando lo que consideraban pertinente desde su conocimiento.

Es importante señalar que antes y durante el período de elaboración del presente estudio, la intimidación, amenaza y criminalización de las personas que defienden derechos o son generadores de opinión pública se ha venido agudizando en la medida que se impone un modelo autoritario y dictatorial que utiliza la ley y la institucionalidad para atacar a quienes ubica como contrarios a sus intereses ideológicos, económicos y que representan la conciencia crítica desde la ciudadanía y el rol de defensa de los derechos ante los abusos.

Finalmente, es importante destacar que por el tipo de metodología utilizada no podemos afirmar y generalizar a partir de las respuestas dadas por las y los participantes, 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.

4.2. Experiencias

Lo expresado por las personas entrevistadas no solo testimonia las experiencias institucionales de hechos acontecidos, sino que narra cómo los constantes ataques les afectan directa o indirectamente, tanto en el ámbito personal como institucional, y todas señalan que en el imaginario colectivo se va tejiendo un régimen de riesgos que crea condiciones de vulnerabilidad para todos y todas en los distintos ámbitos de sus vidas.

4.2.1. Vigilancia

Conforme la información brindada en las entrevistas se analiza que 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. Sin embargo, las organizaciones y personas que realizan activismo de derechos humanos a través de otras formas alternativas como el ciberactivismo, señalan que los métodos que se utilizan son más sutiles, menos visibles y que están encaminados a ocasionar miedo o provocar la autocensura. Tanto las personas entrevistadas como las y los participantes del grupo focal señalan que la vigilancia se ejerce a diario en todo el país de

forma controlada, es decir, las instituciones tanto públicas como privadas utilizan mecanismos de seguridad sofisticados. Entre los mecanismos mas utilizados identificados señalan el "*phishing*"[132] y la inyección de archivos ejecutables como los XSS Cross-site scripting[133]. Por otro lado, reconocen la utilización de sistemas de denegación de servicios (limitación de acceso a páginas de instituciones públicas), y fuga de información a través de Eavesdropping[134], Exploits[135], Spoofing[136] y Malware[137].

De acuerdo a los y las entrevistadas, los perpetradores de los actos de vigilancia no pueden verse de forma aislada en sus ataques, sino como aquel acto donde todos responden a un modelo o sistema que mantiene una estructura de poder, a través de la cual se impone el miedo al ejercer la defensa de todo derecho.

Cuando se hace el ejercicio de identificar posibles perpetradores a partir de hechos concretos que han vivido o conocen, señalan a miembros de la Policía Nacional, el Ejército de Nicaragua, grupos de choques partidarios, la 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 (ISP por sus siglas en inglés), oficiales de Migración y Extranjería, diputados/as, magistrados/as, líderes políticos del partido de gobierno en los barrios y periodistas oficialistas.

Entre las personas técnicas entrevistadas se señalaba que la vigilancia realizada en Nicaragua es dirigida a acallar el accionar de las organizaciones, por ejemplo el caso de una organización defensora de recursos naturales que se opone rotundamente a la construcción del mega proyecto de construcción del canal, cuyo sitio web fue bloqueado desde su proveedor ISP[138]

Desde el sector técnico existe mucha expectativa en torno al anteproyecto de ley de banda ancha, el que en palabras de los técnicos "...pondría en riesgo la privacidad de la información, por lo que cualquier violación a derechos a través de esta vía sería inminente."[139]

132 Mejor conocido como la suplantación de identidad en el mundo informático. Es caracterizado como una herramientas abusiva por intentar adquirir información confidencial de forma fraudulenta.

133 Es la vulnerabilidad mas conocida en el mundo digital, principalmente de sitios Web que utilizan código JavaScript. En español se conoce como "secuencias de ordenes en sitios cruzados".

