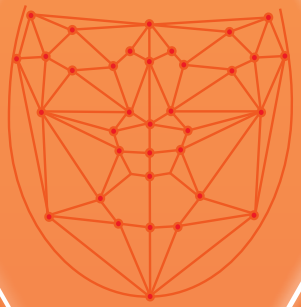
Vigilancia
en Centroamérica

Un análisis de las condiciones legales, políticas, económicas y tecnológicas que podrían propiciar la vigilancia ilegal en El Salvador, Guatemala, Honduras y Nicaragua



FUNDACIÓN Acceso

Fundación Acceso, 2020
Borrador inicial: Rodrigo Baires.
Edición: Larraitz Lexartza
Revisión de la versión inicial: Katitza Rodríguez.
Revisión: Tanya Lockwood y Rafael Bonifaz.

Disclaimer

Este capítulo hace referencia a diferentes aspectos - como condiciones jurídico-legales, aspectos políticos, aspectos económicos y aspectos tecnológicos - que pueden favorecer usos poco transparentes, innecesarios, ilegítimos o desproporcionados de los sistemas de vigilancia por parte de los Estados.

Es importante señalar que el hecho de que las condiciones sean favorables, no implica necesariamente que los usos mencionados estén ocurriendo. Sin embargo, las condiciones ya citadas, aunadas a la falta mecanismos de transparencia o supervisión pública, pueden propiciar abusos.

El objetivo principal de este estudio es hacer un esfuerzo inicial de recabar y recopilar información, datos y condiciones, que puedan llamar la atención a la ciudadanía con el fin de elevar al debate público la falta de mecanismos de transparencia o supervisión pública en esta materia.

Toda la información recabada para este capítulo se obtuvo mediante revisión bibliográfica disponible públicamente y a través de entrevistas con actores clave que dieron su consentimiento para ser citados.

Agradecimientos

Agradecemos a Hivos y DDP su apoyo para la realización de esta investigación.

Índice

Introducción

Esta investigación nace de una preocupación de Fundación Acceso con respecto a la escasez de información sistematizada sobre las capacidades para la adquisición y el uso de algunas tecnologías de vigilancia en El Salvador, Guatemala, Honduras y Nicaragua.

Entre agosto 2018 y febrero del 2019, un equipo de trabajo de Fundación Acceso - con la colaboración de profesionales y personas defensoras de los derechos digitales de Centroamérica, así como de actores clave en la región - recopiló y sistematizó información pública y referencias bibliográficas. También se consideraron percepciones individuales y grupales, obtenidas a partir de entrevistas. Todo esto con el fin de identificar las capacidades jurídico-legales, políticas, económicas y tecnológicas para la adquisición y uso de algunas tecnologías de vigilancia en los cuatro países.

Estos cuatro ámbitos - las capacidades jurídico-legales, políticas, económicas y tecnológicas – han constituido las dimensiones de análisis del estudio. Cada dimensión de análisis cuenta con una serie de indicadores que nos permitieron recabar y analizar la información disponible y comprender de mejor manera el escenario regional con respecto a las capacidades de vigilancia de los Estados. Se trata de entender que la capacidad para desarrollar acciones de vigilancia puede verse favorecida por circunstancias de muy diferente carácter.

La primera dimensión, la relativa a lo jurídico-legal, parte de la premisa de que la legislación vigente en cada país puede ser un resguardo para el derecho de las personas a la privacidad. Sin duda, esto limitaría las posibilidades de realizar acciones de vigilancia desproporcionadas, innecesarias o ilegítimas. Sin embargo, en los últimos años no ha sido aislada la aprobación de normativa tendiente a favorecer enfoques de seguridad que podrían menoscabar el derecho a la privacidad, por carecer – entre otros - de los límites legales y políticos necesarios para evitar el socavamiento de los derechos humanos. Para realizar el análisis sobre la situación de los países seleccionados con respecto a esta dimensión se han considerado cuatro subdimensiones. A su vez, cada subdimensión cuenta con un indicador (Tabla 1). Estos cuatro indicadores buscan

recabar información, por un lado, sobre la protección que se provee en cada país al derecho a la privacidad, y por otro, sobre normativa que más bien podría menoscabar este derecho. Para ello, se indaga acerca de dicha protección a nivel constitucional y en los diferentes instrumentos internacionales que han ratificado los países. Asimismo, se realiza un análisis de normativa nacional de diferente carácter para determinar si es protectora de este derecho o si más bien abre la posibilidad de vulnerarlo.

La segunda dimensión, la política, cuenta con siete subdimensiones y nueve indicadores (Tabla 1). Busca analizar la forma en que se concibe el derecho a la privacidad desde diferentes poderes del Estado. Por un lado, se trata de dar un paso más allá del análisis del marco legal, para indagar acerca de los enfoques que se emplean en los planes de gobierno relativos a la seguridad y la ciberseguridad. Es decir, se busca valorar cuál es el enfoque de seguridad que se maneja en la práctica. También se recaba información sobre el uso de tecnologías de vigilancia para criminalizar o judicializar a personas defensoras de derechos humanos. Finalmente, se indaga acerca de los vínculos entre agentes estatales con entidades empresariales de ámbitos como las telecomunicaciones y la seguridad privada. En este caso, se parte del hecho de que la relación entre estas entidades y agentes estatales podrían, en ciertos lamentables casos, favorecer contubernios que permitan la infiltración de intereses privados en la agenda pública y el accionar del Estado.

La tercera dimensión, la económica, cuenta con dos subdimensiones y siete indicadores (Tabla 1). Esta dimensión se dedica a la identificación de las capacidades de los Estados para adquirir tecnologías de vigilancia. Concretamente, se busca identificar en los presupuestos nacionales y de las instituciones los rubros dedicados a la seguridad, entendiendo que estas tecnologías podrían adquirirse con dichas partidas. En este sentido, son además de particular relevancia las partidas presupuestarias dedicadas a gastos reservados. Se trata de líneas presupuestarias opacas que no permiten rastrear a que se dedican los recursos. Este tipo de partidas podrían prestarse fácilmente para la adquisición de tecnología de vigilancia, ocultando esta información a la opinión pública. Por otro lado, también se valoran aspectos relacionados con las empresas que proveen bienes y servicios vinculados a las tecnologías de vigilancia. Así, se consideran aspectos

como si existen contratos estatales con empresas proveedoras de este tipo de productos y la posibilidad que tienen los Estados de realizar estas adquisiciones.

Finalmente, la cuarta dimensión, la tecnológica, cuenta con siete subdimensiones y once indicadores (Tabla 1). Se trata, en términos generales, de valorar si los Estados cuentan con tecnología que, sin los controles adecuados, podría ser empleada para la vigilancia de manera desproporcionada o innecesaria. En este caso, se toman en cuenta en primer lugar casos concretos de vigilancia relevados por fuentes secundarias, como resultados de investigaciones o medios de prensa. Particularmente, se hace referencia a prácticas como el uso de malware, la realización de escuchas telefónicas o la vigilancia en Internet. Por otro lado, también se ha recabado información acerca de las solicitudes de información que realizan los Estados sobre usuarios de Internet a empresas como Facebook, Twitter o Google. Asimismo, se considera si los estados han adquirido tecnología para el reconocimiento biométrico o para la georeferenciación, u otras herramientas como drones o globos de vigilancia.

Uno de los mayores aprendizajes del proceso de investigación, es que siendo importante para la ciudadanía tener conocimiento sobre la adquisición y uso de tecnologías de vigilancia, la información al respecto no es de fácil acceso aunque sea de interés público.

Esperamos que esta investigación contribuya a ampliar líneas de investigación, y particularmente a proveer información valiosa para la ciudadanía y las organizaciones que trabajan en el ámbito de los derechos digitales y los derechos humanos. Esperamos que pueda ser una herramienta para fortalecer el monitoreo de las acciones de los Estados en cuanto a la adquisición y uso de tecnologías de vigilancia en la región.

Dimensión	Subdimensión	Indicador
Jurídico-legal	1.1 Protección de la privacidad a nivel constitucional	1.1.1 Nivel de protección de la privacidad en el país a nivel constitucional
	1.2 Tratados y Convenciones Internacionales	1.2.1 Nivel de implicación de instrumentos internacionales – Tratados, Acuerdos, Convenciones y otros - firmados por el país con relación a la privacidad
	1.3 Leyes, reglamentos, decretos y normativas nacionales	1.3.1 Nivel de aplicación, transparencia y control de leyes, reglamentos, decretos y normativas relacionados con el derecho a la privacidad (leyes de telecomunicaciones, leyes ciberseguridad, inteligencia de Estado (secreto de Estado), leyes antiterroristas, o reformas de ley con artículos que indican prácticas que protegen o vulneran la privacidad
	1.4 Normativa de seguridad nacional y ciberseguridad	1.4.1 Existencia de legislación relacionada con seguridad nacional y ciberseguridad
Política	2.1 Relación entre Estado, empresas y cámaras de telecomunicaciones	2.1.1 Nivel de relación entre el Estado, empresas y cámaras de telecomunicaciones
		2.1.2 Nivel de representación en cuanto a la relación entre el Estado, empresas y cámaras de telecomunicaciones
	2.2 Contratos entre el Estado y empresas de seguridad privada	2.2.1 Nivel de impacto de los contratos establecidos entre el Estados y empresas de seguridad privada
	2.3 Relación de actores estatales o políticos con las directivas de empresas de seguridad	2.3.1 Nivel de relación entre el Estado y empresas de seguridad privada
	2.4 Planes de Gobierno en vigencia en materia de seguridad nacional.	2.4.1 Planes de gobierno vigentes relacionados con la seguridad nacional y ciberseguridad que protegen o vulneran la privacidad
	2.5 Relación de los planes de seguridad nacional y ciberseguridad con la privacidad	2.5.1 Nivel de protección o vulneración de la privacidad de los planes de gobierno vigentes relacionados con la seguridad nacional y ciberseguridad
	2.6 Uso de tecnologías de vigilancia para criminalizar o judicializar	2.6.1 Casos en los que se usan tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos que ejercen sus derechos humanos y civiles
		2.6.2 Identificación de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos que ejercen sus derechos humanos y civiles
	2.7 Acuerdos bilaterales y multilaterales de cooperación en materia de seguridad	2.7.1 Existencia de acuerdos bilaterales y multilaterales de cooperación en materia de seguridad

Dimensión	Subdimensión	Indicador
Económica	3.1 Presupuestos nacionales destinados a seguridad y gastos reservados	3.1.1 Total de presupuesto en líneas de los presupuesto nacionales destinados a gastos reservados
		3.1.2 Total del presupuesto nacional destinado a seguridad
		3.1.3 Instituciones Estatales que tienen líneas de presupuesto destinadas a seguridad y gastos reservados
		3.1.4 Montos de contratos relacionados con compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia
		3.1.5 Instituciones encargadas de contratos relacionados con compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia
	3.2 Empresas proveedoras de bienes y servicios en materia de tecnologías de vigilancia	3.2.1 Empresas que tienen contratos relacionados de compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia
		3.2.2 Nivel de posibilidad de contrataciones o interés de contratar bienes y servicios en tecnologías de vigilancia
Tecnológica	4.1 Utilización de malware o spyware	4.1.1 Ataques o uso de malware, spyware, phishing u otras
	4.2 Escuchas telefónicas dentro del país	4.2.1 Casos en los que se evidencia el uso de escuchas telefónicas legales e ilegale
	4.3 Peticiones de información del gobierno sobre usuarios de servicios de Internet	4.3.1 Número de peticiones de información sobre usuarios de servicios de Internet por parte del gobierno
		4.3.2 Naturaleza de las peticiones de información sobre usuarios de servicios de Internet por parte del gobierno
		4.3.3 Peticiones gubernamentales aceptadas por las empresas
	4.4 Vigilancia en Internet	4.4.1 Herramientas de vigilancia en Internet con las que cuenta el Estado
	4.5 Tecnologías de reconocimiento biométrico	4.5.1 Capacidad instalada en uso de tecnologías de reconocimiento biométrico
		4.5.2 Tipos de uso de tecnologías de reconocimiento biométrico
	4.6 Drones y globos de vigilancia	4.6.1 Capacidad de los modelos de drones y globos de vigilancia utilizados
	4.7 Georeferenciación	4.7.1 Capacidad de georeferenciación

El Salvador

FUNDACIÓN Acceso

1. Diménsión Jurídico-Legal

1.1 Protección de la privacidad a nivel constitucional

1.1.1 Nivel de protección de la privacidad en el país a nivel constitucional Protección de la privacidad en el país a nivel constitucional

En El Salvador el derecho a la privacidad cuenta con una protección de rango constitucional. Concretamente, es el artículo 2 de la Constitución de la República[1] el que protege este derecho, cuando señala que "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen". Además, según la jurisprudencia de la Sala de lo Constitucional la privacidad se considera un derecho fundamental[2].

"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" (Constitución de la República de El Salvador, Art. 6))

Como lo ha señalado Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión de Naciones Unidas, "El derecho a la privacidad a menudo se entiende como un requisito esencial para la realización del derecho a la libertad de expresión. La interferencia indebida con la privacidad de las personas puede limitar directa e indirectamente el libre desarrollo y el intercambio de ideas. (...) Una infracción de un derecho puede ser tanto la causa como la consecuencia de una infracción del otro"[3] . En ese sentido, el texto constitucional también protege aspectos vinculados al derecho a la privacidad. Así, en su artículo 6 se protege el derecho a la libertad de expresión. Dicho artículo establece que 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 otras personas. Además, establece que este derecho "no estará sujeto a previo examen, censura, ni caución". El artículo 24 por su parte, hace referencia a la inviolabilidad de la correspondencia de toda clase, estableciendo la prohibición

1 Constitución de la República de El Salvador, D.C. Nº 38, del 15 de diciembre de 1983 (D.O. Nº 234, Tomo Nº 281, del 16 de diciembre de 1983).
2 Fundación Acceso. 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 (San José: Fundación Acceso, 2015), http://www.acceso.or.cr/assets/files/investigacion-resumen-ejecutivo.pdf
3 «Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue» (Human Rights Council, twenty-thrid session)

de la interferencia e intervención de telecomunicaciones. Dichas intervenciones solo se pueden considerar legítimas, de forma temporal, cuando hayan sido autorizadas judicialmente.

1.2 Tratados y Convenciones Internacionales

1.2.1 Nivel de implicación de instrumentos internacionales - como tratados, acuerdos convenciones y otros - firmados por el país con relación a la privacidad

Los instrumentos internacionales, como tratados o convenciones, tienen en El Salvador un rango supralegal. Esto significa que en caso de conflicto entre una ley nacional y un convenio o tratado, será el segundo el que prevalezca[4]. Sin embargo, a diferencia de otros países de la región - como Guatemala o Costa Rica - en el caso de que haya conflicto entre la Constitución y la norma internacional, será la primera la que prevalezca.

"La principal norma internacional vinculada a los Derechos Humanos en espacios digitales es la Declaración Universal de Derechos Humanos de la Organización de Naciones Unidas"

Según el documento "Privacidad y Acceso a la información pública en línea para Defensores y Defensoras de Derechos Humanos"[5], la principal norma internacional vinculada a los Derechos Humanos en espacios digitales es la Declaración Universal de Derechos Humanos de la Organización de Naciones Unidas (ONU, 1948). El enunciado de dicha Convención establece un marco básico del que podrían derivarse otras normas relativas a derechos digitales. En este sentido, son particularmente relevantes los siguientes aspectos:

> **Artículo 12**: 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. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.".
>
> **Artículo 19:** "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir

4 La sección tercera de la Constitución de El Salvador de 1983, en la que se incluye del Artículo 144 al 149, da valor de ley de la República todo tratado internacional celebrados por El Salvador con otros estados o con Organismos internacionales y que en caso de conflicto entre el tratado y la ley, prevalecerá el tratado.

5 José Osorio, «Privacidad y Acceso a la información pública en línea para Defensores y Defensoras de Derechos Humanos en: Guatemala, El Salvador, Honduras y Nicaragua» , Fundación Acceso - Medium (blog), 5 de septiembre de 2018, https://medium.com/@facceso.ca/privacidad-y-acceso-a-la-informaci%C3%B3n-p%C3%BAblica-en-l%C3%ADnea-para-defensores-y-defensoras-de-derechos-5690330c3762.

informaciones y opiniones, y el de difundirlas sin limitación de fronteras, por cualquier medio de expresión."

Artículo 29: "1. Toda persona tiene deberes respecto a la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad. 2. En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática. 3. Estos derechos y libertades no podrán, en ningún caso, ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas".

"Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección".

Por otro lado, El Pacto Internacional de Derechos Civiles y Políticos (1966) es también un instrumento de gran relevancia. Dicho Pacto busca garantizar a todas las personas el disfrute tanto de los derechos civiles y políticos, como de sus derechos económicos, sociales y culturales. En este sentido, los Estados firmantes adquieren el compromiso de promover el respeto universal y efectivo de estos derechos. En el ámbito de la privacidad, abarcaría la garantía a la utilización de medios digitales, donde la persona titular de los mismos pueda emitir expresiones que vayan en favor de las libertades de las personas y del interés general. Este instrumento internacional fue ratificado por el Salvador en 1967.

Adicionalmente, a nivel regional, en 1969 se suscribió la Convención Americana de Derechos Humanos (también llamada Pacto de San José). El Pacto de San José fue ratificado por El Salvador en 1978. En el ámbito de la libertad de expresión la Convención señala en su artículo 13 que:

> "Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección".

El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y asegurar:

"a. el respeto a los derechos o a la reputación de los demás, o

b. la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

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".

El artículo 14 de esta misma Convención hace referencia al derechos de rectificación o respuesta, planteando lo siguiente:

"Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentada y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.

En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiese incurrido.

Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial".

Finalmente, es de particular importancia la Declaración de Principios sobre Libertad de Expresión realizada Comisión Interamericana de Derechos Humanos (CIDH) en 2000. En esta Declaración la CIDH establece los siguientes principios:

Principio 1: La libertad de expresión, en todas sus formas y manifestaciones, es un derecho fundamental e inalienable, inherente a todas las personas. Es además, un requisito indispensable para la existencia misma de una sociedad democrática.

Principio 5: La 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.

Principio 10: Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas.

1.3 Leyes, reglamentos, decretos y normativas nacionales

1.3.1 Nivel de aplicación, transparencia y control de leyes, reglamentos, decretos y normativas relacionados con el derecho a la privacidad (leyes de telecomunicaciones, leyes ciberseguridad, inteligencia de Estado (secreto de Estado), leyes antiterroristas, o reformas de ley con artículos que indican prácticas que protegen o vulneran la privacidad

La normativa salvadoreña incluye en varios de sus principales textos legales disposiciones relativas a la privacidad. Entre las disposiciones garantes de este derecho, destacan las incluidas en el Código Penal[6]. En este sentido, el Título VI del Libro II del Código dedica su Capítulo II a los delitos relativos a la intimidad. Entre los delitos tipificados en dicho capítulo, el artículo 184 y 185, hacen referencia a la violación de las comunicaciones, estableciendo sanciones de multa e inhabilitación para ese tipo de conductas. Por otro lado, el artículo 186 sanciona con penas de cárcel de entre 2 a 6 años la captación de comunicaciones.

6 Decreto no 1030, 30 de abril de 1997, Código Penal.

El Código Penal dedica además un capítulo único (en el Título XIV del libro segundo) a los derechos y garantías fundamentales. Los artículos 301 y 302 de dicho capítulo resguardan la inviolabilidad de la correspondencia y la comunicación durante investigaciones policiales o judiciales.

También el Código Procesal Penal[7] incluye disposiciones que pueden considerarse favorables al derecho a la privacidad en alguna medida. Se trata de aspectos de carácter general, principalmente enfocados a garantizar el debido proceso en allanamientos y registros. En este sentido, del artículo 191 al 200 se detallan los procedimientos requeridos en casos de allanamiento, registro, requisa, inspección e intervención corporal. Es de particular importancia el artículo 201, ya que establece las condiciones que las autoridades deben garantizar a la hora de obtener y resguardar información electrónica. Esta disposición busca justamente atender "la dimensión de resguardo de la información, para no infringir el derecho a la intimidad y ponderadamente equilibrar por medio de una orden o autorización judicial" (Art. 201). Supone además que la orden judicial "tiene que ser expresa para estas actividades, no de carácter genérica, salvo en los casos de los registros y allanamientos donde la autorización puede abarcar hasta estos instrumentos, pero aún en estos supuestos debe de enunciar específicamente que uno de los objetivos es de almacenamientos de dispositivos electrónicos o tecnológicos, de lo contrario solo proceder a su respectiva incautación o secuestro"[8].

"El Código Procesal Penal incluye disposiciones que pueden considerarse favorables al derecho a la privacidad en alguna medida. Se trata de aspectos de carácter general, principalmente enfocados a garantizar el debido proceso en allanamientos y registros"

Por otro lado, en 2016 entró en vigencia la Ley Especial contra los Delitos Informáticos y Conexos[9]. Esta ley tiene como objetivo "proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las tecnologías de la información y la comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley" (Art. 1).

7 Rommell Ismael Sandoval Rosales (Coord.), Código procesal penal comentado : volumen I. (San Salvador: Consejo Nacional de Judicatura, 2018), http://www.cnj.gob.sv/images/documentos/pdf/publicaciones/codigo_procesal_penal_comentado_v1.pdf
8 Ibíd.
9 Decreto no 260, 4 de febrero de 2016, Ley Especial Contra los Delitos Informáticos y Conexos (D. O. n.º 40, tomo n.º 410 de febrero de 2016).

Dicha Ley dedica su título II a la tipificación y la sanción de delitos de diferente carácter. El capítulo I de dicho título, hace referencia a los delitos contra los sistemas tecnológicos de información; el Capítulo II a los delitos informáticos; el Capítulo III a los delitos informáticos relacionados con el contenido de datos; el Capítulo IV a los delitos informáticos contra niños, niñas, adolescentes y personas con discapacidad; y el Capítulo V a los delitos contra el orden económico. Las disposiciones específicas incluidas en estos capítulos brindan protección frente a situaciones como el acceso indebido a sistemas informáticos o datos, la revelación indebida de datos o información personal, o la interferencia o interceptación de datos.

Asimismo, es importante señalar que desde 2010 el país cuenta con la Ley Especial para la Intervención de las Telecomunicaciones[10]. En su artículo 1, este texto legal insiste en la garantía al secreto en las comunicaciones, al mismo tiempo que autoriza de manera excepcional su intervención en casos en los que se cuente con una autorización judicial, escrita y justificada. Según el artículo 5 de la norma, esta excepcionalidad no es aplicable a la investigación de cualquier delito.

El artículo 47 establece que un fiscal, previa resolución motivada, podrá "requerir de los operadores los informes relativos a los datos de registro de la línea o líneas telefónicas investigadas y los registros de llamadas, correos electrónicos y otros medios de telecomunicaciones, durante un período determinado así como los datos sobre el origen de las comunicaciones". Los operadores estarán obligados a conservar los registros correspondientes de sus usuarios por un plazo no menor de diez años.

Finalmente, la Ley Especial contra el Delito de Extorsión permite que, en el caso de este delito, la intervención y registro llamadas telefónicas se realice previa autorización de la Fiscalía General

10 La intervención es justificada solo cuando se trata de pesquisas relacionadas con homicidio y su forma agravada; privación de libertad, secuestro y atentados contra la libertad agravados; pornografía, utilización de personas menores de 18 años e incapaces o deficientes mentales en pornografía y posesión de pornografía; extorsión; concusión; negociaciones ilícitas; cohecho propio, impropio y activo; agrupaciones ilícitas; comercio de personas, tráfico ilegal de personas, trata de personas y su forma agravada; organizaciones internacionales delictivas; los delitos previstos en la ley reguladora de las actividades relativas a las drogas; los delitos previstos en la ley especial contra actos de terrorismo; los delitos previstos en la ley contra el lavado de dinero y de activos; los delitos cometidos bajo la modalidad de crimen organizado en los términos establecidos en la ley de la materia; los delitos previstos en la presente ley; y, los delitos conexos con cualquiera de los anteriores.

de la República (Artículo 8). De esta manera, los jueces otorgan valor probatorio a los análisis de bitácoras de llamadas y a las declaraciones de los agentes policiales o particulares que participaron en la negociación y entrega bajo cobertura policial.

1.4 Normativa de seguridad nacional y ciberseguridad

1.4.1 Existencia de legislación relacionada con seguridad nacional y ciberseguridad

El Salvador cuenta desde 2002 con una Ley de la Defensa Nacional. Dicha norma define la seguridad nacional de siguiente manera:

> "Es un conjunto de acciones permanentes que el Estado propicia para crear las condiciones que superan situaciones de conflictos internacionales, perturbaciones a la tranquilidad pública, catástrofes naturales y aquellas vulnerabilidades que limiten el Desarrollo Nacional y pongan en peligro el logro de los Objetivos Nacionales" (Art. 4).

A partir de esta ley, el Estado formuló su política de Seguridad Nacional en el Libro de la Defensa Nacional (2006). Dicho documento sintetiza la doctrina de defensa del país. Se trata de una herramienta con la que cuenta el Estado para guiar y orientar un conjunto de acciones coordinadas y para enfrentar amenazas, tanto en tiempo de paz como de conflicto bélico. Sus objetivos permanentes son "mantener la soberanía del Estado y la integridad del territorio; así como garantizar a sus habitantes el goce de la libertad, la seguridad, la salud, la cultura, el bienestar económico y la justicia social"[11]. Más allá de un escenario posible de conflicto entre países, el documento destaca nuevas amenazas como el terrorismo, la delincuencia organizada transnacional, el narcotráfico, la corrupción, el lavado de activos, el tráfico ilícito de armas o la trata de personas. Además, destaca el terrorismo cibernético, como una de las nuevas amenazas que enfrentan el país y la región[12]. Según el documento, el pilar fundamental de la política de defensa es la Constitución de la República.

11 El Salvador, Libro de la Defensa Nacional, (Junio de 2006), http://www.cedoh.org/Biblioteca_CEDOH/archivos/00237%20LIBRO%20DE%20LA%20DEFENSA%20NACIONAL.pdf
12 Ibíd.

El Salvador no cuenta con una ley específica de Cyberseguridad. La Ley Especial contra los Delitos Informáticos y Conexos es la única norma con la que se cuenta en ese ámbito. Sin embargo, no se trata de una ley de ciberseguridad como tal. Por otro lado, es importante señalar, que El Salvador no es firmante del Convenio de Budapest (2001) sobre la ciberdelincuencia[13], el primer tratado internacional sobre Internet y los delitos informáticos.

2. Dimensión Política

2.1 Relación entre Estado, empresas y cámaras de telecomunicaciones

2.1.1 Nivel de relación entre el Estado, empresas y cámaras de telecomunicaciones

La Superintendencia General de Electricidad y Telecomunicaciones (SIGET) es la entidad que en El Salvador cuenta con atribuciones para aplicar la normativa, nacional e internacional, relativa a los sectores de Electricidad y de Telecomunicaciones. La institución fue creada en 1996 y tiene como objetivo proteger los derechos tanto de las personas usuarias como de quienes desarrollan actividades económicas en este sector. Sus potestades son principalmente regulatorias[14].

El sector empresarial cuenta con representación formal en esta entidad. Concretamente, la Junta Directiva está compuesta por tres directores, unos de los cuales debe ser electo por las asociaciones gremiales del sector privado legalmente establecidas en el país.

Según la Ley de Telecomunicaciones, dentro de las obligaciones de los operadores de servicios de acceso, puntos de venta de saldo para llamadas y uso de Internet, estas deben llevar un registro de todos los usuarios de pago previo, debiendo mantener esa información a disposición de la autoridad competente en la investigación de delitos que la requiera (artículo 30, inciso a). En este sentido, se obliga a los operadores a tener un registro de los nombres de quienes contratan

Según la Ley de Telecomunicaciones los operadores de servicios de acceso, puntos de venta de saldo para llamadas y uso de Internet deben llevar un registro de todos los usuarios de pago previo, debiendo mantener esa información a disposición de la autoridad competente en la investigación de delitos que la requiera (artículo 30, inciso a).

13 Convenio sobre la Ciberdelincuencia, 23 de noviembre de 2001, https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
14 «Estructura organizativa», SIGET, acceso el 25 de agosto de 2019, https://www.siget.gob.sv/institucion/estructura-organizativa/

líneas telefónicas, así como de llamadas efectuadas y de los datos sobre el origen de cualquier otro tipo de comunicación electrónica.

2.1.2 Nivel de representación en cuanto a la relación entre el Estado, las empresas y las cámaras de telecomunicaciones

La relación entre el Ejecutivo y las organizaciones tradicionales del sector empresarial en El Salvador ha sido tensa en los últimos años, particularmente en lo relativo al ámbito de las telecomunicaciones.

La relación entre el Ejecutivo y las organizaciones tradicionales del sector empresarial en El Salvador ha sido tensa en los últimos años, particularmente en lo relativo al ámbito de las telecomunicaciones. Dicha disputa ha tenido que ver con el nombramiento del puesto de dirección de la SIGET que corresponde al sector empresarial.

El nombramiento realizado en 2017 excluyó a la asociaciones empresariales que tradicionalmente han controlado ese puesto – como la Asociación Nacional de la Empresa Privada (ANEP) - y que agrupan a la mayoría de las empresas del sector. Tanto ANEP como la Asociación Salvadoreña de Radiodifusores acusaron al ejecutivo de crear 60 nuevas gremiales con el fin de viciar la elección de la dirección[15]. Es importante señalar, que la Sala Constitucional avaló la posición del sector empresarial y anuló el nombramiento[16].

2.2 Contratos entre el Estado y las empresas de seguridad privada

2.2.1 Nivel de impacto de los contratos establecidos entre el Estado y empresas de seguridad privada

Son muchos los recursos que el Estado Salvadoreño destina a la compra de servicios de seguridad privada. Según fuentes de prensa, entre 2005 y 2015 se destinaron a actividades como la custodia de instalaciones al menos 135.2 millones de dólares. Esto equivaldría "al presupuesto para 10

15 Edwin Teos, Melissa Pacheco y Cristian Meléndez, «GOES juramenta a directores de la SIGET pese a múltiples señalamientos», La Prensa Gráfica, 30 de noviembre de 2017, acceso el 26 de agosto de 2019, https://www.laprensagrafica.com/economia/GOES-juramenta-a-directores-de-la-SIGET-pese-a-multiples-senalamientos-20171129-0116.html

16 Jonathan Laguan, «Sala suspende nombramientos de directores de SIGET y ordena restituir a exdirectores», La Prensa Gráfica, 17 de enero de 2018, acceso el 26 de agosto de 2019, https://www.laprensagrafica.com/elsalvador/Sala-suspende-nombramientos-de-directores-de-SIGET-y-ordena-restituir-a-exdirectores-20180117-0076.html

años de instituciones como la Academia Nacional de Seguridad Pública (ANSP)"[17]. También sería equivalente al gasto necesario "para pagar durante 10 años a 2,000 policías básicos"[18].

Por otro lado, se estima que cerca del 40% de todos los servicios que proveen las empresas de seguridad privada son contratados por instituciones del Gobierno de El Salvador[19].

Llama la atención además, que en periodo señalado son dos empresas las que han acaparado gran parte de los contratos públicos de seguridad privada: SERCONSE y COSASE. Estas dos empresas habrían recibido el 56.6% del total de los recursos destinados a seguridad privada por parte de entidades públicas.

Entre 2005 y 2015 se destinaron a actividades como la custodia de instalaciones al menos 135.2 millones de dólares.

En el caso de SERCONSE, es importante señalar que un informe de auditoría reveló prácticas fraudulentas por su parte. Según fuentes de prensa, dicha auditoria determinó que el Instituto Salvadoreño del Seguro Social (ISSS) entregó a la empresa 5.9 millones de dólares por un servicio que nunca se llegó a brindar[20].

2.3 Relación de actores estatales o políticos con las directivas de empresas de seguridad

2.3.1 Nivel de relación del Estado con empresas de seguridad privada

Investigaciones realizadas en periodos presidenciales previos al actual han demostrado la existencia de estrechos vínculos entre directivos de las empresas de seguridad, miembros del Ejecutivo y dirigentes de los principales partidos políticos. En este sentido, fuentes periodísticas revelaron que entre 2005 y 2015 las empresas más exitosas en el negocio de la seguridad privada fueron "apadrinadas por los operadores políticos"[21].

17 Jessica Ávalos y Olga Chacón, «El emporio de la seguridad privada», La Prensa Gráfica, 15 de marzo de 2015, acceso el 26 de agosto de 2019 https://www.laprensagrafica.com/revistas/El-emporio-de-la-seguridad-privada-20150315-0037.html.
18 Ibíd.
19 Juan Ricardo Gómez Hecht, «Las agencias de seguridad privada en El Salvador: Estado de la colaboración público privada en prevención del delito en el sistema de seguridad pública», Revista Policía y Seguridad Pública, año 4, vol. 2 (2014), https://www.camjol.info/index.php/RPSP/article/view/1759
20 Ibíd.
21 Jessica Ávalos y Olga Chacón, «El emporio de la seguridad privada», La Prensa Gráfica, 15 de marzo de 2015, acceso el 26 de agosto de 2019 https://www.laprensagrafica.com/revistas/El-emporio-de-la-seguridad-privada-20150315-0037.html.

Además, también se han identificado nexos entre políticos y nuevas empresas. Estos vínculos son evidentes en las ya mencionadas empresas SERCONSE y COSASE. La primera, SERCONSE, era propiedad del dirigente del partido ARENA Adolfo Tórrez. Dicha empresa tuvo justamente su principal periodo de crecimiento entre 2004 y 2009, coincidiendo con el gobierno de Elías Antonio Saca, también del partido ARENA. En dicho periodo obtuvo ganancias de, al menos, 38 millones de dólares[22].

Investigaciones realizadas en periodos presidenciales previos al actual han demostrado la existencia de estrechos vínculos entre directivos de las empresas de seguridad, miembros del Ejecutivo y dirigentes de los principales partidos políticos

Según medios de prensa, en 2009, COSASE sustituyó a SERCONSE en la concentración de contratos públicos. Dicha empresa era propiedad de Miguel Menéndez, uno de los padrinos de la campaña del expresidente del Partido FMLN Mauricio Funes. En este caso, algunas de las adjudicaciones se realizaron bajo la modalidad de contratación directa. Es de destacar, que el propio expresidente Funes ha reconocido "que alguien de su círculo cercano acaparó la mayoría de contratos en seguridad"[23].

En los últimos años se han creado además nuevas empresas, que también han buscado acceder a contrataciones del Estado. Este es el caso de la empresa Alternativa Privada de Protección para el Desarrollo (ALPRODESA). Esta entidad está a cargo de la seguridad de todos los negocios de ALBA Petróleos. ALPRODESA fue constituida en 2010 con el sello notarial del "entonces gerente legal de ALBA y luego presidente de la Corte Suprema de Justicia"[24].

Asimismo, investigaciones periodísticas han evidenciado que son más los políticos y funcionarios que participan en empresas de seguridad privada, aunque en estos casos no hay constancia de que hayan sido favorecidos con contrataciones públicas. Por ejemplo, Sigifredo Ochoa, exviceministro de Obras Públicas con ARENA, es socio de la empresa Grupo Los Seis, S. A. de C. V. Por otro lado, el presidente del Fondo Social para la Vivienda (FSV), Tomás Chévez, es propietario de la empresa Servicios de Seguridad Dos Mil[25].

22 Ibíd.
23 Ibíd.
24 Ibíd.
25 Ibíd.

Esta mezcla entre funcionarios públicos y negocios de seguridad privada se ve favorecida por el hecho de que no haya una prohibición legal explícita para ello. De hecho, solo existe prohibición de que miembros activos de la Policía sean propietarios o accionistas de dichas entidades.

Finalmente, destaca que muchos ex militares se han incorporado a las planillas de las empresas de seguridad privada. En este sentido, algunos datos apuntan a que en la actualidad los militares retirados representan el 40% de la planilla de este sector[26].

El plan cuenta con 5 ejes estratégicos y 124 acciones prioritarias. Sin embargo, son pocos los aspectos vinculados a la vigilancia tecnológica y la privacidad.

2.4 Planes de Gobierno en vigencia en materia de seguridad nacional

2.4.1 Planes de gobierno vigentes relacionados con la seguridad nacional y ciberseguridad que protegen o vulneran la privacidad

El plan de seguridad más recientemente implementado en el país data de 2015. Se trata del Plan "El Salvador Seguro" realizado por el Consejo Nacional de Seguridad Ciudadana y Convivencia, con el apoyo del Programa de Naciones Unidas para el Desarrollo (PNUD). Es importante señalar, que dicho plan no incorpora disposiciones específicas relativas al resguardo de la privacidad.

El plan cuenta con 5 ejes estratégicos y 124 acciones prioritarias. Sin embargo, son pocos los aspectos vinculados a la vigilancia tecnológica y la privacidad. En este sentido, las acciones 57, 59 y 63 del eje 3 – dedicado a la rehabilitación y la reinserción – incluyen acciones como el bloqueo de la señal de celular en centros penitenciarios o la adquisición de equipo tecnológico para monitorear la seguridad perimetral e interna de los centros de privación de libertad, así como el ingreso de visitas[27].

26 Juan Ricardo Gómez Hecht, «Las agencias de seguridad privada en El Salvador: Estado de la colaboración público privada en prevención del delito en el sistema de seguridad pública», Revista Policía y Seguridad Pública, año 4, vol. 2 (2014), https://www.camjol.info/index.php/RPSP/article/view/1759

27«Gobierno promueve la seguridad cibernética en instituciones públicas», Presidencia de la República, acceso el 14 de septiembre de 2018, http://www.presidencia.gob.sv/gobierno-promueve-la-seguridad-cibernetica-en-instituciones-publicas/

Por otro lado, si hay un creciente interés en lo relativo a la seguridad digital por parte del Ejecutivo. En esta línea, en el marco de la Estrategia de Gobierno Digital de El Salvador 2018 – 2022, se han realizado acciones tendientes a fortalecer los sistemas del gobierno[28].

2.5 Relación de los planes de seguridad nacional y ciberseguridad con la privacidad

2.5.1 Nivel de protección o vulneración de la privacidad de los planes de gobierno vigentes relacionados con la seguridad nacional y ciberseguridad

Como ya se ha señalado, los planes identificados no incluyen medidas específicas con respecto al derecho a la privacidad. Por otro lado, entre las diferentes acciones previstas en dichos planes, solo aquellas enfocadas al control de la población privada de libertad implican restricciones explícitas de este derecho.

2.6 Uso de tecnológicas de vigilancia como evidencia o caso para criminalizar o judicializar

Los informes de interceptación de comunicaciones brindados por la Fiscalía General de la República (FGR) a la comisión de seguridad de la Asamblea Legislativa son de carácter reservado

2.6.1 Casos en los que se usan evidencias de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos que ejercen sus derechos humanos y civiles

La información existente que de cuenta del uso de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos es muy escasa.

Sin embargo, la videovigilancia, la triangulación de teléfonos móviles y la intervención de comunicaciones han sido herramientas de investigación penal importantes en casos de alta relevancia social y política, como algunos casos de feminicidios, corrupción estatal y crimen organizado. No obstante, no se cuenta con datos que permitan dimensionar el uso de este tipo de prácticas. Esto es así, debido a que muchos de los documentos que registran este tipo de

28 Consejo Nacional de Seguridad Ciudadana y Convivencia, «Plan El Salvador Seguro», (San Salvador: CNSCC. 2015), http://www.seguridad.gob.sv/dia/monitoreo-y-evaluacion/plan-el-salvador-seguro-pess/#

información son confidenciales. Por ejemplo, los informes de interceptación de comunicaciones brindados por la Fiscalía General de la República (FGR) a la comisión de seguridad de la Asamblea Legislativa son de carácter reservado[29].

Además de los casos en los que la obtención y el manejo de las evidencias se hace de acuerdo a lo legalmente dispuesto, medios de comunicación dan cuenta del uso de las tecnologías al margen de sus usos autorizados en procesos judiciales. El reciente caso del sacerdote Antonio Rodríguez da cuenta de ello. En ese caso, la fiscalía empleo grabaciones de conversaciones íntimas del acusado, para presionar al entorno cercano de este y propiciar su confesión. Las grabaciones, habrían sido obtenidas legalmente, sin embargo su difusión ante terceros está prohibida[30].

2.6.2 Identificación de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos que ejercen sus derechos humanos y civiles

Según se detalla en el apartado 4 de este documento en el caso salvadoreño se identifican tecnologías, que dependiendo de su uso, podrían ser empleadas para criminalizar, deslegitimar o amenazar a personas y colectivos. Se trata de tecnologías y herramientas que bien utilizadas pueden aportar pruebas importantes en casos de violación de derechos humanos, pero que - sin controles adecuados - también se prestan para la vulneración de derechos.

Sin embargo, no se ha identificado información que de cuenta del uso de este tipo de tecnologías para criminalizar, deslegitimar o amenazar a personas defensoras de derechos humanos.

29 Ricardo Flores, «Fiscal general destaca uso de escuchas telefónicas», La Prensa Gráfica, 8 de diciembre de 2018, https://www.laprensagrafica.com/elsalvador/Fiscal-general-destaca-uso-de-escuchas-telefonicas-20181207-0329.html.
30 Carlos Martínez, Sergio Arauz, y José Luis Sanz, «Fiscal Usó Conversaciones Íntimas Del Padre Toño Para Conseguir Su Confesión», Elfaro.net, 8 de septiembre de 2014, https://elfaro.net/es/201409/noticias/15912/Fiscal-usó-conversaciones-íntimas-del-padre-Toño-para-conseguir-su-confesión.htm.

2.7 Acuerdos bilaterales y multilaterales de cooperación en materia de seguridad

2.7.1 Existencia de acuerdos bilaterales y multilaterales de cooperación en materia de seguridad

En el caso de El Salvador, en lo relativo a la seguridad ciudadana, se esperaba que la Alianza brindaría la posibilidad de reforzar "los programas de prevención de la violencia y la capacidad de gestión de las fuerzas policiales.

Son numerosos los acuerdos, tanto bilaterales y como multilaterales ,que El Salvador ha suscrito en materia de seguridad. En este sentido, desde 1995, el país es firmante del Tratado Marco de Seguridad Democrática en Centroamérica. Este tratado define que "El Modelo Centroamericano de Seguridad Democrática se basa en la democracia y el fortalecimiento de sus instituciones y el Estado de Derecho (…) y en el irrestricto respeto de todos los derechos humanos en los Estados que conforman la región centroamericana"[31].