134 Termino designado a herramientas diseñadas para las escuchas telefónicas.

135 Es un fragmento de de datos o secuencia de comandos y/o acciones de un software, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

136 Técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de datos en una comunicación.

137 Software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

138 Técnico 1, Managua, Nicaragua, junio 2015.

139 Técnico 2, Managua, Nicaragua, julio 2015.

Otro tipo de vigilancia caracterizada como indirecta por las y los asistentes al grupo focal, ejercida por grupos desestabilizadores de la democracia en el país, 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 que estos mismos grupos han elaborado para desprestigiar el trabajo que realiza el sector de defensa de los derechos humanos.[140]

En cuanto a la vigilancia, el mayor riesgo lo constituye la propia vulnerabilidad en que se encuentran las y los defensores de derechos humanos tanto a título individual como institucional, ya sea por el desconocimiento de herramientas y mecanismos de protección, o bien, por la cultura de negación y resistencia al cambio que los/as lleva a resistirse a incorporar el uso de herramientas digitales seguras, a pesar de haber sido capacitados por técnicos y técnicas en dichas herramientas.

4.2.2. Anonimato y cifrado

Desde el sector de defensoría de derechos humanos, la mayoría de personas entrevistadas aceptan que las medidas implementadas en anonimato y cifrado se quedan en nivel de precauciones ante una posible vigilancia. El factor recursos económicos fue mencionado como una limitante en la implementación de procesos de resguardo de información, "no es suficiente con mejorar las contraseñas y cifrar información si no se cuentan con equipos apropiados, pues esto depende de los limitados recursos para dotarse de los mismos."[141]

Uno de los casos relativo a privacidad digital sistematizado en Nicaragua por Fundación Acceso, refleja que la encriptación o cifrado de información es un asunto que trastoca susceptibilidades ante el sistema judicial, pues ante una resolución dictada en enero de 2009 contra una Organización de Sociedad Civil por el Ministerio Público la premeditación de encriptar información conlleva a la obstrucción de la justicia, violentando a toda luz lo regulado en el precepto constitucional número 26, el cual establece la inviolabilidad del domicilio, su correspondencia, y cualquier otro tipo de comunicaciones.

En cuanto al sector técnico, el anonimato y cifrado se lleva cabo de forma regular tanto desde el ejercicio que realiza institucionalmente como a título individual, haciendo uso de herramientas y aplicaciones para el resguardo de la información, de las comunicaciones, y de la navegación segura.

4.2.3. Allanamientos y requisas

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

140 Página elaborada por supuestos aliados al gobierno: http://www.nicaleaks.com/
141 Defensora 1, Managua, Nicaragua, junio 2015.

proceso acelerado de agudización de la crisis de gobernabilidad democrática en el país, cuestionada por la legitimidad de las instituciones.

El Movimiento Autónomo de Mujeres (MAM), El Centro Nicaragüense de Derechos Humanos (CENIDH), el Centro de Investigación de la Comunicación (CINCO) y mas recientemente la Federación Nacional de Cooperativas (FENACOOP) son organizaciones que han sufrido allanamientos y requisas arbitrarias que han conllevado a la suspensión de personería jurídica como fue el caso de FENACOOP[142]. El proceso de allanamiento es similar en todos los casos mencionados: ordenes judiciales sin fundamentación jurídica, realizado en horario no hábil, con violencia y con el objetivo de extraer libros contables, computadoras y eliminar cualquier información que coyunturalmente pudiese ser opuesta al discurso del gobierno de Daniel Ortega.

Uno de los casos sistematizados por Acceso denota la mala intención e injerencia de parte de las autoridades que tienen bajo su función los allanamientos domiciliares, de citar a la parte agraviada a ser ella quien digitara su contraseña para acceder a la información de su computadora requisada. Los y las entrevistadas mencionan que tal citación la hacen con la intención de intimidar y ahondar en otros aspectos que no es objeto del allanamiento.

La recomendación 114.88 del Examen Periódico Universal 2014 se centra en "velar por que se respeten los derechos de los defensores de los derechos humanos y porque las autoridades judiciales investiguen de manera exhaustiva e imparcial los actos de amenaza, intimidación o violencia cometidos en su contra", sin embargo, y según los entrevistados

> cuando tales injerencias, allanamientos y requisas son ejercidas por las mismas instituciones, prevalece un ambiente de impunidad que denota una conducta propia de política estatal diseñada para proteger a los violadores de los derechos humanos pretendiendo cubrirlos con un manto de olvido[143]

4.2.4. Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones

Según los entrevistados, la estigmatización de ser defensor o defensora de derechos humanos, así como el trabajar en una organización sin fines de lucro (ONG), constituye un riesgo directo de criminalización sumado a las constantes campañas de desprestigio y la sistemática descalificación, "nos catalogan de agentes del imperialismo, las supuestas afiliaciones partidarias o de representación política ideológica, entre muchas otras."[144]

142 Información disponible en: http://confidencial.com.ni/fenacoop-denuncia-disolucion-de-hecho/ (consultado: 23 septiembre, 2015)
143 Defensor 3, Managua, Nicaragua, agosto 2015.
144 Defensora 1, Managua, Nicaragua, junio 2015.