Por otro lado, el país también es firmante de la declaración sobre Seguridad en las Américas (2003)[32] y de la Declaración de San Salvador sobre Seguridad Ciudadana en las Américas (2011)[33].

Otro tratado relevante es la Alianza para la Prosperidad del Triángulo Norte (2014), una iniciativa tripartita entre los gobiernos de Guatemala, Honduras y El Salvador, creada en colaboración con el Banco Interamericano de Desarrollo (BID). Se trata de una estrategia que busca frenar, a mediano plazo, la migración irregular hacia Estados Unidos. Esta estrategia pretendía también tomar medidas en materia de desarrollo productivo e inversión en capital humano para el fortalecimiento de las instituciones locales y la seguridad ciudadana.

En el caso de El Salvador, en lo relativo a la seguridad ciudadana, se esperaba que la Alianza brindaría la posibilidad de reforzar "los programas de prevención de la violencia y la capacidad de gestión de las fuerzas policiales"[34].

31«Tratado Marco de Seguridad Democrtica en Centromerica», diciembre de 1995, https://www.teg.gob.sv/phocadownload/portal/marconormativo/leyesprincipales/Tratado%20Marco%20de%20Seguridad%20Democrtica%20en%20Centromerica.pdf.
32 «Declaración sobre Seguridad en las Américas», 28 de octubre de 2003, http://www.oas.org/36AG/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf.
33 OEA, «Declaración de San Salvador Sobre Seguridad Ciudadana en las Américas», OEA - Organización de los Estados Americanos, 7 de junio de 2011, http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=S-37.
34 «Países del Triángulo Norte de Centroamérica presentan plan Alianza para la Prosperidad», Secretaría Técnica y de Planificación, 14 de noviembre de 2014, http://www.secretariatecnica.gob.sv/comunicado-tripartito-alianza-para-la-prosperidad-del-triangulo-norte/.

Adicionalmente, existen convenios bilaterales en materia de seguridad entre el gobierno nacional y otros gobiernos o agencias de cooperación. En este sentido, en junio de 2017, el Ministerio de Justicia y Seguridad Pública anunció que se fortalecerían los sistemas de videovigilancia en zonas priorizadas de 9 ciudades, con el fin de mejorar la seguridad ciudadana. Para ello, se contó con el apoyo de la cooperación de la República de Taiwán, que realizó una inversión de $4.5 millones. Esta inversión se realizó en el marco del proyecto "Fortalecimiento de las Capacidades Institucionales para la Seguridad Ciudadana"[3536].

El apoyo taiwanes se suspendió, ya que el país emprendió relaciones diplomáticas con el gobierno de China[37]. Esto implicó la ruptura de relaciones con Taiwán y la afectación de los acuerdos de cooperación existentes. Sin embargo, fuentes del Ejecutivo consideraron que la nueva alianza con China tenía el potencial de ampliar sustancialmente los apoyo ofrecidos por Taiwán[38].

También Corea ha cooperado de manera directa a través de su gobierno. En este caso, se trata de una cooperación bajo el programa Knowledge Share Program (KSP), que cuenta con la participación del Banco Interamericano de Desarrollo (BID). Tiene el objetivo de crear políticas públicas con un enfoque de seguridad informática[39]. Esto último es un pilar de la Estrategia de Gobierno Digital, presentada en junio de 2018[40].

Por otro lado, la Policía Nacional Civil (PNC) tiene un "Memorando de Entendimiento" firmado con la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC) para el establecimiento

35 «Fortalecerán sistema de videovigilancia en zonas priorizadas para mejorar la seguridad ciudadana», Ministerio de Justicia y Seguridad Pública, 5 de junio de 2017, http://www.seguridad.gob.sv/fortaleceran-sistema-de-videovigilancia-en-zonas-priorizadas-para-mejorar-la-seguridad-ciudadana/.

36 «El Salvador y la República de China (Taiwán) fortalecen sus lazos de hermandad con la visita del ministro de exteriores», Presidencia de la República de El Salvador, 13 de julio de 2018, http://www.presidencia.gob.sv/el-salvador-y-la-republica-de-china-taiwan-fortalecen-sus-lazos-de-hermandad-con-la-visita-del-ministro-de-exteriores/.

37 Juan Carlos Barahona, «Sistema de vídeovigilancia en Santa Ana no será instalado, por rompimiento de relaciones con Taiwán», *La Prensa Gráfica*, 22 de diciembre de 2018, https://www.laprensagrafica.com/elsalvador/Sistema-de-videovigilancia-en-Santa-Ana-no-sera-instalado-por-rompimiento-de-relaciones-con-Taiwan-20181221-0319.html.

38 Juan Carlos Barahona, «China financiaría la videovigilancia», *La Prensa Gráfica*, 9 de febrero de 2019, https://www.laprensagrafica.com/elsalvador/China-financiaria-la-videovigilancia-20190208-0339.html.

39 «SETEPLAN se capacita en el tema de la ciberseguridad», Secretaría Técnica de Planificación, acceso el 5 de septiembre de 2018, http://secretariatecnica.egob.sv/seteplan-se-capacita-en-el-tema-de-la-ciberseguridad/

40 «Gobierno presenta la estrategia de gobierno digital», Secretaría Técnica de Planificación, acceso el 5 de septiembre de 2018.

y tecnificación de la Unidad de Delitos Cibernéticos en la División de Investigación Criminal de la Policía. Este memorando tiene el objetivo de instalar de capacidades propias en la prevención y lucha contra delitos cibernéticos en El Salvador. Como parte de ese trabajo se ha capacitado personal en recuperación y gestión de pruebas de informática forense, con el uso básico del software de recuperación de información "EnCase"[41].

Finalmente, es necesario mencionar que la Fiscalía General de la República (FGR) tiene convenios firmados con la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) y la Oficina de Asuntos Narcóticos Internacionales y Aplicación de la Ley (INL), que apoyaron la creación y tecnificación de la reciente inaugurada Dirección de Análisis, Técnicas de Investigación e Información (DATI), en octubre de 2018[42].

El Salvador cuenta anualmente con partidas presupuestarias que funcionan bajo la categoría de fondos reservados.

3. Dimemsión Económica

3.1 Presupuestos nacionales destinados a seguridad y gastos reservados

3.1.1 Total de presupuesto en líneas de los presupuesto nacionales destinados a gastos reservados

El Salvador cuenta anualmente con partidas presupuestarias que funcionan bajo la categoría de fondos reservados. En este sentido, el Ejecutivo cuenta con "al menos tres partidas de gastos reservados las cuales están asignadas a la Presidencia de la República, al Ministerio de la Defensa Nacional y a la Policía Nacional Civil (PNC)"[43].

41 «Policía Nacional de El Salvador fortalece sus capacidades en la investigación de delitos cibernéticos», Oficina de las Naciones Unidas contra la Droga y el Delito, acceso el 11 de marzo de 2019, https://www.unodc.org/ropan/es/IndexArticles/Cybercrime/cybercrime-training-in-el-salvador.html.

42 «Fiscal General de la República, Douglas Meléndez, inaugura nuevas instalaciones de la Dirección de Análisis, Técnicas de Investigación e Información», Fiscalía General de la República, 11 de marzo de 2019, https://www.fiscalia.gob.sv/fiscal-general-de-la-republica-douglas-melendez-inaugura-nuevas-instalaciones-de-la-direccion-de-analisis-tecnicas-de-investigacion-e-informacion/

43 FUNDE, «Análisis sobre el manejo de los gastos reservados en el Órgano Ejecutivo», (San Salvador: FUNDE, 2007), https://documentop.com/analisis-sobre-el-manejo-de-los-gastos-reservados-en-el-organo-_5a05d4a61723dd1ef9dd15ea.html

De estas tres entidades, es la Presidencia de la República la que cuenta con un mayor financiamiento a cargo de los fondos reservados. Según las cifras disponibles entre 2013 y 2015 los montos que recibieron el Ministerio de Defensa y la PNC estuvieron en torno al millón de dólares anual. Sin embargo, durante ese mismo periodo, la Presidencia empleó en concepto de gastos reservados más de 50 millones anuales.

Tabla 1. Gastos reservados en El Salvador (2013 - 2014)
(Millones de dólares)

	PNC	Defensa	Presidencia
2013	1.2	0.9	81.7
2014	1.3	0.9	42.9
2015	1.3	0.9	52.5

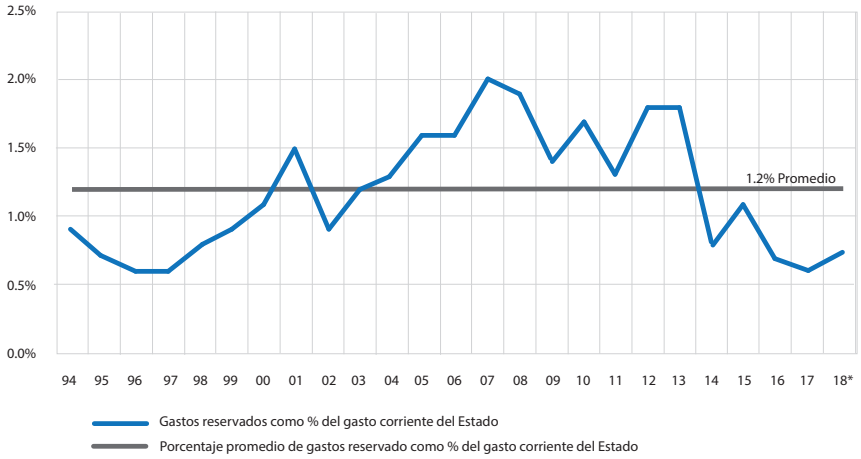
Fuente: FUNDE (2017)

Durante la administración del expresidente Antonio Saca (2004-2009) el 60.4% de los fondos de la Presidencia correspondieron a fondos reservados. De igual forma, durante el periodo del expresidente Mauricio Funes (2009-2016) los fondos reservados representaron el 50.7% del total

Entre 1994 y 2017, los gastos reservados han representado en promedio el 1% del gasto corriente anual total de El Salvador. Sin embargo, en años como 2007 el gasto reservado como porcentaje del total duplicó el promedio, ya que fue del 2%[44].

44 Secretaría de Participación, Transparencia y Anticorrupción, «Informe de gastos reservados de la Presidencia de la República», (San Salvador: SPTA, 2018), https://tinyurl.com/y42kmwaf

Gráfico 1.Gastos reservados como porcentaje del gasto corriente anual del Estado (1994-2018)



Fuente: Secretaría de Participación, Transparencia y Anticorrupción (2018). *Monto de gastos reservados actualizado a junio 2018

En 2018 el monto destinado a Defensa Nacional fue de 141 millones dólares. Ese mismo año, el gasto dedicado a Justicia y Seguridad Pública fue casi 3 veces superior, ya que alcanzó los 416 millones de dólares

Como ya se ha señalado, es la Presidencia la que obtiene el porcentaje más alto del total de estos fondos. Además, son una parte importante de su financiamiento, ya que durante los últimos 25 años en promedio han representado casi la mitad (el 45.7%) del total de sus gastos. Dos administraciones han estado por encima de este promedio. Durante la administración del expresidente Antonio Saca (2004-2009) el 60.4% de los fondos de la Presidencia correspondieron a fondos reservados. De igual forma, durante el periodo del expresidente Mauricio Funes (2009-2016) los fondos reservados representaron el 50.7% del total[45].

Por otro lado, para 2019 se aprobó por concepto de gastos reservados de Casa Presidencial una partida presupuestaria de US$30.6 millones de dólares. Según fuentes de prensa, el Ministerio de Hacienda habría declarado que dichos fondos estabas destinados al Organismo de Inteligencia del Estado (OIE).

3.1.2 Total del presupuesto nacional destinado a seguridad

Para calcular el gasto total que destina el Estado salvadoreño a seguridad son dos las ramas presupuestarias a considerar: Defensa Nacional y Justicia y Seguridad Pública. La primera

45 Ibíd.

considera los gastos dedicados a la defensa del territorio salvadoreño, la segunda comprende los gastos destinados a la seguridad interna. En este sentido, el sistema de seguridad salvadoreño comprende las siguientes instituciones:

- Ministerio de Justicia
- Ministerio de Defensa
- Policía
- Academia Nacional de Seguridad Pública
- Centros Penales
- Migración y Extranjería

En 2018 el monto destinado a Defensa Nacional fue de 141 millones dólares. Ese mismo año, el gasto dedicado a Justicia y Seguridad Pública fue casi 3 veces superior, ya que alcanzó los 416 millones de dólares. La suma de lo invertido en ambas ramos representó en 2018 el 10,2% del presupuesto total del El Salvador (Tabla 2).

Tabla 2. Presupuesto Nacional destinado a Seguridad (2018)

	Abs. (USD$)	% del presupuesto nacional
Defensa nacional	141.172.347	2,6%
Justicia y Seguridad Pública	416.636.925	7,6%
Total defensa, justicia y seguridad	557.809.272	10,2%
Total presupuesto 2019	5.467.500.000	100%

Fuente: elaboración propia a partir de Secretaría de Participación, Transparencia y Anticorrupción (2018a) (2018b) y (2019).

Por otro lado, es importante considerar que estos cálculos no incluyen los recursos que cada institución del Estado destina a contratar servicios de seguridad privada, ya mencionados en el apartado 2.2.1.

3.1.3 Instituciones Estatales que tienen líneas de presupuesto destinadas a seguridad y gastos reservados

Como ya se ha señalado, todas las instituciones del Estado cuentan con una partida presupuestaria dedicada a gastos de seguridad. No se ha logrado acceder a información desagregada que de cuenta del gasto de cada institución en este ámbito. Sin embargo, la importante inversión que realizan las instituciones en su conjunto por conceptos como custodia de instalaciones, da cuenta de que no se trata de un gasto marginal (Ver apartado 2.2.1).

En el caso, de los gastos reservados, como ya se ha señalado (ver apartado 3.1.1), es la presidencia quien condensa el mayor porcentaje de este tipo de gastos. Sin embargo, desde la presidencia se cuenta con la posibilidad de emplear dichos fondos en cualquier ámbito o institución.

NewSmart busca convertir Santa Tecla en una Smart City. En la práctica esto implica la implantación de un sistema de videovigilancia en toda la ciudad. Para ello, se realizó un inversión inicial de 6 millones de dólares para la colocación de 300 cámaras y 102 kilómetros de fibra óptica, que abarcarán en total un territorio de 16 kilómetros cuadrados

3.1.4 Montos de contratos relacionados con compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

No se ha conseguido acceder a información presupuestaria desagregada. En consecuencia, no ha sido posible calcular el monto de los contratos destinados a compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia.

3.1.5 Instituciones encargadas de los contratos relacionados con compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

Debido a las limitaciones ya señaladas, tampoco se ha logrado información detallada con respecto a este punto. Sin embargo, habida cuenta del importante gasto que realizan las instituciones salvadoreñas en materia de seguridad privada, puede inferirse que cualquier institución con la autoridad legal y las posibilidades económicas puede comprar este tipo de bienes y servicios.

3.2 Empresas proveedoras de bienes y servicios en materia de tecnologías de vigilancia

3.2.1 Empresas que tienen los contratos relacionados de compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

Habida cuenta de la alta inversión que realizan las instituciones salvadoreñas en seguridad privada, resulta bastante probable que una porción de dicha inversión esté vinculada con la compra y el uso de tecnologías de vigilancia. Sin embargo, no existe información detallada que de cuenta de la inversión que se realiza en este ámbito específico. En cualquier caso, algunas de las actividades que sí se pueden identificar dan cuenta de su envergadura.

En 2018 se realizó por primera vez la actividad ExpoSecurity en la que numerosas empresas mostraron las diferentes opciones de seguridad privada disponibles. Este tipo de ferias son frecuentes en países más grandes, sin embargo, hasta la fecha no se habían realizado en El Salvador.

Uno de los casos que mejor ilustra esta situación es el de la sociedad NewSmart. Se trata de una alianza público-privada con la Municipalidad de Santa Tecla y la empresa Soluciones en Conectividad, en la que la municipalidad cuenta con el 20% de las acciones y la empresa el 80% restante[46].

NewSmart busca convertir Santa Tecla en una Smart City. En la práctica esto implica la implantación de un sistema de videovigilancia en toda la ciudad. Para ello, se realizó un inversión inicial de 6 millones de dólares para la colocación de 300 cámaras y 102 kilómetros de fibra óptica, que abarcarán en total un territorio de 16 kilómetros cuadrados. Asimismo, la inversión cubre también los gastos derivados de creación de instalaciones para el funcionamiento de New Smart. El uso de la tecnología prevista permitirá el reconocimiento de rostros, placas de vehículos y monitoreo aéreo a través de drones. Además, dicha tecnología está habilitada también para visión nocturna[47].

Diferentes cuerpos policiales – como el Cuerpo de Agentes Municipales de Santa Tecla (CAMST), y Policía Nacional Civil (PNC) – están involucrados en la implementación de este sistema. De

46 Guadalupe Hernández, «NewSmart apuesta por la creación de más ciudades inteligentes en El Salvador», El Diario de Hoy, 11 de abril de 2017, https://www.elsalvador.com/noticias/negocios/335599/newsmart-le-apuesta-a-la-creacion-de-mas-ciudades-inteligentes-en-el-salvador/.

47 «Santa Tecla Inicia el Camino para una "Smart City"», Alcaldía de Santa Tecla, acceso el 10 de septiembre de 2019 http://www.santatfvdecla.gob.sv/blog.php?noticia=864

hecho, la Municipalidad ha suscrito un convenio con la PNC para compartir las bases de datos generadas a partir del sistema de vigilancia[48].

3.2.2 Nivel de posibilidad de contrataciones o interés de contratar bienes y servicios en tecnologías de vigilancia

Una investigación realizada por la propia Fiscalía en 2016, evidenció en años anteriores había habido "un mal manejo de respuesta equivocada al centro de escuchas; porque el centro de escuchas arrojó elementos probatorios de que había un fraude procesal, que se había estado creando prueba"

Como ya se ha señalado, la posibilidad de adquirir tecnologías de vigilancia es alta. Las principales empresas del sector venden este tipo de bienes y servicios. De hecho, COSASE – una de las principales proveedoras de servicios de seguridad privada al Estado en los últimos años – ofrece servicios de videovigilancia. Concretamente, según la información que brinda en su página web, ofrece diferentes tipos de cámaras: con función día y noche, cámaras día y noche con iluminadores infrarrojos, cámaras con Tecnología IP, mini domos y domos de alta velocidad con función de rotación sobre dos ejes (PTZ)[49].

Por otro lado, en los últimos años se identifican tendencias que apuntan a un aumento en la demanda de este tipo de servicios. En 2018 se realizó por primera vez la actividad ExpoSecurity en la que numerosas empresas mostraron las diferentes opciones de seguridad privada disponibles. Este tipo de ferias son frecuentes en países más grandes, sin embargo, hasta la fecha no se habían realizado en El Salvador. Sin duda, es un indicador de que se trata de un mercado en expansión. Entre los productos de seguridad privada ofrecidos durante la feria, destacan varios de tecnologías de vigilancia como cámaras, drones, GPSs y sistemas de seguridad digital[50].

48 Ibíd.
49 «Cámaras de vigilancia», COSASE, acceso el 10 de septiembre de 2019, http://www.cosase.com/index.php/camaras-de-vigilancia
50 «ExpoSecurity El Salvador», Exposecurity, acceso el 11 de marzo de 2019, http://exposv.com/.

4. Dimensión Tecnológica

4.1 Utilización de malware o spyware dentro del país

4.1.1 Evidencias de ataques o uso de malware, spyware, phishing u otras

No se identificaron estudios que demuestren el uso de software espía en El Salvador.

4.2 Escuchas telefónicas dentro del país

4.2.1. Casos en los que se evidencia el uso de escuchas telefónicas

Con respecto a las escuchas realizadas de acuerdo a los procedimientos legales, según cifras brindadas a la prensa por quien fue Fiscal General entre 2015 y 2018, Douglas Meléndez, en 2016 se intervinieron 209.000 llamadas[51]. Según indicó estas se relacionaban con casos de corrupción y crimen organizado[52].

Es escasa la información disponible sobre escuchas ilegales. Sin embargo, una investigación realizada por la propia Fiscalía en 2016, evidenció que en años anteriores había habido "un mal manejo de respuesta equivocada al centro de escuchas; porque el centro de escuchas arrojó elementos probatorios de que había un fraude procesal, que se había estado creando prueba"[53].

51Jorge Reyes, «Operación Jaque se desarrolló a través de escuchas telefónicas», ElSalvador.com, 30 de enero de 2017, acceso el 5 de marzo de 2019, https://historico.elsalvador.com/historico/309945/operacion-jaque-se-desarrollo-a-traves-de-escuchas-telefonicas.html
52 Ibíd.
53 Douglas Meléndez, citado por Juan Carlos Vázquez, «Fiscal denuncia mal uso de centro de escuchas telefónicas», 25 de agosto de 2016, acceso el 8 de enero de 2019, https://elmundo.sv/fiscal-denuncia-mal-uso-de-centro-de-escuchas-telefonicas/

4.3 Peticiones de información del gobierno sobre usuarios de servicios de Internet

Facebook[54], Google[55] y Twitter[56] publican informes semestrales de transparencia en los que muestran las solicitudes de información de datos sobre sus usuarios. En esta sección se realiza un análisis de la información recabada a partir de estas fuentes desde el primer semestre de 2016 hasta el primer semestre de 2018.

En el caso de Facebook, ha habido un incremento paulatino de las solicitudes tramitadas por situaciones de emergencia.

Además de la información relativa a Internet, es importante señalar que los gobiernos también solicitan información a las empresas que proveen servicios de telefonía. Según el último informe publicado por Telefónica esta entidad no recibió en 2017 solicitudes para interceptación de llamadas. Sin embargo, el propio informe señala que esto no es indicador de que no se realizaran, ya que la fiscalía salvadoreña cuenta con un centro de intervención de llamadas conectado a todos los operadores de telefonía[57]. Por otro lado, con respecto a la solicitud de metadatos, el informe reporta que en 2017 se recibieron 12.546 solicitudes y todas ellas fueron aceptadas. Esto significó un importante aumento con respecto a los años anteriores, ya que en 2015 se recibieron 5.181 solicitudes y en 2016 10.124[58].

También Millicom publica anualmente un informe de transparencia. Sin embargo, en este caso los datos se presentan agregados para toda la región centroamericana, de manera que no es posible conocer las solicitudes realizadas específicamente por El Salvador[59].

54 «Requests For User Data - SV, Facebook transparency», accedido 4 de marzo de 2019, https://transparency.facebook.com/government-data-requests/country/SV.
55 «Solicitudes de información sobre usuarios – Informe de transparencia de Google», Google, accedido 4 de marzo de 2019, https://transparencyreport.google.com/user-data/overview
56 «Information Requests», Twitter, accedido 4 de marzo de 2019, https://transparency.twitter.com/en/information-requests.html
57 Telefónica, «Report on Transparency in Communications», (Telefónica, 2018), https://www.telefonica.com/documents/153952/183394/Report-Transparency-Communications-2018.pdf/4f05af2f-1542-485f-ca5e-bb50da4a7468
58 Ibíd.
59 Millicom, «Millicom GroupLaw Enforcement Disclosure (LED) Report», (Millicom, 2018), https://www.millicom.com/AnnualReport2018Millicom/pdf/Millicom-2018-LED-Report.pdf

4.3.1 Número de peticiones de información sobre usuarios de servicios de Internet por parte del gobierno

La Tabla 3 da cuenta de las solicitudes de información realizadas por El Salvador a Google, Facebook y Twitter. Es importante considerar que cada solicitud puede contemplar una o más cuentas de usuarios. En consecuencia, la columna (S) hace referencia al número de solicitudes y la columna (U) al número de cuentas afectadas.

En el caso de Facebook, sin embargo, desde 2016 ha habido un incremento de las solicitudes aceptadas. En el primer semestre de 2016, no se aceptó ninguna solicitud. Sin embargo, para el segundo semestre de ese mismo año las solicitudes que generaron información fueron el 33,3% del total.

Tabla 3. Solicitudes de información realizadas por El Salvador a Facebook, Google y Twitter (2016 - 2018)

	2016				2017				2018	
	1er semestre		2do semestre		1er semestre		2do semestre		1er semestre	
	S	U	S	U	S	U	S	U	S	U
Facebook	6	8	3	3	10	18	16	23	23	35
Google	2	2	1	1	1		3	3	0	0
Twitter	4	4	0	0	0	0	4	4	4	11

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

La tabla muestra una tendencia a la alza en el caso de la solicitudes realizadas a Facebook. Sin embargo, aún está muy lejos de alcanzar los niveles de otros países de la región como Guatemala.

4.3.2 Naturaleza de las peticiones de información sobre usuarios de servicios de Internet por parte del gobierno

La tabla 4 muestra el tipo de solicitudes generadas por semestre. La información de cada semestre se divide en el total de solicitudes (T), las solicitudes de carácter legal (L) y las de tipo de emergencia (E). Las primeras (L) requieren que se haya establecido una solicitud legal en el país. Las segundas (E) proveen la información cuando sucede una emergencia. En el caso de Twitter, no se expresa la motivación de la solicitud.

Según se evidencia, particularmente en el caso de Facebook, ha habido un incremento paulatino de las solicitudes tramitadas por situaciones de emergencia. Así, mientras que en 2016 no se

realizó ninguna solicitud de este tipo, en el segundo semestre 2017 las solicitudes por emergencia fueron el 18,7% del total. Esta cifra aumentó al 34,8% durante el primer semestre de 2018.

Tabla 4. Solicitudes realizadas por El Salvador a Facebook, Google y Twitter según tipo de solicitud (2016 - 2018)

	2016						2017						2018		
	1er semestre			2do semestre			1er semestre			2do semestre			1er semestre		
	T	L	E	T	L	E	T	L	E	T	L	E	T	L	E
Facebook	6	6	0	3	3	0	10	10	0	16	13	3	23	15	8
Google	2	2	0	1	1	0	1	1	0	3	3	0	0	0	0
Twitter	4			0		0	0			4			4		0

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

En El Salvador se identificó empresas que ofertan productos en todas las categorías mencionadas, salvo en la de Malware. Se trata de las empresas Penlink, Verint, Cellebrite, Encase e IBM I2

4.3.3 Peticiones aceptadas por las empresas

Los informes brindados por las empresas presentan el porcentaje de solicitudes que generan datos. Se entienden que cuando generan datos, las empresas han provisto información a las agencias estatales que lo han solicitado. En este caso, es destacable que ni Google ni Twitter han generado información a partir de las solicitudes realizadas por El Salvador.

En el caso de Facebook, sin embargo, desde 2016 ha habido un incremento de las solicitudes aceptadas. En el primer semestre de 2016, no se aceptó ninguna solicitud. Sin embargo, para el segundo semestre de ese mismo año las solicitudes que generaron información fueron el 33,3% del total. El semestre en el que se aceptaron mayor número de solicitudes fue el segundo de 2017, cuando más de la mitad de las solicitudes – el 56% - fueron aceptadas.

Tabla 5. Solicitudes realizadas por El Salvador a Facebook, Google y Twitter aceptadas (2016 - 2018)

	2016				2017				2018	
	1er semestre		2do semestre		1er semestre		2do semestre		1er semestre	
Facebook	6	0%	3	33%	10	40%	16	56%	23	48%
Google	2	0%	1	0%	1	0%	3	0%	0	0%
Twitter	4	0%	0	0%	0	0%	4	0%	4	0%

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

4.4 Vigilancia en Internet

4.4.1 Evidencia de Vigilancia en Internet por parte del gobierno

En el documento "Herramientas de Vigilancia Digital Identificadas en Centroamérica" realizado paralelamente a esta investigación se describen las capacidades técnicas de diversas herramientas y su uso identificado en la región. Dichas herramientas se clasificaron en las siguientes categorías: vigilancia en la red, inteligencia de fuentes abiertas (OSINT), Malware y herramientas forenses. Además de las formas de recolectar información que emplean estas herramientas, también se considera su capacidad para analizar la información recolectada.

En El Salvador se identificó empresas que ofertan productos en todas las categorías mencionadas, salvo en la de Malware. Se trata de las empresas Penlink, Verint, Cellebrite, Encase e IBM I2 (Tabla 6). Es importante señalar que no se trata de un listado exhaustivo ya que incluye solo información que se ha podido comprobar. Sin embargo, habida cuenta de el amplio mercado y la gran cantidad de compañías que participan en el, sería esperable que otras empresas también se hayan acercado al gobierno salvadoreño.

Tabla 6. Herramientas de vigilancia y empresas proveedoras presentes en El Salvador

	Recolección de información				Análisis de información
	Red	Internet/OSINT	Malware	Forense	
Penlink	X	X			X
Verint	X	X			X
Cellebrite				X	X
Encase				X	X
IBM I2					X

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

4.5 Tecnologías de Reconocimiento Biométrico

4.5.1 Capacidad instalada en uso de tecnologías de reconocimiento biométrico

La Policía Nacional Civil (PNC) de El Salvador tiene, junto a su sistema de emergencias 911, cámaras de videovigilancia, producto de una donación de la cooperación Coreana. Según fuentes policiales, estos sistemas habrían sido altamente eficientes a la hora de favorecer la labor policial.

> "Gracias al Sistema de Video Vigilancia de la División de Emergencias 911 de la PNC, disminuyó la cifra de incidentes delincuenciales y aumentó la seguridad y la respuesta a la demanda ciudadana durante el año 2013, en el área capitalina y municipios aledaños"[60].

Por otro lado, gracias a las ya mencionadas ayudas de la cooperación internacional, se ha fortalecido el sistema de videovigilancia en la capital salvadoreña y en los 13 municipios aledaños, que conforman lo que se conoce como el Gran San Salvador. En esta área vive el 30% de la población del país. El proyecto es manejado por el centro de monitoreo de la Policía Nacional

60 «Sistema de videovigilancia policial agiliza respuesta a demanda de seguridad ciudadana», Policía Nacional Civil - Gobierno de El Salvador, accedido 11 de marzo de 2019, http://www.pnc.gob.sv/portal/page/portal/informativo/novedades/noticias/Sistema%20de%20videovigilancia%20policial%20agiliza%20respuesta%20%20a%20dem.

Civil (PNC)[61] y aunque no hay indicios de que empleen algoritmos de reconocimiento facial, sí se publicitó que poseen sistemas de lectura OCR que captan números de placas de vehículos y los cruzan automáticamente con listados de interés. Además, el sistema permite seguimiento por colores, tamaño de vehículos, conteo de personas y seguimiento de patrones.

Por otra parte, como ya se ha señalado en el punto 2, a partir del concepto de las Smart Cities (ciudades inteligentes) algunas municipalidades están instalando sus propios sistemas de videovigilancia. El ya mencionado caso de la ciudad de Santa Tecla ilustra esta situación.

4.5.2 Tipos de uso de tecnologías de reconocimiento biométrico

En el caso de El Salvador se evidencia un uso extensivo de herramientas de videovigilancia que incluyen capacidades de reconocimiento facial y de movimiento.

4.6 Drones y globos de Vigilancia

4.6.1 Capacidad de los modelos de drones y globos de vigilancia utilizados

Desde 2017, la Policía Nacional Civil (PNC) cuenta con 20 Drones Phantom 4. Además el cuerpo de agentes municipales de la Alcaldía de Santa Tecla, tendría a su disposición este tipo de equipamiento. No se cuenta, sin embargo, con información detallada y exhaustiva que permita conocer la presencia y el uso de este tipo de tecnología en el país[62].

4.7 Georeferenciación

4.7.1 Capacidad de georeferenciación

El teléfono móvil sigue siendo la forma más fácil de hacer seguimiento de georreferenciación. Además, también es relevante el reconocimiento OCR de matrículas, que permite triangular la ubicación de un vehículo.

61 López, Jaime, «Así funcionará el nuevo Centro de Control de Videovigilancia del sistema de emergencia 911», El Diario de Hoy, 25 de abril de 2018, https://www.elsalvador.com/noticias/nacional/474629/inauguran-centro-de-control-de-videovigilancia-del-sistema-de-emergencia-911/.
62 «Conoce el nuevo equipo con el que la Policía quiere combatir el crimen», El Diario de Hoy, 20 de abril de 2017, https://www.elsalvador.com/noticias/nacional/339323/conoce-el-nuevo-equipo-con-el-que-la-policia-combatira-el-crimen/.

Se ha mantenido la vigilancia física como un mecanismo de seguimiento y amedrentamiento. Periodistas de diferentes medios alternativos han documentado el seguimiento y vigilancia en los últimos años[63]. También otras personas con exposición pública, como políticos, han denunciado este tipo de situaciones[64].

63 Sergio Arauz, «El Organismo de Inteligencia del Estado persigue a periodistas - ElFaro.net», 15 de enero de 2018, https://elfaro.net/es/201801/el_salvador/21328/El-Organismo-de-Inteligencia-del-Estado-persigue-a-periodistas.htm.
64 Gabriel Labrador, «Diputados Piden Comisión Especial Para Investigar Al OIE», elfaro.net, 19 de enero de 2018, https://elfaro.net/es/201801/el_salvador/21369/Diputados-piden-comisión-especial-para-investigar-al-OIE.htm.

Guatemala

FUNDACIÓN Acceso

1. Dimensión Jurídico-Legal

1.1 Protección de la privacidad a nivel constitucional

1.1.1 Nivel de protección de la privacidad en el país a nivel constitucional Protección de la privacidad en el país a nivel constitucional

En Guatemala la protección a la privacidad tiene rango constitucional. En este sentido, los artículos 23, 24 y 25 de la Constitución[1] reconocen derechos como la inviolabilidad de la vivienda, la correspondencia, los documentos, los libros, los vehículos y las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.

Los artículos 23, 24 y 25 de la Constitución reconocen derechos como la inviolabilidad de la vivienda, la correspondencia, los documentos, los libros, los vehículos y las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.

Adicionalmente, con relación a la protección de datos, el artículo 31 del texto constitucional consigna el respeto a los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) en archivos y registros estatales, cuando plantea que:

"Toda persona tiene el derecho de conocer lo que de ella conste en archivos, la finalidad a que se dedica esta información, así como a su corrección, rectificación y actualización." (Art. 31).

En síntesis, se puede concluir que la Constitución guatemalteca protege el derecho a la intimidad y la inviolabilidad de las comunicaciones, así como el derecho a la autodeterminación informativa y el *habeas data*.

1.2 Tratados y Convenciones Internacionales

1.2.1 Nivel de protección de la privacidad en el país a nivel constitucional

En primer lugar, es importante señalar que en el caso de Guatemala los tratados y convenciones internacionales relativos a derechos humanos tienen rango supraconstitucional. Esto significa que las disposiciones de estos instrumentos internacionales prevalecen por encima de la normativa nacional e incluso de la Constitución. Así lo dispone el artículo 46 del texto constitucional:

1 Constitución Política de la República de Guatemala, 1985 con reformas de 1993,del 17 de Noviembre de 1993, Acuerdo legislativo No. 18-93 .

> "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" (Art. 46).

Por otro lado, el Artículo 44 de la norma suprema establece que los derechos reconocidos constitucionalmente son un parámetro mínimo, que no excluye el reconocimiento de otros derechos fundamentales:

> "los derechos y garantías que otorga la Constitución no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana"[2],

Entre los instrumentos internacionales que amparan los derechos humanos en espacios digitales destaca la Declaración Universal de Derechos Humanos de la Organización de Naciones Unidas (ONU). Este texto, que data de 1948, incluye disposiciones de gran relevancia como las siguientes:

> Artículo 12: 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. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.".
>
> Artículo 19: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas sin limitación de fronteras, por cualquier medio de expresión."
>
> Artículo 29: "1. Toda persona tiene deberes respecto a la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad. 2. En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática. 3. Estos derechos y libertades

2 José Osorio, «Privacidad y Acceso a la información pública en línea para Defensores y Defensoras de Derechos Humanos en: Guatemala, El Salvador, Honduras y Nicaragua» , Fundación Acceso - Medium (blog), 5 de septiembre de 2018, https://medium.com/@facceso.ca/privacidad-y-acceso-a-la-informaci%C3%B3n-p%C3%BAblica-en-l%C3%ADnea-para-defensores-y-defensoras-de-derechos-5690330c3762.

no podrán, en ningún caso, ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas".

Por otro lado, el Pacto Internacional de Derechos Civiles y Políticos también es un instrumento internacional importante en lo que concierne al derecho a la privacidad. Dicho Pacto data de 1966 y fue ratificado por Guatemala en 1992. Este texto busca garantizar el disfrute de los derechos civiles y políticos y de los derechos económicos, sociales y culturales para todas las personas. Para ello, impone a los Estados la obligación de promover el respeto universal y efectivo de los derechos y las libertades humanas, también en la utilización de medios digitales.

Posteriormente, en 1969, a nivel regional, se suscribió el Pacto de San José o la Convención Américana de Derechos Humanos (CADH). Este instrumento entró en vigor en 1978 y fue ratificado por Guatemala ese mismo año. Entre las disposiciones más relevantes de la CADH destacan las siguientes:

Artículo 13: "Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a. el respeto a los derechos o a la reputación de los demás, o

b. la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

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".

Artículo 14: "Derecho de Rectificación o Respuesta, toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentada y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.

En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiese incurrido.

Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial".

La 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.

Principio 5, Declaración de Principios sobre la Libertad de Expresión

Adicionalmente, la Comisión Interamericana de Derechos Humanos ha desarrollado la Declaración de Principios sobre Libertad de Expresión. Se trata de un instrumento de gran relevancia ya que desarrolla algunos principios básicos en materia de libertad de expresión y privacidad:

Principio 1: La libertad de expresión, en todas sus formas y manifestaciones, es un derecho fundamental e inalienable, inherente a todas las personas. Es además, un requisito indispensable para la existencia misma de una sociedad democrática.

Principio 5: La 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.

Principio 10: Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias

el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas.

1.3 Leyes, reglamentos, decretos y normativas nacionales

1.3.1 Nivel de aplicación, transparencia y control de leyes, reglamentos, decretos y normativas relacionados con el derecho a la privacidad (leyes de telecomunicaciones, leyes ciberseguridad, inteligencia de Estado (secreto de Estado), leyes antiterroristas, o reformas de ley con artículos que indican prácticas que protegen o vulneran la privacidad

Son numerosas las leyes que en Guatemala se vinculan con el derecho a la privacidad. En este sentido, el Código Penal[3] recoge en su artículo 274 una serie de delitos informáticos. Se trata de un artículo extenso que sanciona delitos como los siguientes:

> ARTICULO 274 "A". Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a dos mil quetzales, el que destruyere, borrare o de cualquier modo inutilizare registros informáticos.
>
> ARTICULO 274 "B".. La misma pena del artículo anterior se aplicará al que alterare, borrare o de cualquier modo inutilizare las instrucciones o programas que utilizan las computadoras.
>
> ARTICULO 274 "D".. Se impondrá prisión de seis meses a cuatro años y multa de doscientos a mil quetzales, al que creare un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas.
>
> ARTICULO 274 "F".. Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos.
>
> ARTICULO 274 "G".. Será sancionado con prisión de seis meses a cuatro años, y multa de doscientos a mil quetzales, al que distribuyere o pusiere en circulación programas o

3 Código Penal, del 27 de julio de 1973, Decreto 17-73.

instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación.

Por otro lado, el Código Procesal Penal[4] detalla entre los artículos 187 y 193 las condiciones en las que se pueden realizar allanamientos y registros. El artículo 190 establece que cuando se trate de dependencias cerradas, como casas de habitación o negocios, se requerirá una orden judicial escrita.

El artículo 183 de este mismo Código establece que "son inadmisibles, en especial, los elementos de prueba obtenidos por un medio prohibido, tales como la tortura, la indebida intromisión en la intimidad del domicilio o residencia, la correspondencia, las comunicaciones, los papeles y los archivos privados".

Quienes compran una tarjeta SIM deben "proporcionar al vendedor una copia física o electrónica de su documento legal de identificación personal" Art. 3, Ley de Equipos Terminales Móviles

En el ámbito de las telecomunicaciones, destaca la Ley de Equipos Terminales Móviles de 2013[5]. El artículo 3 de esta norma obliga a los operadores de telefonía a realizar un registro de sus usuarios. Si bien los operadores no son responsables de la veracidad de la información que sus usuarios les proporcionan, deben garantizar la confidencialidad de la misma, a excepción de cuando se solicite por juez competente. Este mismo artículo señala que quienes compran una tarjeta SIM deben "proporcionar al vendedor una copia física o electrónica de su documento legal de identificación personal" (Art. 3). Dicha copia quedará en posesión del vendedor y este deberá anotar "el número de SIM, es decir el número de teléfono que está adquiriendo el usuario, o suscribir en formulario respectivo que podrá ser electrónico los datos antes mencionados, debiendo conservar el vendedor esos archivos o documentación por un período de tres (3) años" (Art. 3).

Por otro lado, la Ley de Terminales Móviles prohíbe también "prestar el servicio de identificador anónimo, desconocido o privado que impida que el equipo terminal móvil receptor de una llamada nacional pueda identificar el número de línea telefónica de origen." (Art. 9).

4 Código Procesal Penal, del 7 de diciembre de 1992, Decreto 51-92.
5 Ley de Equipos Terminales Móviles, del 2 de octubre de 2013, Decreto 08-2013

Finalmente, es importante mencionar que Ley de Acceso a la Información Pública[6] dedica su capítulo VI al habeas data. En su Artículo 31 incluye la prohibición "difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que hubiere mediado el consentimiento expreso por escrito de los individuos a que hiciere referencia la información".

1.4 Normativa de seguridad nacional y ciberseguridad

1.4.1 Existencia de legislación relacionada con seguridad nacional y ciberseguridad

Guatemala cuenta con un Sistema Nacional de Seguridad consignado por la Ley Marco del Sistema Nacional de Seguridad (decreto número 18-2008)[7]. El artículo 5 de esta norma define los objetivos del Sistema de la siguiente manera:

> a) Dar coherencia y coordinación al funcionamiento de instituciones, políticas normativas y controles en materia de seguridad, en el marco del Estado de Derecho;
>
> b) Establecer una institucionalidad de máximo nivel en materia de seguridad, que permita coordinar las instituciones e integrar y dirigir las políticas públicas en esta materia; y,
>
> c) Ser el instrumento a través del cual el Estado enfrente los desafíos que en materia de seguridad se presentan (Art. 5).

El quehacer del Sistema se orienta además a partir de diferentes instrumentos como el Libro Blanco de Seguridad (Guatemala 2025 con Seguridad y Desarrollo); la Política Nacional de Seguridad; la Agenda Nacional de Riesgos y Amenazas; la Agenda Estratégica de Seguridad de la Nación; y el Plan Estratégico de Seguridad de la Nación.