Tanto en las entrevistas como en el grupo focal, se hizo mención a que la vigilancia a la labor que se realiza abarca los perfiles personales en redes sociales, "es un modus operandi contratar a gente "Stalker" para intimidar y en el peor de los casos extraer información hackeando tus cuentas personales."[145]De acuerdo a una de las personas técnicas entrevistadas, muchas de estas acciones pueden ser ciertas y otras quizás provengan de criminales cibernéticos que buscan tener ganancias financieras, por ello sugiere

> diferenciar entre las fuentes de información y cómo evaluarlas para determinar si son reales; por ello es necesario ayudar a las personas a navegar exitosamente entre el gran historial de información en la web, las habilidades para orientar a las personas a descubrir, usar y evaluar las fuentes de información que posibiliten su desarrollo tanto personal como profesional[146].

Sobresale el temor y angustia entre las y los entrevistados expresando que, al momento de entablar conversaciones se auto-censuran, lo que podría catalogarse como un mecanismo de criminalización debido a la intimidación, "a nivel individual tengo cuidado con el contenido de mis mensajes. Que no sea información que tenga que ver con cuestiones políticas. Mis posiciones políticas las trato de ventilar en tono respetuoso, no caer en adjetivar, en dirección moderada pero crítica."[147]

4.3 Inquietudes

4.3.1. Vigilancia

A pesar de que la mayoría de las y los entrevistados tienen conocimiento de los supuestos bajo los cuales se puede interceptar o intervenir una comunicación, es generalizado el discurso de que en Nicaragua "la interpretación de la ley beneficia a quien ostenta el poder" por lo tanto y aunque la intervención no forme parte de los supuesto, "el poder se lo inventa."[148]

Técnicos y técnicas señalaron que la Ley de Protección de Datos Personales no los protege, pues los mecanismos a los cuales podrían acceder para proteger sus datos no son una realidad debido a la falta de institucionalidad que la misma ley manda crear. Por otro lado, se desconoce la existencia de normativa jurídica que apunte a proteger la labor que realizan. Destaca la preocupación de que en el ejercicio de su labor sean demandados o enjuiciados por violación ilícita de comunicaciones, acceso abusivo a un sistema informático, robo, daño en bien ajeno, estafa, piratería, entre otros, lo que podría ser respondido con un marco jurídico claro y protector en la defensa del derecho a la privacidad digital.

145 Defensor 2, Managua, Nicaragua, junio 2015.
146 Técnico 2, Managua, Nicaragua, julio 2015.
147 Defensora 4, Managua, Nicaragua, junio 2015.
148 Técnico 2, Managua, Nicaragua, julio 2015.

Nicaragua se preocupa más por garantizar el desarrollo económico sostenible del país otorgando seguridad jurídica a los inversionistas nacionales y extranjeros de las TIC, que a sus propios ciudadanas y ciudadanos que contribuimos al desarrollo social del país.[149]

En cuanto al anteproyecto de ley de banda ancha existe mucha incertidumbre e incluso ya se habla de posibles repercusiones de la vigilancia que puede llegar a ejercer el Estado a través de los ISP. Para los y las entrevistadas del sector técnico, crear una comisión multidisciplinaria donde sean incluidos para debatir el mismo daría mayor credibilidad al proceso de formación de ley; sin embargo, se cuestionan el alcance que la futura ley pueda conllevar para la criminalización en el uso de herramientas seguras.

"Proteger la información de las personas con quienes trabajamos, muchas veces no garantiza la seguridad física de dicha persona y es en parte impotencia de no poder ayudar a garantizar el derecho primario de todo ser que es la vida."[150]

4.3.2. Anonimato y cifrado

Las inquietudes respecto a este acápite surgen desde dos vías. Por un lado, en cuanto a la legalidad del uso de un simple firewall o de encriptar información, pues según las y los entrevistados puede darse el caso de que el gobierno, a través de su facultad como ente regulador de comunicaciones, requiera mis datos. Por otro lado, la imposición de una sanción o pena bajo el supuesto de que si cifro o navego de forma anónima obstruyo la justicia.

4.3.3. Allanamientos y requisas

Como se mencionaba anteriormente, los allanamientos realizados a organizaciones de sociedad civil en Nicaragua se han dado de forma arbitraria, lo que ha llevado a las organizaciones a conocer sobre los procedimientos bajo los cuales debe llevarse a cabo un allanamiento; sin embargo, desconocen si entre el procedimiento de allanamiento cabe la requisa de información reservada, computadoras, servidores, celulares o cualquier otro dispositivo electrónico.

4.3.4 Otros mecanismos para la criminalización vinculada al derecho a la privacidad digital, en internet y en las telecomunicaciones

La existencia de diversidad de normativa que directa e indirectamente aborda la privacidad digital limita el completo conocimiento para el sector técnico y de defensa de derechos humanos. Para las y los entrevistados preocupa la posible investigación proveniente de una actividad delictiva, ¿es la

149 Técnico 1, Managua, Nicaragua, junio 2015.
150 Técnica 3, Managua, Nicaragua, julio 2015.

ley de crimen organizado una ley que se puede utilizar en el contexto de privacidad digital? ¿qué mecanismos existen para hacer efectivo mi derecho a la privacidad digital y proteccionismo de datos? Estas son algunas de las inquietudes respecto al ordenamiento jurídico.

Para finalizar, es importante destacar que conforme a las entrevistas se evidencia que, en general, las organizaciones y personas defensoras de derechos humanos no tienen diseñados o previstos planes de seguridad o protocolos de protección ante situaciones concretas. Existe una contradicción entre la claridad de conocer los riesgos del contexto y la resistencia a retomar mecanismo de protección o seguridad personales o institucionales que puedan mitigar o reducir los mismos.

5. Conclusiones nacionales

El contexto de Nicaragua durante el período de elaboración del presente estudio marca un acelerado deterioro del sistema democrático. Prevalece un clima de inseguridad jurídica y deterioro del respeto de los derechos de la ciudadanía lo que origina mayores riesgos para el desempeño de la labor de las personas que defienden derechos fundamentales.

El nivel de las amenazas, intimidación e intentos de criminalización han evolucionado hacia la agudización de las mismas y están encaminadas a implantar en la población nicaragüense el miedo, donde se estigmatiza el trabajo de toda persona defensora de los derechos humanos, pues la coloca en mayor vulnerabilidad ante los perpetradores que gozan de total impunidad para actuar.

En Nicaragua, el derecho a la vida privada, es entendida bajo un concepto que está relacionado con la prohibición de que una persona sea objeto de injerencias arbitrarias hacia ella misma o hacia su familia, su domicilio o su correspondencia, así como de ataques a su honra o a su reputación, contando con la protección de la ley contra tales injerencias o ataques, lo que supone un reconocimiento positivo del artículo 26 de la Constitución Política de Nicaragua, que protege la autonomía del individuo en su ámbito privado, mas no así el reconocimiento tácito y expreso del derecho a la privacidad bajo un contexto digital.

La adecuación de la normativa nacional respecto a los estándares internacionales en el contexto de la privacidad digital es un desafío para Nicaragua. 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 procedimiento que dicha norma manda a crear resulta un indicador de precariedad de acceso a la justicia en Nicaragua.

En cuanto a la percepción del sector técnico y de defensa de derechos humanos es generalizada la actitud de que en Nicaragua las acciones de criminalización (interceptaciones de comunicaciones, campañas de desprestigio, hostigamientos, amenazas, entre otras) se realizan de hecho y no de derecho. En el último año, los allanamientos ilegales de parte de la Policía Nacional a organizaciones sociales, la criminalización de la protesta, las detenciones ilegales a miembros de organizaciones de sociedad civil y la cancelación de personería jurídica a movimientos sociales surtieron un aumento, con la intención de intimidar y acallar voces disidentes del actual gobierno.