En el punto 2.4.1 de este documento se exploran a mayor detalle los contenidos de varios de estos instrumentos. Sin embargo, es importante señalar que el Libro Blanco de la Seguridad coloca la tecnología como un eje esencial de la estrategia de seguridad del Estado.

6 Ley de acceso a la información pública, del 22 de octubre de 2008, Decreto 57-2008.
7 Ley marco del Sistema de Seguridad Nacional, del 1 de marzo de 2008, Decreto 18-2008.

2. Dimensión Política

2.1 Relación entre Estado, empresas y cámaras de telecomunicaciones

2.1.1 Nivel de relación entre el Estado, empresas y cámaras de telecomunicaciones

El sector guatemalteco de las telecomunicaciones ha estado fuertemente vinculado al poder político y económico. Son tres las compañías que controlan los servicios de telefonía e Internet: Tigo, Claro y Telefónica. Entre ellas es Tigo la que controla un mayor porcentaje del mercado, el 47%. Claro y Telefónica controlan el 31% y el 21% respectivamente[8].

Son tres las compañías que controlan los servicios de telefonía e Internet: Tigo, Claro y Telefónica. Entre ellas es Tigo la que controla un mayor porcentaje del mercado, el 47%. Claro y Telefónica controlan el 31% y el 21% respectivamente.

Poderosas familias guatemaltecas tienen ans importante participación en las empresas Tigo y Telefónica. En el caso de Tigo, la empresa está controlada por Mario David López Estrada, ya que tiene el 45% de las acciones. En Telefónica por su parte, un 40% de las acciones son propiedad de la Corporación Multi Inversiones de la familia Bosch Gutiérrez[9].

Es destacable además que López Estrada es una de las personas más ricas de Guatemala. De hecho, es el único guatemalteco incluido en la lista de billonarios de Forbes 400[10]. El medio independiente digital Nómada reportó que su apoyo fue crucial en una de las crisis más fuertes del gobierno de Otto Pérez Molina (2012-2015). Según reporta esta fuente de prensa, el empresario prestó su respaldo al presidente – evitando así su renuncia – a cambio de diferentes concesiones[11]. Llama la atención que este respaldo, conforme al reportaje, llegó en un momento en el que sus principales aliados daban la espalda a Pérez Molina. Por otro lado, el medio Plaza Pública señaló que en ese momento estaba en juego la concesión de la banda 4G de Internet, un negocio de gran interés para Tigo[12].

8 Martín Rodríguez Pellecer y Ana Carolina Alpírez, «El multimillonario rescata a OPM (a cambio de un tesoro)», Nómada, Guatemala. (blog), 27 de agosto de 2015, https://nomada.gt/pais/el-multimillonario-rescata-a-opm-a-cambio-de-un-tesoro/.
9 Martín Rodríguez Pellecer y Ana Carolina Alpírez, «El multimillonario rescata a OPM (a cambio de un tesoro)», Nómada, Guatemala. (blog), 27 de agosto de 2015, https://nomada.gt/pais/el-multimillonario-rescata-a-opm-a-cambio-de-un-tesoro/.
10 «Mario Lopez Estrada», Forbes, 3 de febrero de 2015, https://www.forbes.com/profile/mario-lopez-estrada/.
11 Martín Rodríguez Pellecer y Ana Carolina Alpírez, «El multimillonario rescata a OPM (a cambio de un tesoro)», Nómada, Guatemala. (blog), 27 de agosto de 2015, https://nomada.gt/pais/el-multimillonario-rescata-a-opm-a-cambio-de-un-tesoro/.
12 Bill Barreto, «La crisis política, los intereses de Tigo y "un negocio de US$250 millones"», Plaza Pública, 27 de agosto de 2015, http://www.plazapublica.com.gt/content/la-crisis-politica-los-intereses-de-tigo-y-un-negocio-de-us250-millones.

Dichos medios, además llamaron la atención sobre el hecho de que días después de la realización de esta alianza, altos cargos de Tigo pasaron a ocupar puestos de relevancia en el gobierno de Pérez Molina[13]. Así, Acisclo Valladares Urruela, ex director de Fundación Tigo e hijo del embajador guatemalteco en Londres, pasó a ser el director del Programa Nacional de Competitividad (PRONACOM). Por otro lado, Ricardo Sagastume, presidente de la Gremial de Telecomunicaciones hasta ese momento, pasó a ser Ministro de Economía. Es importante señalar, que tan solo Tigo es parte de dicha gremial, ya que ni Claro ni Telefónica participan de ella[14].

La participación de Valladares Urruela en el gobierno se habría mantenido más allá del periodo del presidente Pérez Molina. Ya que durante el mandato de Jimmy Morales (2016 - 2019) fue viceministro de Desarrollo de la Mediana y Pequeña Empresa, y después asumió como Ministro de Economía[15].

Diferentes publicaciones periodísticas destacan que el poder político de Estrada López le ha permitido que se legisle a la medida de sus intereses económicos[16]. Esto a su vez habría propiciado el crecimiento de su empresa y el acceso a contratos públicos millonarios[17].

Tigo llegó a Guatemala en 1989, bajo la inscripción de COMCEL S.A., con el apoyo del gobierno en aquel momento. En poco tiempo se convirtió en el principal proveedor de servicios de telecomunicaciones para instituciones del Estado[18].

Fuentes periodísticas revelaron que en el periodo que Valladares Urruela estuvo a cargo de PRONACOM, a Tigo le fueron adjudicados diferentes contratos. Además, algunos de ellos fueron obtenidos por un mecanismo de excepción. Por ejemplo, se le otorgó un contrato para la instalación de un sistema de cámaras de vigilancia por 1.281 millones de quetzales, además

13 Martín Rodríguez Pellecer y Ana Carolina Alpírez, «El multimillonario rescata a OPM (a cambio de un tesoro)», Nómada, Guatemala. (blog), 27 de agosto de 2015, https://nomada.gt/pais/el-multimillonario-rescata-a-opm-a-cambio-de-un-tesoro/.
14 Martín Rodríguez Pellecer y Ana Carolina Alpírez, «El multimillonario rescata a OPM (a cambio de un tesoro)», Nómada, Guatemala. (blog), 27 de agosto de 2015, https://nomada.gt/pais/el-multimillonario-rescata-a-opm-a-cambio-de-un-tesoro/.
15 https://nomada.gt/pais/entender-la-politica/el-embajador-que-ansia-ser-fiscal-tiene-un-hijo-en-problemas/
16 Luis Solano, «Los números de Tigo, el nieto de Estrada Cabrera y un negocio millonario», CMI Guatemala, 29 de agosto de 2015, https://cmiguate.org/los-numeros-de-tigo-el-nieto-de-estrada-cabrera-y-un-negocio-millonario/.
17 Ibíd.
18 Ibíd.

de otros cuatro contratos - por 1.232 millones de quetzales - para el arrendamiento de dichas cámaras de vigilancia[19].

2.1.2 Nivel de representación en cuanto a la relación entre el Estado, las empresas y las cámaras de telecomunicaciones

Según se recoge en el punto anterior, más que una participación de agentes estatales en las estructuras empresariales, en el caso de Guatemala se observa que ha habido un trasvase de funcionarios de alto nivel, sobre todo de Tigo, a cargos de gran relevancia en el Estado. De hecho, fuentes periodísticas señalan que el sector de las telecomunicaciones ha logrado reemplazar el rol y la influencia que tenía sobre los gobiernos anteriormente el Comité Coordinador de Asociaciones Agrícolas, Comerciales, Industriales y Financieras (CACIF). Así, la llegada de personeros de Tigo al gobierno de Pérez Molina habría implicado un importante cambio en la cuota de poder del sector empresarial agremiado en esta cámara[20].

2.2 Contratos entre Estados y empresas de seguridad privada

Al igual que en otros países de la región, el sector de la seguridad privada ha tenido en los últimos años un crecimiento significativo en Guatemala

2.2.1 Nivel de impacto de los contratos establecidos entre el Estado y empresas de seguridad privada

Al igual que en otros países de la región, el sector de la seguridad privada ha tenido en los últimos años un crecimiento significativo en Guatemala[21]. Este sector está reglamentado en el país por la Ley que Regula los Servicios de Seguridad Privada[22]. Dicha ley establece que para poder funcionar a derecho, las operaciones de las empresas deben ser autorizadas por la Dirección General de Servicios de Seguridad Privada (DIGESSP). La ley entró en vigor en 2010, con un objetivo de control y fiscalización de las personas naturales o empresas que brindaban servicios

19 Bill Barreto, «La crisis política, los intereses de Tigo y "un negocio de US$250 millones"», Plaza Pública, 27 de agosto de 2015, http://www.plazapublica.com.gt/content/la-crisis-politica-los-intereses-de-tigo-y-un-negocio-de-us250-millones.
20 Ibíd.
21 «Inseguridad Ciudadana en Centroamérica: El negocio de la violencia» (Guatemala, CEG, 2015), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjOq-_zjavjAhUMx1kKHe4ZDTYQFjAAegQIBRAC&url=http%3A%2F%2Fwww.ceg.org.gt%2Fimages%2Fdocumentos%2Fpublicaciones%2FInseguridad_Ciudadana.pdf&usg=AOvVaw3uXQVuhSEM5YSpIP-1j6Kv
22 Ley que Regula los Servicios de Seguridad Privada, 23 de noviembre de 2010, Decreto número 52-2010.

de seguridad, protección, transporte de valores, vigilancia, tecnología y consultoría en seguridad e investigación en el ámbito privado. Incluye disposiciones para el control de las empresas que brinden servicios de instalación y monitoreo de dispositivos electrónicos satelitales o de posicionamiento global o cualquier tipo de tecnología para la protección de personas y bienes.

Según los datos disponibles en DIGESSP, en la actualidad hay 153 empresas que cuentan con licencia de operación[23]. Adicionalmente, hay 10 empresas cuyo funcionamiento está autorizado por un acuerdo gubernativo[24] y 34 autorizadas mediante un acuerdo ministerial[25]. Sin embargo, los propios representantes del sector empresarial reconocen que hay un importante número de empresas no autorizadas, así como decenas de miles de agentes sin certificar[26].

Por otro lado, fuentes periodísticas reportan que el Estado guatemalteco destina un importante monto a la compra de servicios de seguridad privada. Así, en los últimos 14 años habría gastado 3.300 millones de quetzales – aproximadamente 429 millones de dólares – en este tipo de contrataciones. Esto sería equivalente al 13,2% del presupuesto asignado a la Policía Nacional Civil (PNC) durante el mismo periodo. También supone que 20 de cada 100 quetzales del presupuesto dedicado a seguridad ciudadana se destina a pagar estos servicios[27].

El Estado guatemalteco destina un importante monto a la compra de servicios de seguridad privada. En los últimos 14 años habría gastado 3.300 millones de quetzales – aproximadamente 429 millones de dólares – en este tipo de contrataciones.

Los años en que las empresas de seguridad privada han recibido más fondos del Estado fueron 2013 y 2014. De hecho, los fondos destinados a estas contrataciones se triplicaron, pasando de 164 millones de quetzales en 2012, a 499 millones en 2013 y 667 millones en 2014[28]. En este sentido, una investigación periodística realizada en 2018 por el medio Nuestro Diario evidenció que el ejecutivo guatemalteco destinó importantes montos de dinero a realizar prácticas de vigilancia ilegal en ese mismo periodo[29]. En consecuencia, sería razonable pensar que aumentos

23 «Empresas de seguridad privada con Licencia de Operación», DIGESSP, acceso el 10 de julio de 2019, http://digessp.gob.gt/wp-content/uploads/2019/01/licencias-JULIO-08.pdf
24 Ibíd.
25 Ibíd.
26 Suchit Chaves, «Los dueños de la seguridad privada en Guatemala», Plaza Pública, 10 de marzo de 2019. http://plazapublica.com.gt/multimedia/guate_armada/Los%20due%C3%B1os%20de%20la%20seguridad%20privada%20en%20Guatemala.html
27 Ibíd.
28 Luis Angel Sas, «Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I)», agosto de 2018, https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/.
29 Ibíd.

desproporcionados y no justificados de este tipo de partidas deberían preocupar a la población.

Por otro lado, es de destacar que un número reducido de empresas han concentrado los principales contratos estatales. Se trata de 25 empresas, de las cuales 22 brindan servicios de seguridad privada y las otras 3 ofrecen servicios de circuitos de videovigilancia. Finalmente, es relevante señalar que las contrataciones públicas son una fuente muy importante de recursos para las empresas del sector, ya que representan al menos el 40% de sus ingresos[30].

2.3 Relación de actores estatales o políticos con las directivas de empresas de seguridad

2.3.1 Nivel de relación entre el Estado y empresas de seguridad privada

Con respecto a los vínculos de las empresas de seguridad privada y agentes estatales, fuentes de prensa coinciden al señalar que el sector está ocupado en gran medida por exmilitares.

Con respecto a los vínculos de las empresas de seguridad privada y agentes estatales, fuentes de prensa coinciden al señalar que el sector está ocupado en gran medida por exmilitares. Se trata de una tendencia que empezó a consolidarse tras los Acuerdos Paz. La firma de los acuerdos implicó una reducción importante del Ejército, ante esta situación los militares retirados habrían encontrado en las empresas privadas un nuevo canal de "relacionarse con el poder económico"[31].

Para contar con un panorama más claro a este respecto, el medio virtual Plaza Pública analizó la situación en 22 empresas. Su investigación logró concluir que 15 de esas empresas tienen o han tenido a exmilitares en puestos auxiliares, de gerencia o de dirección. Además, en 9 de ellas, estos nombramientos se habrían realizado tras los Acuerdos de Paz[32].

Investigaciones realizadas con anterioridad también dan cuenta de esta situación. Así, un estudio realizado por la Organización de Estados Americanos (OEA) en 2008, evidenció que 75% de las empresas de seguridad privada guatemaltecas estaban dirigidas o gestionadas por exmilitares, mientras que el 25% restante estaba a cargo de expolicias[33].

30 Suchit Chaves, «Los dueños de la seguridad privada en Guatemala», *Plaza Pública*, 10 de marzo de 2019. http://plazapublica.com.gt/multimedia/guate_armada/Los%20due%C3%B1os%20de%20la%20seguridad%20privada%20en%20Guatemala.html
31Ibíd.
32 Ibíd.
33 Ibíd.

Es importante señalar que la presidencia de la Cámara de Seguridad de Guatemala está también a cargo de un exmilitar. Se trata de Rodolfo Muñoz Piloña, capitán retirado del Ejército[34].

Por otro lado, la ya mencionada investigación realizada por el medio digital Plaza Pública documentó evidencias de que hay una estrecha relación entre las empresas y altos cargos políticos. Así, aspectos como la seguridad presidencial han llegado a quedar en manos de empresas privadas. Por ejemplo, en el gobierno de Oscar Berger (2004-2008) el secretario de Seguridad presidencial - Daniel Salomón Azar - era también propietario de la empresa de seguridad SIS[35]. Dicha empresa había estado previamente a cargo de la seguridad de Berger durante la campaña electoral. El grupo SIS logró ganar importantes licitaciones con el Estado un año después de que Azar hubiese trabajado para el presidente. Según las cifras disponibles, habría facturado 1.281.829 quetzales[36].

La investigación realizada por el medio digital Plaza Pública documentó evidencias de que hay una estrecha relación entre las empresas y altos cargos políticos.

La situación fue similar durante el gobierno de Álvaro Colom (2008-2012). En aquella ocasión, la seguridad presidencial estuvo a cargo de Carlos Herlindo Quintanilla, a su vez dueño de la empresa Servicios de Protección Particular, la más grande del sector[37].

Posteriormente, en el Gobierno de Jimmy Morales (2016), se ha repetido este mismo patrón. El coronel retirado Jorge Ignacio López Jiménez - quien fuera el Secretario de Asuntos Administrativos y de Seguridad de la Presidencia (SAAS) durante los primeros 9 meses del Gobierno de este presidente - era también propietario de la empresa VISEGUA. Esta empresa recibió entre 2005 y 2014 contratos por al menos 32 millones de quetzales por brindar servicios de seguridad a la PNC[38]. Esta empresa ha sido denunciada además por su vinculación a actividades criminales. Concretamente, en abril de 2016, la PNC detuvo a tres agentes de seguridad privada de VISEGUA por suministrar armas de fuego a pandillas[39].

34 Ibíd.
35 Ibíd.
36 Ibíd.
37 Ibíd.
38 «Empresa de jefe de SAAS vende armas a pandilleros», *Centro de Medios Independientes*, 20 de abril de 2016, https://cmiguate.org/empresa-de-jefe-de-saas-vende-armas-a-pandilleros/
39 José Manuel Patzán, «Guardias privados proveían armas a pandilleros», *Prensa Libre*, 26 de abril de 2016, https://www.prensalibre.com/guatemala/justicia/guardias-privados-proveian-armas-a-pandilleros/.

Otra investigación, realizada también por Plaza Pública, apunta a que exmilitares vinculados a empresas de seguridad habrían contribuido económicamente a las campañas electorales de algunos candidatos. Concretamente, este sería el caso de la campaña de Jimmy Morales. El teniente coronel Alsider Antonio Arias habría aportado 75 mil quetzales a la campaña de este político. Arias era en aquel momento el representante legal de la empresa Satélites e Informática S.A. Dicha empresa también habría obtenido contratos públicos mediante la venta de equipos tecnológicos y la provisión de servicios de manejo de bases de datos al Ministerio de Gobernación. El mismo Arias había representado en un periodo anterior a la empresa Security Professional Systems S.A.[40].

2.4 Planes de Gobierno en vigencia en materia de seguridad nacional

2.4.1 Planes de gobierno vigentes relacionados con la seguridad nacional y ciberseguridad que protegen o vulneran la privacidad

Actualmente está vigente "Plan Estratégico de Seguridad de la Nación 2016-2020". Se trata de un plan de carácter general, que se plantea en articulación con el ya mencionado Libro Blanco de la Seguridad Nacional y la Política Nacional de Seguridad. En consecuencia, a partir de los desafíos planteados en Libro Blanco y los lineamientos que desarrolla la Política, el Plan detalla objetivos y acciones estratégicas[41].

Concretamente, cuenta con 13 objetivos y un total de 67 acciones. Entre estas acciones, son varias las que hacen referencia al uso de las tecnologías para fortalecer los sistemas de seguridad. Así, el Objetivo Estratégico 2 - Combatir la delincuencia común y organizada para la mejora de la protección de las personas y sus bienes – prevé entre sus actividades desarrollar y optimizar las plataformas tecnológicas institucionales interoperables y modernizar los sistemas de seguridad e inteligencia[42].

40 Daniel Villatoro García, «Los militares que financian a Jimmy Morales», *Plaza Pública*, 13 de octubre de 2015, https://www.plazapublica.com.gt/content/los-militares-que-financian-jimmy-morales.
41 «Plan Estratégico de Seguridad de la Nación 2016-2020», junio de 2016, Consejo Nacional de Seguridad.
42 Ibíd.

El Objetivo 5 - Fortalecer las relaciones internacionales para el resguardo de la soberanía e integridad territorial – por su parte, propone mejorar las capacidades de comunicación y logística para el control del espacio aéreo, marítimo y terrestre[43].

Son de particular relevancia el Objetivo 9 - Producir Inteligencia Estratégica de Estado, que coadyuve a la toma de decisiones en función de los Objetivos Nacionales - y el Objetivo 12 - Desarrollar la investigación científica, tecnológica y la transferencia de capacidades para atender integralmente la Seguridad de la Nación. El objetivo 9, busca consolidar el Sistema de Inteligencia del Estado. Para ello propone acciones como: desarrollar la carrera profesional en el Sistema de Inteligencia de Estado; desarrollar, implementar y optimizar las plataformas tecnológicas institucionales interoperables; o implementar el Centro Nacional de Inteligencia.

Guatemala cuenta también con una Estrategia Nacional de Seguridad Cibernética.

El Objetivo 12 por su parte, plantea acciones como sistematizar, estandarizar y optimizar el uso de la tecnología en las instituciones del Sistema Nacional de Seguridad; desarrollar y optimizar las plataformas tecnológicas institucionales interoperables; y desarrollar programas de investigación científica y tecnológica en materia de seguridad, con estándares internacionales[44].

Como se puede observar son numerosas las actividades enfocadas al desarrollo y el uso de la tecnología, lo cual da cuenta de su relevancia. Por otro lado, el Plan también cuenta con una propuesta dirigida al ámbito legislativo, en la cual se propone tanto la aprobación de normativa nueva, como la reforma de algunas de las leyes existentes. Entre la nueva normativa a promulgar se propone la formulación de la Ley del Sistema Nacional de Inteligencia y la Ley de Tecnología –Seguridad Cibernética[45].

Guatemala cuenta también con una Estrategia Nacional de Seguridad Cibernética. Se trata de un esfuerzo para dar contenido, en términos de directrices y objetivos, al Eje de Transformación tecnológica planteado en la Política Nacional de Seguridad. Esta estrategia cuenta con 4 ejes, 10 objetivos y 37 acciones[46].