Finalmente, es importante destacar que el rápido crecimiento de las tecnologías, aunado al Estado como ente de control (en alianza con el sector privado) frente a los ciudadanos lleva a la vigilancia

y la recopilación de datos, sin respetar el derecho a la privacidad de las personas. El siglo XXI crea nuevos desafíos para los Estados y para todos/as los/las ciudadanos, las exigencias y contexto actual en Nicaragua demanda un mayor control, y en vista de ello, se necesita una ciudadanía informada, que no tenga restricción de información, ni sea perseguida por los propios gobiernos.

Bibliografía

Libros

Bertoni, Eduardo. *Solicitud de Audiencia temática sobre el Impacto de Internet en la Defensa y el Ejercicio de los Derechos Humanos ante la Comisión Interamericana de Derechos Humanos*. Argentina: Universidad de Palermo, 2014. 4-5.

Centro Nicaragüense de Derechos Humanos. *Nicaragua ante la segunda revisión del Examen Periódico Universal 2014*. Nicaragua: CENIDH, 2014. 20.

Cerda Silva, Alberto J. "Protección de datos personales y prestación de servicios en línea en América Latina". En *Hacia una internet libre de censura. Propuestas para América Latina*, 165-180. Buenos Aires, Argentina: CELE, UP, 2012. 1.

Comisión Interamericana de Derechos Humanos. *Segundo Informe sobre la Situación de las Defensoras y Defensores de los Derechos Humanos en las Américas 2011.* Estados Unidos de Norteamérica: CIDH, 2011, párr. 57.

COPREDEH. *El derecho a la privacidad en la era digital*. Informe presentado por el gobierno de Guatemala a la Oficina del Alto Comisionado para los Derechos Humanos. Ginebra: OACDH, 2014.

Cortés Castillo, Carlos. "Las llaves del ama de llaves: la estrategia de los intermediarios en internet y el impacto en el entorno digital". En *Internet y derechos humanos. Aportes para la discusión en América Latina,* compilado por Eduardo Andrés Bertoni, 61-88. Buenos Aires, Argentina: CELE, UP, 2014.

Cortés Castillo, Carlos. "Vigilancia de la red: ¿Qué significa monitorear y detectar contenidos en internet". En *Internet y derechos humanos. Aportes para la discusión en América Latina,* compilado por Eduardo Andrés Bertoni, 35-60. Buenos Aires, Argentina: CELE, UP, 2014. 3.

Lara Gálvez, J. Carlos; Jaramillo Gajardo, Paula; Rayman Labrin, Danny. *El Derecho a la Privacidad en Latinoamérica: normativa y jurisprudencia. Documento preparatorio para presentación en audiencia ante la Corte Interamericana de Derechos Humanos*. (Santiago de Chile: Derechos Digitales, 2014). 48-147.

Organización de Estados Americanos, *Tren Micro. Tendencias en la seguridad cibernética en América Latina y el Caribe y Respuestas de los gobiernos*. Washintong: OEA, 2013. 1.

Unidad de Protección a Defensoras y Defensores de Derechos Humanos en Guatemala. *Criminalización en contra de Defensores y Defensoras de Derechos Humanos. Reflexión sobre Mecanismos de Protección 2009*. (Guatemala: UDEFEGUA, 2009). 7.

Villegas Carrasquilla, Lorenzo. "Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet". En *Hacia una internet libre de censura. Propuestas para América Latina*, 125-164. Buenos Aires, Argentina: CELE, UP, 2012.

Revistas

Lara, Juan Carlos y Vera, Francisco. “Responsabilidad de los prestadores de servicios de internet”. En *Policy Papers,* n° 03 (2014).

Tesis

Obando Quezada, Adriana. “El Habeas Data como mecanismo de Defensa de los Derechos Humanos”. Tesis de Licenciatura, Universidad Centroamérica, Nicaragua, 2010.

Legislación nacional

Instituto Nicaragüense de Telecomunicaciones y Correos. Acuerdo Administrativo 001-2004 del 8 de Enero de 2004.

Nicaragua. “Código de Organización, Jurisdicción y Previsión Social Militar”. La Gaceta No. 41 (3, marzo 2007).

Nicaragua. “Código Penal”. La Gaceta No. 232 (3, diciembre 2007).

Nicaragua. “Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados.” La Gaceta, No. 199 y 200 (19-20, octubre 2010).