43 Ibíd.
44 Ibíd.
45 Ibíd.
46 Estrategia Nacional de Seguridad Cibernética, 2018, Ministerio de Gobernación.

El primer eje, tiene que ver con el marco legal. El primer objetivo que se plantea en este ámbito es el de "adecuar el marco legal guatemalteco con un enfoque de prevención y manejo de riesgos cibernéticos"[47]. Para alcanzar este objetivo se proponen acciones como la inclusión de la ciberseguridad en los instrumentos del Sistema Nacional de Seguridad, la creación de una Ley contra la Ciberdelincuencia y la aprobación de una ley de privacidad y protección de datos, entre otras[48].

En este eje vinculado al marco legal también se incluyen objetivos como "promover la investigación criminal para mantener niveles aceptables de seguridad cibernética" y "determinar una estrategia de divulgación que promueva la transparencia de la información"[49].

El segundo eje está dedicado a la educación y tiene los siguientes dos objetivos: "promover la oferta educativa y formativa en Seguridad Cibernética que permita cubrir la demanda técnica y profesional en el país" y "desarrollar e implementar programas de educación para la formación y la investigación/desarrollo de la seguridad cibernética". En este sentido, se plantean principalmente acciones de diagnóstico, de diseño de programas formativos, y de implementación de capacitaciones[50].

El tercer eje está enfocado en la cultura y la sociedad. Su primer objetivo consiste en "gestionar la Seguridad Cibernética para la prevención, detección y reacción ante amenazas del ciberespacio". Para ello, una de las principales acciones previstas es la creación de Comité Nacional de Seguridad Cibernética que brinde asesoría al Consejo Nacional de Seguridad. El segundo objetivo tiene que ver con "establecer programas de sensibilización para contribuir en la gestión efectiva de riesgos y amenazas cibernéticas". Para ello, se prevé la realización de acciones de diseño e implementación de diferentes campañas y esfuerzos de sensibilización en esta materia[51].

Finalmente, el eje 4 – denominado Tecnología de la Información – cuenta con 3 objetivos: "regular la protección de los sistemas de información digital en los sectores público y privado,

47 Ibíd.
48 Ibíd.
49 Ibíd.
50 Ibíd.
51 Ibíd.

para garantizar la continuidad de sus servicios", "establecer las organizaciones de coordinación para implementar la seguridad cibernética nacional", y "diseñar un plan de protección nacional de infraestructuras críticas para fortalecer los planes de contingencia y de recuperación". Es importante señalar, que el segundo objetivo prevé la creación del Centro de Seguridad Interinstitucional de Respuesta Técnico-jurídica ante incidentes informáticos–Guatemala (CSIRT-GT)[52].

2.5 Relación de los planes de seguridad nacional y ciberseguridad con la privacidad

2.5.1 Nivel de protección o vulneración de la privacidad de los planes de gobierno vigentes relacionados con la seguridad nacional y ciberseguridad

A partir de la revisión del Plan Estratégico Seguridad de la Nación se puede concluir que dicho documento no parte de un enfoque de derechos humanos y que el resguardo de la privacidad no es una preocupación contemplada en su formulación. En consecuencia, cuando se plantea el fortalecimiento de los sistemas de inteligencia no se consideran medidas para garantizar que esto no vulnere el derecho a la privacidad de la ciudadanía.

Por otro lado, la Estrategia Nacional de Seguridad Cibernética incluye entre sus principios orientadores menciones al derecho a la privacidad y a los derechos humanos. A lo largo del plan si se considera en una de sus acciones el resguardo de la privacidad. Se trata de la acción 4, del objetivo 1.1, del eje dedicado al marco legal. Concretamente, dicha acción propone "crear, aprobar e implementar la ley de privacidad y protección de datos con referencia en convenios internacionales de derechos humanos"[53].

52 Ibíd.
53 Ibíd.

Es importante señalar además que el sector privado tiene su propia entidad de respuesta a incidentes, el CERT Cyberseg[54]. Según su propia página web, es una empresa guatemalteca, fundada en 2010, y actualmente parte de FIRST (Forum of Incident Response and Security Teams). Guatemala es el primer país de Centroamérica asociado oficialmente y uno de los primeros a nivel latinoamericano. Cyberseg a través de su Computer Emergency Response Team, (CERT, por sus siglas en inglés) recibe, analiza y responde a las notificaciones y actividades relacionadas con incidentes de seguridad de la información, para instituciones privadas de América Latina.

2.6 Uso de tecnologías de vigilancia como prueba o caso para criminalizar o judicializar

2.6.1 Casos en los que se usan evidencias de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos que ejercen sus derechos humanos y civiles

No se identificaron casos específicos en el país en los se haya deslegitimado o amenazado a personas y colectivos que ejercen sus derechos humanos y civiles con base a pruebas recabadas mediante el uso de tecnologías de vigilancia para criminalizarles.

2.6.2 Identificación de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos que ejercen sus derechos humanos y civiles

No se identificaron ejemplos concretos de tipos de tecnologías de vigilancia utilizados en el país que hayan servido para deslegitimar o amenazar a personas y colectivos que ejercen sus derechos humanos y civiles.

54 «Servicios 4x7», Ciberseg, acceso el 10 de enero de 2020, https://www.cyberseg.com

2.7 Acuerdos bilaterales y multilaterales de cooperación en materia de seguridad

2.7.1 Existencia de acuerdos bilaterales y multilaterales de cooperación en materia de seguridad

Son numerosos los acuerdos bilaterales o multilaterales sobre seguridad vigentes en Guatemala. En este sentido, uno de los más relevantes es la Declaración sobre Seguridad en las Américas (2003)[55]. Además, el país es también firmante de la Declaración de San Salvador sobre Seguridad Ciudadana en las Américas (2011)[56]. En dicha Declaración los Estados signatarios manifiestan su compromiso con el trabajo para mejorar la seguridad ciudadana. Asimismo, la Declaración plantea que los Estados deben desarrollar e implementar políticas en materia de seguridad ciudadana en un marco de respeto a los derechos humanos. También hace un llamado al fortalecimiento de los mecanismos bilaterales y multilaterales de cooperación para prevenir y enfrentar la delincuencia organizada.

Hasta 2008 no existía en Guatemala un procedimiento que permitiera, mediante una autorización judicial, esta práctica. Eso no significa que de forma previa no se realizaran escuchas. De hecho, las comunicaciones telefónicas eran escuchadas de manera ilegal por agencias de seguridad públicas o privadas.

Otro acuerdo relevante es "Acuerdo entre la Organización de las Naciones Unidas y el Gobierno de Guatemala Relativo al Establecimiento de una Comisión Internacional Contra la Impunidad en Guatemala (CICIG)"[57] adoptado en diciembre de 2006. La CICIG se instaló en Guatemala a partir de dicho acuerdo con el objetivo de:

> "apoyar y fortalecer a las instituciones del Estado de Guatemala encargadas de la investigación y persecución penal de los delitos cometidos por cuerpos ilegales y aparatos clandestinos de seguridad (ciacs): grupos criminales que han infiltrado las instituciones estatales fomentando la impunidad y socavando los logros democráticos alcanzados en Guatemala desde el final del conflicto armado interno, en la década de 1990"[58].

55 «Declaración sobre Seguridad en las Américas», 28 de octubre de 2003, http://www.oas.org/36AG/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf.
56 «Declaración de San Salvador Sobre Seguridad Ciudadana en las Américas», OEA - Organización de los Estados Americanos, 7 de junio de 2011.
57 «Acuerdo entre la Organización de las Naciones Unidas y el Gobierno de Guatemala relativo al establecimiento de una comisión internacional contra la impunidad en Guatemala (CICIG)», CICIG, 2 de diciembre de 2006, https://www.cicig.org/uploads/documents/mandato/acuerdo_creacion_cicig.pdf.
58 «¿Qué es la CICIG?», CICIG, acceso el 6 de enero de 2020, https://www.cicig.org/que-es-la-cicig/.

Este organismo ha realizado un importante trabajo en ámbitos como la lucha contra la impunidad y la corrupción, o la justicia transicional. En el ámbito de la seguridad la CICIG impulsó el proceso de reglamentación de las escuchas telefónicas con fines de investigación judicial. Hasta 2008 no existía en Guatemala un procedimiento que permitiera, mediante una autorización judicial, esta práctica. Eso no significa que de forma previa no se realizaran escuchas. De hecho, las comunicaciones telefónicas eran escuchadas de manera ilegal por agencias de seguridad públicas o privadas[59].

Por otro lado, en las últimas décadas Guatemala ha realizado diferentes acuerdos en materia de seguridad con Estados Unidos. A continuación se mencionan algunos de los más relevantes:

- "Acuerdo por canje de notas entre el Gobierno de la República de Guatemala y el Gobierno de los Estados Unidos de América referente al ejercicio PKO-North 2006"[60].
- Memorándum de entendimiento entre el Gobierno de la República de Guatemala y el Gobierno de los Estados Unidos de América para establecer el marco de cooperación en materia de prevención, control y sanción de las actividades relativas a la trata de personas[61].
- Convenio entre el Gobierno de la República de Guatemala y el Gobierno de los Estados Unidos de América para cooperar en la supresión del tráfico ilícito marítimo y aéreo de estupefacientes y sustancias psicotrópicas[62].
- Tratado entre el Gobierno de la República de Guatemala y el Gobierno de los Estados Unidos de América relativo a la devolución de vehículos y aeronaves hurtados, robados, apropiados o retenidos indebidamente[63].

59 «La CICIG: Un Instrumento Innovador Contra Redes Criminales y para el Fortalecimiento del Estado de Derecho», WOLA, marzo de 2015), https://www.wola.org/sites/default/files/CICIG%203.25.pdf
60 Heike Hasenauer, «Fostering Cooperation in Latin America», The United States Army, 19 de septiembre de 2006, https://www.army.mil/article/168/fostering_cooperation_in_latin_america.
61 «Tratados, convenios y acuerdos entre Guatemala y Estados Unidos», Embajadas de los Estados Unidos de América en Guatemala, 2013, http://guatemalaembassyusa.org/wp-content/uploads/2013/08/tratados-guatemala-bueno.pdf
62 Ibíd.
63 Ibíd.

- Carta Convenio para FY 1997 para la prevención del uso de narcóticos en Guatemala entre el Gobierno de los Estados Unidos de América y el Gobierno de la República de Guatemala[64].

El país también ha realizado acuerdos a nivel centroamericano. Así, es firmante del Tratado Marco de Seguridad Democrática en Centroamérica (1995). Este Tratado establece que "el Modelo Centroamericano de Seguridad Democrática se basa en la democracia y el fortalecimiento de sus instituciones y el Estado de Derecho (…) y en el irrestricto respeto de todos los derechos humanos en los Estados que conforman la región centroamericana"[65].

En Guatemala los gastos reservados se conocen como gastos confidenciales. Formalmente, en la actualidad se trata de una figura que no puede emplearse, ya que fueron prohibidos por una reforma constitucional realizada en 1994

También participa de la Iniciativa Regional para la Seguridad de Centroamérica (Central America Regional Security Initiative, CARSI)[66]. Esta iniciativa se desarrolla a través de la agencia de cooperación USAID y desde 2008 la iniciativa ha invertido 979 millones de dólares en los países de la región[67].

Finalmente, uno de los principales acuerdos realizados a nivel regional en últimos años es la Alianza para la Prosperidad del Triángulo Norte. Se trata de un esfuerzo en el que participan los Gobiernos de Guatemala, Honduras y El Salvador, y que se desarrolla con el apoyo del Banco Interamericano de Desarrollo (BID). Este esfuerzo busca frenar en el medio plazo la migración irregular hacia Estados Unidos. Para ello desarrolla acciones a partir de 4 ejes. Uno de ellos está dedicado a "mejorar la seguridad ciudadana y el acceso a la justicia". En el marco de esta iniciativa Guatemala ha recibido 732.7 millones de dólares en préstamos y 24.2 millones en fondos no reembolsables. En el eje relativo a la seguridad se han construido 2 sedes regionales de defensa penal, 11 juzgados de paz, 7 comisarías de policía nacional y 8 fiscalías[68].

64 Ibíd.
65 «Tratado Marco de Seguridad Democrtica en Centromerica», diciembre de 1995, https://www.teg.gob.sv/phocadownload/portal/marconormativo/leyesprincipales/Tratado%20Marco%20de%20Seguridad%20Democrtica%20en%20Centromerica.pdf.
66 «Central America Regional Security Initiative», U.S Department of State, mayo de 2018, https://www.state.gov/documents/organization/261079.pdf.
67 «Central America Regional Security Initiative», Embajada de los Estados Unidos de América en Guatemala, 20 de enero de 2017, acceso el 27 de noviembre de 2019, https://gt.usembassy.gov/our-relationship/policy-history/carsi/.
68 «Plan de la Alianza para la Properidad del Triángulo Norte - Guatemala», Banco Interamericano de Desarrollo, acceso el 20 de noviembre de 2019, https://www.iadb.org/es/alianza-para-la-prosperidad/guatemala

3. Dimensión Económica

3.1. Presupuestos nacionales destinados a seguridad y gastos reservados

3.1.1. Total de presupuesto en líneas de los presupuesto nacionales destinados a gastos reservados

En Guatemala los gastos reservados se conocen como gastos confidenciales. Formalmente, en la actualidad se trata de una figura que no puede emplearse, ya que fueron prohibidos por una reforma constitucional realizada en 1994. Así, el artículo 237 de la Constitución señala que

> "No podrán incluirse en el Presupuesto General de Ingresos y Egresos del Estado gastos confidenciales o gasto alguno que no deba ser comprobado o que no esté sujeto a fiscalización. Esta disposición es aplicable a los presupuestos de cualquier organismo, institución, empresa o entidades descentralizada o autónoma"[69].

Sin embargo, algunas fuentes de prensa han señalado que en los últimos años se han estado empleando diferentes estrategias para ocultar algunos gastos estatales. Por ejemplo, se señala que en los últimos años se han asignado más recursos al Ministerio de Defensa, y propiciando que dichos fondos no se sometan a auditorías ni a la Ley de Compras y Contrataciones del Estado. Esta discrecionalidad se estaría justificando con el argumento de que se trata de un tema de seguridad nacional[70].

El presupuesto destinado a seguridad se compone principalmente de dos partidas: la dedicada al Ministerio de la Defensa Nacional y la dedicada al Ministerio de Gobernación (...) la suma total de los montos presupuestados para estos ministerios ha representado en los últimos años entorno al 9% del presupuesto nacional total.

3.1.2 Total de presupuesto nacional destinado a seguridad

El presupuesto destinado a seguridad se compone principalmente de dos partidas: la dedicada al Ministerio de la Defensa Nacional y la dedicada al Ministerio de Gobernación. Según muestra la Tabla 2, la suma total de los montos presupuestados para estos ministerios ha representado en los últimos años entorno al 9% del presupuesto nacional total. A pesar de que el porcentaje global

69 Constitución Política de la República de Guatemala, 1985 con reformas de 1993,del 17 de Noviembre de 1993, Acuerdo legislativo No. 18-93 .

70 «Otros confidenciales», *La Hora*, 22 de agosto de 2017, acceso el 5 de octubre de 2019, https://lahora.gt/otros-confidenciales/

dedicado a la seguridad en su conjunto no ha sufrido grandes alteraciones en el último periodo, es importante señalar que en años recientes se observa una tendencia a reducir el presupuesto de defensa y aumentar el de gobernación.

Según datos del Ministerio de Finanzas de Guatemala, lo destinado a seguridad ciudadana en 2018 sería equivalente al 0.6% del Producto Interno Bruto (PIB), mientras que los destinado a defensa representaría el 0.2%.

Tabla 1. Presupuesto votado para los ramos de Defensa Nacional y Gobernación para Guatemala (2012-2018)

	Ministerio de Defensa Nacional		Ministerio de Gobernación		Total	
	Abs.	%	Abs.	%	Abs.	%
2012	1,654,912,072.0	2.78%	3,955,031,980.0	6.64%	5,609,944,052.0	9.42%
2013	2,037,900,000.0	3.04%	4,428,700,000.0	6.61%	6,466,600,000.0	9.65%
2014	2,037,900,000.0	3.04%	4,428,700,000.0	6.61%	6,466,600,000.0	9.65%
2015	2,100,300,000.0	2.97%	4,526,500,000.0	6.41%	6,626,800,000.0	9.38%
2016	2,061,647,718.0	2.90%	4,473,547,829.0	6.30%	6,535,195,547.0	9.20%
2017	1,908,316,000.0	2.48%	5,465,598,000.0	7.10%	7,373,914,000.0	9.58%
2018	1,908,316,000.0	2.48%	5,465,598,000.0	7.10%	7,373,914,000.0	9.58%

Fuente: Elaboración propia con base a datos públicos del presupuesto aprobado en el Congreso de la República en cada año. Montos en quetzales.

El presupuesto del Ministerio de Gobernación incluye rubros como administración, servicios de inteligencia civil, servicios de seguridad a la personas y su patrimonio, servicios de custodia y rehabilitación de privados de libertad, servicios migratorios, divulgación, registro de personas jurídicas, prevención de hechos delictivos contra el patrimonio, reducción del índice de homicidios o prevención de la violencia. Entre estos rubros es el de servicios de seguridad a las personas y su

patrimonio el que tiene un mayor monto asignado. De hecho, el 74% del presupuesto destinado a este Ministerio se dedica a dicho rubro[71].

Por otro lado, el Ministerio de Defensa destina líneas presupuestarias a administración; servicios de educación y salud; defensa de la soberanía e integridad territorial; prevención de hechos delictivos contra el patrimonio; apresto para la movilización de defensa, prevención y mitigación de desastres; regulación de espacios acuáticos; proyección diplomática y apoyo en misiones de paz; o reducción del índice de homicidios. En este caso, el monto principal del presupuesto se dedica a la defensa de la soberanía territorial. Esta línea presupuestaria representa el 41,5% del presupuesto total del Ministerio[72].

3.1.3 Instituciones Estatales que tienen líneas de presupuesto destinadas a seguridad, gastos y reservados

Como ya se ha señalado, todas las instituciones del Estado cuentan con una partida presupuestaria dedicada a gastos de seguridad. No se ha logrado acceder a información desagregada que de cuenta del gasto de cada institución en este ámbito. Sin embargo, la importante inversión que realizan las instituciones en su conjunto por conceptos como custodia de instalaciones, da cuenta de que no se trata de un gasto marginal (Ver apartado 2.2.1).

3.1.4 Montos de contratos relacionados con compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

No se ha conseguido acceder a información presupuestaria desagregada. En consecuencia, no ha sido posible calcular el monto de los contratos destinados a compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia.

3.1.5 Instituciones encargadas de los contratos relacionados con compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

Como ya se ha señalado, en general el presupuesto no es lo suficientemente transparente, de manera que no se puede detectar la compra de bienes o servicios de seguridad que incluyan

71 Ley del Presupuesto General de Ingresos y Egresos del Estado para el Ejercicio Fiscal 2017, 2016, Decreto número 50-2016.
72 Ibíd.

tecnologías de vigilancia. Así, las entidades estatales pueden adquirir tecnología de vigilancia y registrarlas en líneas presupuestarias generales "software", "comunicaciones" o "seguridad". Por ejemplo, las compras de equipamiento especializado en pruebas forenses, como el UFED Celebrite o el intento de compra de licencias de Pen Link, estaban bajo la categoría de computación y telecomunicaciones[73].

3.2 Empresas proveedoras de bienes y servicios en materia de tecnologías de vigilancia

3.2.1 Empresas que tienen los contratos relacionados de compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

Entre las principales empresas dedicadas a la venta de tecnología de vigilancia desde 2012, destaca COMSUR. Esta sociedad anónima constituida en 2012 vendió una plataforma de software integral de inteligencia a la Secretaría de Inteligencia Estratégica del Estado (SIE) ese mismo año. Según el contrato firmado entre ambas entidades, se adquirió software de Inteligencia Memex Serie VI por un poco más de 299 mil dólares[74].

Esta misma empresa vendió a la Policía Nacional Civil (PNC) 110 Cámaras fotográficas digitales, 51 de video, 51 micrograbadoras, 28 lapiceros tipo espía y 25 gorras con cámara, por un monto de 114 mil dólares[75].

Por otro lado, también es relevante el Grupo ITD, quien desde 2015 ha sido proveedor del Estado. A partir de ese año ha vendido a instituciones del Estado desde certificados de seguridad hasta equipos de análisis forense digital UFED Touch 2. Entre sus clientes están diferentes ministerios, instituciones autónomas y municipalidades[76].

73 Rafael Bonifaz, «Herramientas de Vigilancia Digital Identificadas en Centroamérica», Fundación Acceso, 2019.
74 «NOG: 2333260», Guatecompras - Sistema de Contrataciones y Adquisiciones del Estado de Guatemala, octubre de 2012, http://www.guatecompras.gt/Concursos/consultaConcurso.aspx?nog=2333260&o=0&lper=2012&lprv=701916.
75 «NOG: 2379716», Guatecompras - Sistema de Contrataciones y Adquisiciones del Estado de Guatemala, noviembre de 2012, http://www.guatecompras.gt/Concursos/consultaConcurso.aspx?nog=2379716&o=0&lper=2012&lprv=701916.
76 «Grupo ITD, Sociedad Annónima», Guatecompras - Registro de Proveedores - Datos de un proveedor, accedido 12 de marzo de 2019, http://www.guatecompras.gt/proveedores/consultaDetProvee.aspx?rqp=8&lprv=4728070.

Por otra parte, hay compras de programas con la capacidad de realizar análisis de grandes cantidades de datos como el I2 de IBM. Este tipo de programas pueden ser utilizados para procesar grandes cantidades de datos como toda la información de casos del Ministerio Público, permitiendo construir redes de personas de interés en corto tiempo[77].