Nicaragua. “Ley de Protección de Datos Personales”. La Gaceta, No. 61 (29, marzo 2012).

Nicaragua. “Ley de Reforma Parcial a la Constitución Política de la República de Nicaragua”. La Gaceta No. 26 (08, febrero 2014).

Nicaragua. “Ley de Seguridad Democrática de la República de Nicaragua”. La Gaceta No.750 (23, diciembre 2010).

Nicaragua. “Ley General de Telecomunicaciones y Servicios Postales”. La Gaceta No. 154 (18, agosto 1995).

Nicaragua.“Ley de Amparo con reformas incorporadas”. La Gaceta No 61 (08, abril 2013).

Jurisprudencia

Alto Comisionado de las Naciones Unidas para los Derechos Humanos. “El derecho a la privacidad en la era digital”. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos de 30 de junio de 2014.

Asamblea General de las Naciones Unidas. *Pacto Internacional de Derechos Civiles y Políticos 1966*. (New York, Asamblea General de las Naciones Unidas, 1966), artículo 17.

Organización de Estados Americanos, *Convención Americana sobre Derechos Humanos 1969*. (Costa Rica: Organización de Estados Americanos, 1969), artículo 11.

Organización de Estados Americanos. Declaración Americana de los Derechos y Deberes del Hombre 1948. (Colombia: Organización de Estados Americanos, 1948), artículo V.

lqVRomqgghOAGr2Ov9VxK/Eb

r79b8K3hVurUKZnLI8ag

RXlyjpbQioxwxvU1jeZpj86Z/sIDhll vy5WvrrskJ4A1dbQioxwx

CPRXlyjpbQioxwxvU1jeZpj86Z/sIDhll vy5

wxvConclusiones/sID

sCPRXlyjpbQioxwxvU1jeZpj86Z/sIDhll vy5WvrrskJ4A1dbQiox

Luciana Peri
Katitza Rodríguez

CONCLUSIONES COMPARATIVAS SOBRE EL DERECHO A LA PRIVACIDAD EN LA NORMATIVA CENTROAMERICANA[2]

1. 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*.

1.1 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.[3]

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

2 Las presentes conclusiones han sido elaboradas con la información contenida en los diferentes capítulos que integran la investigación "¿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."

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

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".[4] 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 […].[5]

Igualmente, la Constitución de Guatemala[6] 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.[7]

Por su parte, la Constitución Política de Nicaragua reconoce el derecho a la vida privada y a la de su familia.[8] 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.[9]

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).

1.2 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.

4 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)

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

6 Guatemala "Constitución Política de Guatemala" Asamblea Nacional Constituyente (1985), artículo 25.

7 Corte de Constitucionalidad. *Inconstitucional General Total. Expediente 1201-2006.* (Guatemala, 2007)

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

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

La Constitución de El Salvador reconoce expresamente el derecho de protección de la morada y la protección de la correspondencia y telecomunicaciones.[10] De la misma manera, la Constitución de Nicaragua reconoce el derecho a la inviolabilidad del domicilio, correspondencia y comunicaciones de todo tipo.[11]

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 cierta limitaciones al derecho.[12] Ese reconocimiento fue luego tomado por la Constitución Federal de Centroamérica de 1824, y su reforma de 1835.[13] 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.[14]

Actualmente, la Constitución vigente de Guatemala reconoce expresamente la inviolabilidad de la vivienda[15] y la inviolabilidad de la correspondencia, documentos y libros.[16] En el 2007, la Corte Constitucional de este 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.[17]

---

10 Artículo 23 de la Constitución de la República de El Salvador: 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 autorizase 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 (...)¨

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

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

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

14 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."

15 Artículo 23 de la Constitución de Guatemala: 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.

16 Artículo 24 de la Constitución de Guatemala: 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 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.

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

Por su parte, la Constitución y la jurisprudencia de Honduras también protegen la inviolabilidad del domicilio[18] y de las comunicaciones.[19] 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.[20]

1.3. 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".[21] 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."[22] Los datos personales generalmente se entienden como aquellos datos que pueden identificar o llegar a identificar a una persona determinada.