3.2.2 Nivel de posibilidad de contrataciones o interés de contratar bienes y servicios en tecnologías de vigilancia

La posibilidad de que las instituciones del Estado contraten bienes o servicios en tecnologías de vigilancia es alta, ya que el mercado privado de seguridad en Guatemala tiene una importante oferta de este tipo de productos.

Entre las evidencias disponibles de compras realizadas, destaca que el INACIF compró programas de análisis forense digital[78] a la empresa Grupo ITD, S.A.[79]. La compra incluyó dos computadoras de alta potencia especializada para la recuperación de evidencia forense en dispositivos, un equipo para análisis y manejo forense de teléfonos celulares, dos kits de bloqueadores de escritura, un duplicador forense de datos y un software para manejo de evidencia digital. Las compras se realizaron en el formato de compra directa, por ser los únicos proveedores en el mercado Sistemas Aplicativos (SISAP)[80] y Grupo ITD, S.A[81].

Según Hellen Mack Chang de la Fundación Mirna Mack "Estamos ante un caso más de voluntades políticas y confianza en las instituciones que tienen estos tipos de programas"[82]. Esto significa que no se descarta la posibilidad de que el Estado o terceros adquieran tecnología para realizar vigilancia.

77 «NOG: 7622201», Guatecompras - Sistema de Contrataciones y Adquisiciones del Estado de Guatemala, 7 de marzo de 2018, http://www.guatecompras.gt/concursos/consultaConcurso.aspx?nog=7622201&o=4.
78 «SECRETARIA EJECUTIVA DE LA INSTANCIA COORDINADORA DE MODERNIZACIÓN DEL SECTOR JUSTICIA PRESTAMO BID 1905/OC-GU», septiembre de 2015, http://www.guatecompras.gt/concursos/files/911/4551192%40Solicitud%20o%20Requerimiento.pdf
79 «NOG: 4551192», Guatecompras - Sistema de Contrataciones y Adquisiciones del Estado de Guatemala, 19 de febrero de 2016, http://www.guatecompras.gt/concursos/consultaConcurso.aspx?nog=4551192&iEnt=455&iUnt=5&iTipo=4&o=22.
80«Sisap - SISAP», SISAP, acceso 12 de marzo de 2019, https://www.sisap.com/.
81 «ITD», ITD, acceso12 de marzo de 2019, https://intertd.com/.
82 Hellen Mack Chang, Entrevista a Hellen Mack Chang, entrevistad por Rodrigo Baires, noviembre de 2018.

En este sentido, Elvyn Díaz, residente del Instituto de Estudios Comparados en Ciencias Penales de Guatemala (ICCPG) plantea "que las instituciones tengan el equipamiento tecnológico permite mayor rapidez en la investigación y disminuye la posibilidad de filtración de información a terceros"[83]. Para Díaz, a nivel público "no se debería de derivar a terceros el uso de esta tecnología de vigilancia en investigaciones que realice el Estado"[84].

4. Dimensión Tecnológica

4.1 Utilización de malware o spyware dentro del país

4.1.1 Evidencias de ataques o uso de malware, spyware, phishing u otras.

Una investigación realizada por el medio "Nuestro Diario" en 2018 denunció el uso del software de NSO y de software provisto por la empresa Hacking Team en Guatemala

Una investigación realizada por el medio "Nuestro Diario" en 2018 denunció el uso del software de NSO y de software provisto por la empresa Hacking Team en Guatemala[85]. Si bien era conocido el uso de NSO en el vecino país de México, esta fue la primera vez que se mencionó el uso de esta herramienta en Centroamérica.

En el caso de Hacking Team una investigación realizada por la organización Derechos Digitales – basada en una filtración de correos y documentos – se menciona que esta empresa realizó negociaciones con el país. Así, la Dirección de Análisis Criminal habría buscado capacitar a 200 agentes para que pudieran utilizar las herramientas de Hacking Team. En este caso fue Ori Zoller – quien también aparece como proveedor en las publicaciones realizadas por Nuestro Diario – quién habría liderado la negociación[86]. Sin embargo, no hay evidencia de que las compras llegaran a concretarse.

83 Elvyn Díaz, Entrevista a Elvyn Díaz, entrevista realizada en noviembre de 2018.
84 Ibíd.
85 Luis Angel Sas, «Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I)», agosto de 2018, https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/.
86 Pérez de Acha, Gisela, «Hacking Team Malware para la Vigilancia en América Latina», Derechos Digitales, 2016.

4.2 Escuchas telefónicas dentro del país

4.2.1 Casos en los que se evidencia el uso de escuchas telefónicas.

Diferentes artículos de prensa han reportado situaciones relacionadas con escuchas ilegales. En 2013, el periódico La Prensa, reportó la existencia de servicios de escuchas ilegales. Concretamente, mencionaba una empresa que ofrecía la venta de celulares con tecnología que permitía espiar a la víctimas, que recibirían el dispositivo como regalo. Por otro lado, también hacía referencia a la posibilidad de emplear malware para la realización de las escuchas. Los costo de este tipo de servicios rondaban en aquel momento los 10.000 quetzales[87].

Años más tarde, en 2018, el periódico Nuestro Diario reveló la existencia de una estructura de espionaje, que empleaba diversa tecnología para desarrollar prácticas de vigilancia ilegal. Las escuchas teléfonicas eran también parte de estas prácticas[88].

En 2019 una investigación realizada por la CICIG evidenció la realización de escuchas telefónicas ilegales por parte de la empresa TIGO

Más recientemente, en 2019 una investigación realizada por la CICIG evidenció la realización de escuchas telefónicas ilegales por parte de la empresa TIGO. Los hallazgos de dicha investigación arrojaron "indicios relevantes y significativos que permiten inferir la práctica de seguimientos, escuchas e intervenciones de teléfonos celulares sin la debida orden judicial, por parte de funcionarios de la empresa telefónica TIGO"[89]. Los resultados de dichas escuchas eran reportados al ya mencionado Acisclo Valladares Urruela[90].

Por otro lado, también es importante señalar que en enero de 2018, diferentes sectores de la sociedad civil denunciaron la existencia de una red ilegal de intervenciones a las comunicaciones[91].

Finalmente, es importante señalar que un informe realizado por la organización no gubernamental Oficina en Washington para Asuntos Latinoamericanos señala que "en Guatemala las

87 Luis Ángel Sas, «Escucha telefónica cuesta Q10 mil – Prensa Libre», Prensa Libre, 29 de julio de 2013, https://www.prensalibre.com/guatemala/justic

88 Luis Angel Sas, «Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I)», agosto de 2018, https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/.

89 «Espionaje y escuchas ilegales en la compañía TIGO», CICIG, 2019, https://www.cicig.org/wp-content/uploads/2019/08/DENUNCIA_02_Espionaje.pdf

90 Ibíd.

91 Evelyn Boche, «Denuncian red ilegal de escuchas telefónicas», El Periódico, 1 de agosto de 2018, https://elperiodico.com.gt/nacion/2018/08/01/denuncian-red-ilegal-de-escuchas-telefonicas/.

comunicaciones telefónicas se escuchaban de manera ilegal por agencias de seguridad públicas o privadas para fines ilícitos o delictivos"[92].

4.3 Peticiones de información del gobierno sobre usuarios de servicios de Internet

Diferentes proveedores de servicios de Internet como Facebook[93], Google[94] y Twitter[95] publican informes semestrales de transparencia donde muestran las solicitudes de información de datos sobre sus usuarios que realizan los Estados. En esta sección se hace un análisis de la información recabada a partir de estas fuentes, desde el primer semestre de 2016 hasta el primer semestre de 2018 que es el último informe publicado al momento de escribir este documento.

4.3.1 Número de peticiones de información sobre usuarios de servicios de Internet por parte del gobierno

Las solicitudes de información que se realizan pueden contemplar una o más cuentas de usuarios. En la siguiente tabla se ve el resumen de solicitudes (S) y las cuentas de usuarios afectadas (U). Llama la atención el caso de Facebook, ya que supera de largo a las otras empresas. Además, el número de solicitudes es significativamente mayor a la reportada para otros países. En el primer semestre de 2017, por ejemplo, se realizaron 66 solicitudes en Facebook que afectaron a 738 cuentas en esta plataforma.

92 «La CICIG: Un Instrumento Innovador Contra Redes Criminales y para el Fortalecimiento del Estado de Derecho» (WOLA, marzo de 2015), https://www.wola.org/sites/default/files/CICIG%203.25.pdf.
93 Requests For User Data - GT, acceso el 4 de marzo de 2019, https://transparency.facebook.com/government-data-requests/country/GT.
94 «Solicitudes de información sobre usuarios – Informe de transparencia de Google», Google, accedido 4 de marzo de 2019, https://transparencyreport.google.com/user-data/overview.
95 Information Requests, accedido 4 de marzo de 2019, https://transparency.twitter.com/en/information-requests.html.

Tabla 2. Solicitudes de información realizadas por Guatemala a Facebook, Google y Twitter (2016 - 2018)

	2016				2017				2018	
	1er semestre		2do semestre		1er semestre		2do semestre		1er semestre	
	S	U	S	U	S	U	S	U	S	U
Facebook	16	45	34	82	66	738	82	208	169	338
Google	0	0	2	2	0		0		6	10
Twitter	0	0	5	5	2	2	1	1	1	1

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

En 2019 una investigación realizada por la CICIG evidenció la realización de escuchas telefónicas ilegales por parte de la empresa TIGO

4.3.2 Naturaleza de las peticiones de información sobre usuarios de servicios de Internet por parte del gobierno

En la siguiente tabla se puede ver una división según tipo de solicitudes generadas por semestre. La información de cada semestre se divide en el total de solicitudes (T), las solicitudes de carácter legal (L) y las de tipo de emergencia (E). Las solicitudes de tipo legal requieren que se haya establecido una solicitud legal en el país. Las solicitudes de emergencia proveen la información cuando sucede una emergencia. En el caso de Twitter, esta empresa no detalla la motivación de las solicitudes que recibe.

Tabla 3. Solicitudes realizadas por Guatemala a Facebook, Google y Twitter según tipo de solicitud (2016 - 2018)

	2016						2017						2018		
	1er semestre			2do semestre			1er semestre			2do semestre			1er semestre		
	T	L	E	T	L	E	T	L	E	T	L	E	T	L	E
Facebook	29	19	7	34	24	10	66	50	16	82	45	17	169	87	81
Google	0	0	0	2	0	2	0	0	0	0	0	0	6	2	0
Twitter	0	-	-	5	0	0	2	-	-	1	-	-	1	-	-

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

4.3.3 Peticiones aceptadas por la empresa de la plataforma al Gobierno

La siguiente tabla presenta el porcentaje de solicitudes que generan datos. Se entiende que cuando generan datos, las empresas han provisto información a las agencias estatales que la han solicitado.

Tabla 4. Solicitudes realizadas por Guatemala a Facebook, Google y Twitter aceptadas (2016 - 2018)

	2016				2017				2018	
	1er semestre		2do semestre		1er semestre		2do semestre		1er semestre	
Facebook	26	85%	34	50%	66	62%	82	73%	169	62%
Google	0	0%	2	0%	0	0%	0	0%	6	67%
Twitter	0	0%	5	0%	2	50%	1	0%	1	0%

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

En 2017 Telefónica recibió 765 solicitudes de intercepción de comunicaciones telefónicas, o de otro tipo. Entre ellas, fueron rechazadas 65

Por otro lado, también algunas de las empresas proveedoras de servicios de Internet y telefonía (IPS por sus siglas en inglés) publican en sus informes de transparencia información relativa a la solicitudes de información que realizan los Estados. Entre las empresas que operan en Guatemala solo se han encontrado disponibles los informes de Millicom (Tigo) y Telefónica.

Según reporta el informe de Millicom del año 2018, los datos agregados de Honduras, Costa Rica, El Salvador y Guatemala muestran que las solicitudes de metadatos en el conjunto de estos cuatro países se han reducido entre entre 2016 y 2018. Así, se pasó de 16.758 a 11.278 solicitudes[96]. A pesar, de la reducción en el último bienio, sin embargo, la cifra revela una importante demanda de este tipo de información. Sin embargo, el hecho de que los datos no están desagregados por país, impide conocer cuál ha sido el comportamiento en cada caso. Es más, aunque la cifra global se haya reducido podría haber aumentado en alguno de los países si se considera individualmente.

Por otro lado, Telefónica, sí reporta información específica de Guatemala. En este caso, señala que en 2017 recibió 765 solicitudes de intercepción de comunicaciones telefónicas, o de otro tipo.

96 «2018 Millicom GroupLaw Enforcement Disclosure (LED) Report», Millicom, 2018, https://www.millicom.com/AnnualReport-2018Millicom/pdf/Millicom-2018-LED-Report.pdf

Entre ellas, fueron rechazadas 65. Es importante señalar que el número de este tipo de solicitudes ha aumentado significativamente en los últimos años, ya que en 2013 fueron 310. Es decir, en 5 años se ha duplicado el número de solicitudes.

Las solicitudes de acceso a metadata también son numerosas. En 2017, se solicitó este tipo de información en 3.628 ocasiones. Asimismo, ha habido un aumento importante con respecto a 2013, ya que en aquel año las solicitudes realizadas fueron 2.172. En este caso no se denegó ninguno de los accesos[97].

La ya mencionada investigación realizada por "Nuestro Diario" en agosto de 2018 identificó el uso de herramientas como Penlink, Circles o Conceptus.

4.4 Vigilancia en Internet

4.4.1 Evidencia de vigilancia en Internet por parte del gobierno

En el año 2013, una investigación realizada por por Citizenlab de la Universidad de Toronto identificó que en Guatemala se ejecutaban servidores del producto BlueCoat, los mismos que podrían servir para vigilar la actividad en Internet[98].

Por otro lado, la ya mencionada investigación realizada por "Nuestro Diario" en agosto de 2018[99] identificó el uso de herramientas como Penlink, Circles o Conceptus.

En el caso Penlink se puede confirmar en el portal Guatecompras, que en 2017 la Dirección General de Inteligencia Civil del Ministerio de Gobernación quiso adquirir dicho software. El proceso se canceló aduciendo lo siguiente:

> "Se finaliza anulado el presente concurso, debido a que se van a modificar y ampliar las especificaciones técnicas, derivado a lo complejo del Software solicitado"[100].

La siguiente tabla tomada del artículo "Herramientas de Vigilancia Digital Identificadas en Centroamérica"[101] se puede ver las capacidades para la vigilancia identificadas en Guatemala.

97 «Report on transparency in communications 2017», Telefónica, 2017, https://www.telefonica.com/en/web/responsible-business/report-on-transparency-in-communications
98 Morgan Marquis-Boire *et* al., «Some Devices Wander by Mistake: Planet Blue Coat Redux», julio de 2013, https://citizenlab.ca/2013/07/planet-blue-coat-redux/.
99 Luis Angel Sas, «Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I)», agosto de 2018, https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/.
100 «NOG: 6557961», Guatecompras - Sistema de Contrataciones y Adquisiciones del Estado de Guatemala, accedido 15 de enero de 2019,
101 Rafael Bonifaz, «Herramientas de Vigilancia Digital Identificadas en Centroamérica», Fundación Acceso, 2019.

Tabla 5. Herramientas de vigilancia y empresas proveedoras presentes en Guatemala

	Recolección de información				Análisis de información
	Red	Internet/OSINT	Malware	Forense	
Penlink	X	X			X
BlueCoat	X				
Circles	X				
Conceptus		X			
NSO			X		
Hacking Team			X		

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

El Ministerio de Gobernación instaló en 2014 3.431 cámaras de vigilancia en diferentes ciudades del país.

4.5 Tecnologías de reconocimiento biométrico

4.5.1 Capacidad instalada en uso de tecnologías de reconocimiento biométrico

La aplicación de sistemas de videovigilancia no es nueva en Guatemala. Así, desde 2010 el programa Alertos - impulsado desde CACIF (Comité Coordinador de Asociaciones Agrícolas, Comerciales, Industriales y Financieras) y la Fundación para el Desarrollo de Guatemala (FUNDESA) dentro de la iniciativa "Mejoremos Guate" - ha promovido la instalación de cámaras para la videovigilancia en diferentes zonas[102].

Por otro lado, el Ministerio de Gobernación instaló en 2014 3.431 cámaras de vigilancia en diferentes ciudades del país. Así, anunció la colocación de otras 1.569 en 2015, en el marco de un proyecto de videovigilancia cuyo objetivo era la instalación de un total para alcanzar 7.800 cámaras[103].

102 «Alertos», Mejoremos Guate, acceso el 20 de febrero de 2019, http://www.mejoremosguate.org/cms/es/que-estamos-haciendo/alertos

103 «Guatemala fortalece la seguridad ciudadana con la instalación de 3.431 cámaras de vigilancia en 2014», Teleprensa, acceso el 20 de febrero de 2019, https://www.teleprensa.com/guatemala/guatemala-fortalece-la-seguridad-ciudadana-con-la-instalacion-de-3431-camaras-de-vigilancia-en-2014.html

Por otro lado, con el apoyo de la Embajada de Estados Unidos, se han instalado cámaras de videovigilancia que son monitoreadas por las policías municipales de tránsito de diferentes alcaldías. Este es el caso de Salcajá, Quetzaltenango[104] y de otras municipalidades[105].

No obstante, las personas entrevistadas señalan no tener conocimiento sobre uso de tecnologías de reconocimiento biométrico. En este sentido, se señala que actividades oficiales con asistencia masiva de público, policías y soldados tenían listados contra los que verificaban los documentos de identidad de quienes pretendían ingresar a las actividades de la independencia. "Si tuvieran reconocimiento facial, con la cantidad de cámaras que hay en el palacio Nacional de Cultura, donde funciona oficinas estatales y en la misma plaza no necesitarían verificar listados", razonó un defensor de derechos humanos.

Finalmente, es importante señalar que existe una demanda desde la sociedad civil con respecto a la regulación de la videovigilancia con un enfoque de derechos humanos y de respeto al derecho a la privacidad y los derechos ARCO[106].

4.5.2 Tipos de uso de tecnologías de reconocimiento biométrico

Si bien se han identificado capacidades de videovigilancia, no se han encontrado indicios de uso de software de reconocimiento facial.

4.6 Drones y globos de vigilancia

4.6.1 Capacidad de los modelos de drones y globos de vigilancia utilizados

La Policía Nacional Civil (PNC) de Guatemala ha publicitado que posee 10 drones que utiliza en casos de operativos policiales o contextos de aglomeración[107]. Por lo descrito en las notas de

104 «Inauguran centro de monitoreo de cámaras en Salcajá», Stereo 100, 31 de octubre de 2017, https://stereo100.com.gt/inauguran-centro-de-monitoreo-de-camaras-en-salcaja/.
105 «Investigadores capacitan a policías municipales y de tránsito en el manejo de cámaras de videovigilancia», Ministerio de Gobernación, 26 de julio de 2018, http://mingob.gob.gt/investigadores-capacitan-a-policias-municipales-y-de-transito-en-el-manejo-de-camaras-de-videovigilancia/.
106 Rony Ríos, «Buscan regular el uso de cámaras de videovigilancia», El Periódico, 19 de octubre de 2017, https://elperiodico.com.gt/nacion/2017/10/19/buscan-regular-el-uso-de-camaras-de-videovigilancia/.
107 Roni Pocón, «La PNC vigilará en directo sobre 10 puntos a 500 metros de altura», Prensa Libre, 28 de marzo de 2018, https://www.prensalibre.com/guatemala/justicia/la-pnc-vigilara-en-directo-sobre-10-puntos-a-500-metros-de-altura/.

prensa, el operador de los aparatos mantiene comunicación radial con elementos en tierra para reportar movimientos sospechosos[108]. De hecho este tipo de aparatos han sido empleados en manifestaciones públicas[109] o en el marco de la atención de emergencias de desastres como erupciones volcánicas[110].

La Policía Nacional Civil (PNC), no es la única dependencia estatal que posee este tipo de herramientas tecnológicas. Por ejemplo, el Ministerio de Agricultura y Ganadería (MAGA) posee 17 drones con capacidad de hacer tomas de temperaturas y gran independencia de vuelo[111].

Es importante destacar, que defensores de derechos humanos entrevistados reportan sospechas de prácticas de vigilancia por medio de drones.

Concretamente, hacen referencia a una reunión realizada en una vivienda en el interior del país. La casa contaba con un jardín central. En un momento determinado escucharon un ruido extraño como de unas aspas de un helicóptero y al salir vieron un dron sobrevolando el jardín de la vivienda. Así, sospechan que el dron tomó imágenes de la reunión y de quienes participaron en ella. Sin embargo, no pudieron constatar quién manejaba el dron, de manera que no tienen certeza de si se trató de un operativo de vigilancia desde el Estado o no.