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:[23]

---

18 Artículo 99 de la Constitución de de Honduras: 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.

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

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

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

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

23 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 (consultado: 16 noviembre, 2015)

> 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.[24]

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.[25]

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*.[26]

1.4. 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.[27] 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.

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

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

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

27 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.

Si bien países en Centroamérica reconocen expresamente este derecho,[28] 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.

2. 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.[29]

28 Nicaragua "Constitución Política de Nicaragua" Asamblea Nacional (1948), artículo 26,
29 Información tomada del capítulo "Nicaragua" de esta misma publicación, escrito por Mireya Zepeda Rivera.

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.[30]

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).[31]

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 actividades del crimen organizado con énfasis en la narcoatividad 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.[32]

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"[33] y constituir "una herramienta esencial

30 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)

31 El Salvador "Código Procesal Penal" Asamblea Legislativa (2009), articulo 176.

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

33 El Salvador "Ley Especial para la Intervención de las Comunicaciones" Asamblea Legislativa (2010), artículo 1.

en la lucha contra la criminalidad tradicional, y sobre todo contra la criminalidad organizada o no convencional";[34] es decir que la ley tiene aplicabilidad en la investigación de cualquier delito.[35]

En El Salvador se especifica que podrá hacerse uso de la facultad de la ley en un listado que incluye 14 delitos[36], 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.[37]

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.

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

34 El Salvador "Ley Especial para la Intervención de las Comunicaciones", artículo 1.

35 Información tomada del capítulo "Honduras" de esta misma publicación, escrito por Edy Tábora Gonzales.

36 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.

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

- 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 Infornet 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 Personales[38], 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.[39]

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.

Aunado a esto, para garantizar el resguardo y protección de los datos personales, en el año 2013 se reforma la Ley de Amparo[40] en la que se adiciona el recurso de *habeas data* con el objetivo de

38 Nicaragua "Ley de Protección de Datos Personales" La Gaceta No. 61 (2012)
39 Nicaragua "Ley de protección de datos personales", artículo 1.
40 Nicaragua "Ley de Amparo"La Gaceta del08, abril 2013.

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.[41]

El recurso de *habeas data* hace referencia al derecho legítimo del individuo a "la libre disposición de los datos personales"[42]. 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 informativa[43] (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).[44]

41 Nicaragua "Ley de Amparo" artículo 6.

42 Osvalo Alfredo Gozaíni, "Hábeas Data. Protección de los datos personales. Doctrina y Jurisprudencia". (Argentina: Rubinzal Culzoni Editores, 2011), 67.

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

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

3. 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 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 público[45].

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

4. 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.[46]

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. [47]

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,[48] el informe de la Comisión Interamericana de Derechos Humanos,[49] el Reporte sobre Anonimato y Cifrado del Relator sobre Libertad de Expresión de Naciones Unidas,[50] y el Reporte de Privacidad en la Era Digital del Alto Comisionado de Derechos Humanos de Naciones Unidas,[51] entre otros.

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

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

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

49 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)

50 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)

51 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.[52]

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.[53]

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.[54]

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.[55]

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

52 Información tomada del capítulo “El Salvador” de esta misma publicación, escrito por Marlon Hernández Anzora.
53 Información tomada del capítulo “El Salvador” de esta misma publicación, escrito por Marlon Hernández Anzora.
54 Información tomada del capítulo “El Salvador” de esta misma publicación, escrito por Marlon Hernández Anzora.
55 Información tomada del capítulo “Guatemala” de esta misma publicación, escrito por Jorge Jiménez Barillas y Hedme Sierra-Castro.

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.[56]

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 sea el mínimo, se debe contar con transparencia en las estadísticas de las limitaciones a este derecho y con verdaderos mecanismos independientes de supervisión. [57]

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 sospechosa 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.[58]

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.[59]

56 Información tomada del capítulo “Guatemala” de esta misma publicación, escrito por Jorge Jiménez Barillas y Hedme Sierra-Castro.
57 Información tomada del capítulo “Guatemala” de esta misma publicación, escrito por Jorge Jiménez Barillas y Hedme Sierra-Castro.
58 Información tomada del capítulo “Honduras” de esta misma publicación, escrito por Edy Tábora Gonzales.
59 Información tomada del capítulo “Nicaragua” de esta misma publicación, escrito por Mireya Zepeda Rivera.