4.7 Georeferenciación

4.7.1 Capacidad de georeferenciación

El teléfono móvil sigue siendo la estrategia para la georeferenciación más sencilla. También es accesible el reconocimiento OCR de matrículas, que permite triangular la ubicación de una

108 «El dron que es el arma secreta de la PNC contra los extorsionistas», Soy502, 21 de abril de 2017, https://www.soy502.com/articulo/asi-como-pnc-localiza-viviendas-extorsionadores-32419.
109 «El "drone" que usa la PNC para resguardar a los diputados», Soy502, 13 de noviembre de 2018, https://www.soy502.com/articulo/drone-pnc-resguardar-diputados-63338.
110 Nancy Alvarez, «PNC ubica por medio de drones un área afectada por la erupción a la que no se había accedido», Publinews, 6 de junio de 2018, https://www.publinews.gt/gt/noticias/2018/06/06/pnc-ubica-medio-drones-una-comunidad-afectada-la-erupcion-la-no-se-habia-accedido.html.
111 «Insumos - Compras MAGA», accedido 12 de marzo de 2019, https://sistemas.maga.gob.gt/compras/Insumos?page=414&sortOrder=CodigoPresentacion_desc.

persona en el territorio. Por otro lado, no hay pruebas técnicas que den cuenta del uso de aparatos GPS para dar seguimiento a personas específicas.

Si hay evidencia, sin embargo, de que se ha mantenido la vigilancia física como un mecanismo de seguimiento y amedrentamiento. "El seguimiento es físico, es visible. Después de los intentos de sacar a la CICIG del país, vimos eso: policías uniformados siguiéndonos, sin ningún tipo de intento de esconderse. Lo veo cómo una forma de amedrentarnos", comentó la defensora de derechos humanos Helen Mack Chang. En enero de 2019, Mack Chang denunció públicamente que estaba siendo vigilada. Esto levantó una alerta en la comunidad de derechos humanos de la región[112].

De forma legal, las bitácoras de llamadas, el posicionamiento geográfico y el rastreo de GPS de teléfonos móviles han servido para ligar a procesos a estructuras delincuenciales en las que incluso participaban agentes de la sección de Reconocimiento, Vigilancia y Seguimiento de la Policía Nacional Civil de Guatemala, quedando demostrado el valor como pruebas técnicas en casos de corrupción estatal[113].

El Ministerio Público (MP) ha promocionado el uso de tecnología para analizar patrones y modus operandi de estructuras criminales, identificación de rasgos físicos de presuntos delincuentes y automotores e información de dispositivos móviles, en casos de extorsiones a comerciantes y empresarios de transporte colectivo[114][115].

112 «#AlertaDefensoras GUATEMALA / Vigilancia, persecución e intimidación contra Helen Mack, directora de la Fundación Myrna Mack», Iniciativa Mesoamericana de Mujeres Defensoras de Derechos Humanos (blog), 18 de enero de 2019, https://im-defensoras.org/2019/01/alertadefensoras-guatemala-vigilancia-persecucion-e-intimidacion-contra-helen-mack-directora-de-la-fundacion-myrna-mack/.

113 «Expolicías y particulares deben enfrentar proceso penal por allanamiento ilegal», Ministerio Público de Guatemala, 10 de octubre de 2018, https://www.mp.gob.gt/noticias/2018/10/10/expolicias-y-particulares-deben-enfrentar-proceso-penal-por-allanamiento-ilegal/.

114 «MP dirige Operativo Rescate del Sur para desarticular estructura de extorsionistas», Ministerio Público de Guatemala, 2 de mayo de 2016, https://www.mp.gob.gt/noticias/2016/05/02/mp-dirige-operativo-rescate-del-sur-para-desarticular-estructura-de-extorsionistas/.

115 «Ministerio Público logra que mujer enfrente proceso penal por el delito de extorsión», Ministerio Público de Guatemala, 28 de febrero de 2018, https://www.mp.gob.gt/noticias/2018/02/28/ministerio-publico-logra-que-mujer-enfrente-proceso-penal-por-el-delito-de-extorsion/.

Honduras

FUNDACIÓN Acceso

1. Dimensión Jurídico-Legal

1.1 Protección de la privacidad a nivel constitucional

1.1.1 Nivel de protección de la privacidad en el país a nivel constitucional Protección de la privacidad en el país a nivel constitucional

Si bien el derecho a la privacidad no se menciona de manera explícita en el texto constitucional hondureño[1], varios de sus artículos contienen disposiciones para su resguardo. En este sentido, el artículo 76 plantea que

> "se garantiza el derecho al honor, a la intimidad personal, familiar y a la propia imagen" (Artículo 76).

Si bien el derecho a la privacidad no se menciona de manera explícita el texto constitucional hondureño, varios de sus artículos contienen disposiciones para su resguardo

Por otro lado, el artículo 99 establece la inviolabilidad del domicilio, mientras que en el artículo 100 se consigna la inviolabilidad y el secreto de las comunicaciones, "en especial de las postales, telegráficas y telefónicas, salvo resolución judicial" (Artículo 100).

Además, la Constitución establece en su artículo 182 la garantía de *Hábeas Data*. Al amparo de esta garantía

> "Toda persona tiene el derecho 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 y, en caso de que fuere necesario, actualizarla, rectificarla y-o enmendarla" (Art. 182).

Según establece este mismo artículo, las acciones de *Hábeas Data* se ejercerán sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, ante la Sala de lo Constitucional de la Corte Suprema de Justicia.

1 Constitución Política de la República de Honduras, 12 de enero de 1982, Decreto número 131.

1.2 Tratados y Convenciones Internacionales

1.2.1 Cantidad y nivel de implicación de Tratados / Acuerdos / Convenciones y otros firmados por el país relacionados con la privacidad

Las normas internacionales cuentan en Honduras con rango supraconstitucional. Esto significa que la legislación y la Constitución deben adecuarse a las disposiciones de los convenios y las convenciones que se ratifican. Además, en caso de conflicto, siempre prevalecerá el convenio internacional frente a la normativa nacional e incluso frente a la Constitución[2].

En caso de conflicto, siempre prevalecerá el convenio internacional frente a la normativa nacional e incluso frente a la Constitución

La Declaración Universal de Derechos Humanos de la Organización de Naciones Unidas (ONU), adoptada 1948, reconoce los siguientes derechos:

> Artículo 12: 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. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".
>
> Artículo 19: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas sin limitación de fronteras, por cualquier medio de expresión".
>
> Artículo 29: "1. Toda persona tiene deberes respecto a la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad. 2. En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática. 3. Estos derechos y libertades no podrán, en ningún caso, ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas".

2 Humberto Hendersor, «Los tratados internacionales de derechos humanos en el orden interno: la importancia del principio *pro homine, Revista IIDH,* 2004, https://www.corteidh.or.cr/tablas/R06729-3.pdf.

También es relevante el Pacto Internacional de Derechos Civiles y Políticos (1966). Este tratado, ratificado por Honduras en 1981, impone a los Estados la obligación de promover el respeto universal y efectivo de los derechos y libertades, inclusive en el ámbito de los medios digitales.

A nivel regional, en 1969 se suscribió la Convención Interamericana de Derechos Humanos, también conocida como el Pacto de San José. Está Convención entro en vigor en 1978 y fue ratificada por Honduras en 1977. Entre las principales disposiciones de este tratado destacan las siguientes:

> Artículo 13: Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
>
> El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:
>
> a. el respeto a los derechos o a la reputación de los demás, o
>
> b. la protección de la seguridad nacional, el orden público o la salud o la moral públicas.
>
> 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.
>
> Artículo 14: Derecho de Rectificación o Respuesta, toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentada y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.

En ningún caso la rectificación o la respuesta eximirá de las otras responsabilidades legales en que se hubiese incurrido.

Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial.

Adicionalmente, la Comisión Interamericana de Derechos Humanos ha desarrollado la Declaración de Principios sobre Libertad de Expresión. Se trata de un instrumento de gran relevancia ya que desarrolla algunos principios básicos en materia de libertad de expresión y privacidad:

Principio 1: La libertad de expresión, en todas sus formas y manifestaciones, es un derecho fundamental e inalienable, inherente a todas las personas. Es además, un requisito indispensable para la existencia misma de una sociedad democrática.

Principio 5: La 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.

La 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.

Principio 5, Declaración de Principios sobre la Libertad de Expresión

Principio 10: Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas.

1.3 Leyes, reglamentos, decretos y normativas nacionales

1.3.1 Nivel de aplicación, transparencia y control de leyes, reglamentos, decretos y normativas relacionados con el derecho a la privacidad (leyes de telecomunicaciones, leyes ciberseguridad, inteligencia de Estado (secreto de Estado), leyes antiterroristas, o reformas de ley con artículos que indican prácticas que protegen o vulneran la privacidad

Uno de los principales instrumentos en este ámbito es la Ley Marco del Sector de Telecomunicaciones. Esta ley - que fue aprobada en 1995 y actualizada en 1997 - reconoce que

> "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 pena" (Artículo 3)[3].

"Las telecomunicaciones son inviolables, por consiguiente, no podrán ser interceptadas o interferidas, salvo por resolución judicial. Cualquier información obtenida sin orden judicial, no podrán ser utilizadas en ninguna forma y originarán responsabilidad civil y penal"

Artículo 3. Ley Marco del Sector de Telecomunicaciones

El reglamento de dicha ley insiste en este aspecto, recordando que:

> "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, salvo en los siguientes casos:
>
> a) que exista consentimiento previo por escrito del usuario, en caso de comunicaciones maliciosas u otras situaciones en beneficio de éste,
>
> b) que exista una orden judicial expresa" (Artículo 8)[4].

Por otro lado, también la Ley de Transparencia y Acceso a la Información Pública incluye aspectos importantes relativos a la privacidad. El Capítulo V de esta ley se refiere a los datos personales y el *Hábeas Data*. Concretamente, el artículo 23 reconoce esta garantía. Asimismo, el artículo 24 establece que "el acceso a los datos personales únicamente procederá por decreto judicial

3 Ley Marco del Sector de Telecomunicaciones, 5 de diciembre de 1995, Decreto 185-95.
4 Reglamento General de la Ley Marco del Sector de Telecomunicaciones, 2002, Decreto 141-2002, http://www.conatel.gob.hn/doc/Regulacion/reglamentos/REGLAMENTO_GENERAL.pdf

o a petición de la persona cuyos datos personales se contienen en dicha información o de sus representantes o sucesores"[5].

Adicionalmente, Honduras posee una Ley Especial sobre la Intervención de las Comunicaciones Privadas[6]. En el Artículo 39 de la misma se establece la obligatoriedad de las empresas de telefonía a mantener por un plazo de cinco años un registro de todas las conexiones de cada usuario. Esto incluye información como los números de teléfono que participan en cada conversación, la duración y hora de las llamadas realizadas y las llamadas entrantes. Además, en el caso de llamadas con teléfono móvil, deberá guardarse el lugar donde se encuentra la persona usuaria cuando hace la llamada, contesta, o envía un mensaje de texto o de voz.

Por otro lado, esta misma ley establece en su artículo 42 que los operadores deben proveer, previa orden judicial, información como la almacenada en la agenda electrónica del aparato, mensajes de voz y de texto, tanto de la memoria interna como externa de los dispositivos. Asimismo, en este tipo de requerimientos se podrá solicitar, también a solicitud judicial, información como nombre y apellidos de quien compró el dispositivo, copia de los documentos de identificación, número IMEI, o información sobre antiguos propietarios, además de los aspectos ya señalados anteriormente.

Los operadores deben proveer, previa orden judicial, información como la almacenada en la agenda electrónica del aparato, mensajes de voz y de texto, tanto de la memoria interna como externa de los dispositivos

Se trata de una ley que violenta de forma clara el derecho a la privacidad, ya que obliga a los operadores a recabar y guardar información de sus clientes. Resulta preocupante también el hecho que no se especifican las medidas que deben emplear las empresas para resguardar esta información. Es importante señalar además, que esta información no estaría amparada por la Ley de Transparencia y Acceso a la Información Pública, ya que esta norma protege tan solo datos personales depositados en el sector público.

5 Ley de Transparencia y Acceso a la Información Pública, 30 de diciembre de 2006, https://portalunico.iaip.gob.hn/assets/docs/leyes/ley-de-transparencia-y-reglamento.pdf.
6 Ley Especial sobre Intervencion de las Comunicaciones Privadas, 12 de diciembre de 2011, Decreto 243-2011, http://www.poderjudicial.gob.hn/CEDIJ/Leyes/Documents/Ley%20Especial%20sobre%20Intervencion%20de%20las%20Comunicaciones%20Privadas%20(8,2mb).pdf.

1.4 Normativa de seguridad nacional y ciberseguridad

1.4.1 Existencia de legislación relacionada con seguridad nacional y ciberseguridad

En 2011, al amparo del artículo 287 de la Constitución, el Estado hondureño aprobó la Ley Especial del Consejo Nacional de Defensa y Seguridad. Esta ley tiene como objetivo la creación del Consejo Nacional de Defensa y Seguridad (CNDS)[7].

Los Artículos 6 y 7 de la ley disponen que el ente operativo de la CNDS es la Dirección Nacional de Investigación e Inteligencia (DNII). Esta instancia está integrada por las diferentes unidades especiales de investigación existentes y sus actuaciones deberán de estar enmarcadas "dentro de las disposiciones constitucionales legales y reglamentarias" (Artículo 7).

La DNII por su parte, fue creada en 2013 mediante la Ley de Inteligencia Nacional[8]. Tiene como objetivo desarrollar las actividades de investigación e inteligencia estratégica para proteger los derechos y libertades de los ciudadanos y residentes del país contra amenazas internas o externas (Artículo 2). Esta instancia goza de independencia funcional, administrativa y presupuestaria (Artículo 3).

"Los gastos realizados en la adquisición, contratación y ejecución de bienes, servicios, obras y recurso humano, que de hacerse en forma pública pondría en riesgo la seguridad nacional, la integridad del personal de inteligencia o sus fuentes de información tendrán la calidad de reservados".

Art. 8. Ley de Inteligencia Nacional

La DNII maneja el Sistema de Inteligencia Nacional (SIN), que también está integrado por la Dirección de Información Estratégica (C-2) de las Fuerzas Armadas de Honduras; la Dirección de inteligencia policial; la Secretaría de Estado en el Despacho de Relaciones Exteriores; y la Unidad de Información Financiera (UIF).

Aún cuando el Artículo 8 de la ley establece que todas las actuaciones de investigación e inteligencia realizadas por la DNII estarán sometidas al ordenamiento jurídico vigente, la misma norma propicia la opacidad en su actuar. En este sentido, la ley establece que "los gastos realizados en la adquisición, contratación y ejecución de bienes, servicios, obras y recurso humano, que de hacerse en forma pública pondría en riesgo la seguridad nacional, la integridad del personal de inteligencia o sus fuentes de información tendrán la calidad de reservados". (Artículo 16). Asimismo, señala que "los comprobantes contables de los gastos reservados

7 Ley Especial del Consejo Nacional de Defensa y Seguridad, 12 de diciembre de 2011, Decreto 249-2011.
8 Ley de Inteligencia Nacional, 15 de abril de 2013, Decreto 211-2021.

permanecerán depositados y bajo custodio de la DNII durante un plazo de 10 años para efectos de fiscalización a posteriori" (Artículo 17).

Además, la DNII el artículo 6 establece que

> "Será de obligación de las instituciones públicas brindar la información que 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" (Artículo 6).

Por otro lado, lo dispuesto por la Ley de Transparencia parece carecer de valor en el caso de la DNII. Así, el artículo 18 establece 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". En consecuencia, "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" (Artículo 19).

Finalmente, es importante señalar que la Ley de Inteligencia Nacional también crea el Centro Nacional de Información, como dependencia en la que se "integrarán las diferentes bases de datos de las entidades públicas que administran información de interés para la seguridad y la defensa nacional; para tal fin, el Centro Nacional de Información adquirirá la plataforma tecnológica que permita la interconexión con las entidades públicas, quienes facilitarán este proceso" (Artículo 29).

2. Dimensión Política

2.1 Relación entre Estado, empresas y cámaras de telecomunicaciones

2.1.1 Nivel de Relación Estado empresas y cámaras de telecomunicaciones

El mercado de las telecomunicaciones hondureño está en manos de unas pocas empresas. En el caso de la telefonía móvil el negocio se reparte entre 3 operadores: Tigo (Telefonía Celular S. A., CELTEL), Claro (SERCOM) y Hondutel (Empresa Hondureña de Telecomunicaciones). Son las dos primeras las que acaparan la mayor parte del mercado. Así, en 2018 Claro contaba con el 62% de las líneas y Tigo con el 37%. La participación de la empresa pública Hondutel es marginal, ya que contaba con menos del 1% de las líneas[9].

En 2018 Claro contaba con el 62% de las líneas y Tigo con el 37%. La participación de la empresa pública Hondutel es marginal, ya que contaba con menos del 1% de las líneas

En el caso de la telefonía fija es Hondutel la empresa que controla la mayor parte del servicio. En 2018 recibió el 75,1% de los ingresos generados por la telefonía fija, mientras que CELTEL y SERCOM recibieron el 7,9% y el 7,4% respectivamente. Además, otras 5 empresas minoritarias recibieron el 9,7% de los ingresos generados en este ámbito del mercado. En cualquier caso, es importante señalar que la telefonía fija ha conocido en los últimos años una notable reducción[10].

Por otro lado, en cuanto a la provisión de servicios de Internet de banda fija, los principales proveedores son Navega y Cablecolor. La primera cuenta con el 35,46% de las actividades en este ámbito mientras que la segunda asume el 29,38%. El resto de la actividad se distribuye entre varias empresas, sin embargo, ninguna de ellas cuenta con más del 8% del mercado[11].

2.1.2 Nivel de representación en cuanto a la relación entre el Estado, las empresas y las cámaras de telecomunicaciones

La instancia a cargo del sector es el Consejo Nacional de Telecomunicaciones (CONALTEL). Esta entidad fue creada por la ya mencionada Ley Marco del Sector de Telecomunicaciones.

9 Estudio sectorial sobre el mercado de telecomunicaciones en Honduras, Comisión para la Defensa y la Promoción de la Competencia, 2018, https://www.cdpc.hn/sites/default/files/Privado/estudios_mercado/Estudio%20Sectorial%20de%20Telecomunicaciones%20en%20Honduras%20%28Telefon%C3%ADa%20Móvil%2C%20Fija%20e%20Internet%29.pdf
10 Ibíd.
11 Ibíd.

Tiene potestades de asesoramiento, representación, regulación, supervisión, promoción, administración y sanción[12].

A diferencia de instancias homólogas en otros países de la región, entre los comisionados de la CONATEL no hay ningún puesto reservado para la representación empresarial. De hecho, todos los comisionados titulares y suplentes son nombrados de forma directa por el presidente[13].

A diferencia de instancias homólogas en otros países de la región, entre los comisionados de la CONATEL no hay ningún puesto reservado para la representación empresarial. De hecho, todos los comisionados titulares y suplentes son nombrados de forma directa por el presidente

No se han identificado fuentes que den cuenta de manera expresa de la relación entre el sector empresarial de las telecomunicaciones y el Estado. En este sentido, las personas entrevistadas señalaron que se trata de una relación eminentemente comercial. Sin embargo, información brindada por canales oficiales del Gobierno apuntaría a que al menos Tigo, representado por su presidente, estaría brindando apoyo a la administración del actual presidente Juan Orlando Hernández. En este sentido, en 2016 el ejecutivo lanzó el Plan Honduras 20/20. Se trata de una alianza público-privada que tiene el objetivo de generar empleo[14]. El empresario y presidente de Tigo, Antonio Tavel, ha participado activamente en esta iniciativa y se ha manifestado a favor del Gobierno[15].

2.2 Contratos entre el Estado y las empresas de seguridad privada

2.2.1 Nivel de impacto de los contratos establecidos entre el Estado y empresas de seguridad privada

Al igual que en otros países de la región, el negocio de la seguridad privada se ha ampliado de forma significativa en los últimos años en Honduras. Fuentes periodísticas señalan que el aumento de las actividades delictivas y el crimen organizado ha creado un contexto propicio

12 «Sobre nosotros», CONATEL, acceso el 10 de enero de 2020, http://www.conatel.gob.hn/index.php/sobre-nosotros/
13 Ley Marco del Sector de Telecomunicaciones, 25 de octubre de 1997, Decreto 185-95, https://www.tsc.gob.hn/web/leyes/LEY%20MARCO%20DEL%20SECTOR%20DE%20TELECOMUNICACIONES.pdf.
14 «Presidente Hernández presenta Programa Nacional de Desarrollo Económico Honduras 20/20», Presidencia, 1 de marzo de 2016, acceso el 15 de diciembre de 2019, https://www.presidencia.gob.hn/index.php/gob/casa-presidencial/honduras-20-20/532-presidente-hernandez-presenta-programa-nacional-de-desarrollo-economico-honduras-20-20
15 Ibíd y «En Honduras no hay crisis económica: Antonio Tavel Otero», *Criterio.hn*, 22 de abril de 2019, acceso 10 de diciembre de 2019, https://criterio.hn/2019/04/22/en-honduras-no-hay-crisis-economica-antonio-tavel-otero/

para la proliferación de este tipo empresas. Así, en una década el número de compañías de seguridad privada aumentó en un 800%, pasando de 116 compañías en el año 2007 a 1.038 en 2018[16]. Se estima además que la planilla de agentes de seguridad privada podría duplicar en número a los agentes de seguridad del Estado. Honduras cuenta con 15.000 oficiales de policía y 25.000 militares, mientras que se estima que los agentes de seguridad privada son entre 70.000 y 100.000[17].

En una década el número de compañías de seguridad privada aumentó en un 800%, pasando de 116 compañías en el año 2007 a 1.038 en 2018

Algunas de las personas entrevistadas señalan que el Estado ha alentado el crecimiento desmedido de este tipo de empresas. En este sentido, uno de los principales proyectos para la seguridad a nivel municipal – Barrios más Seguros – ha promovido el cierre de colonias y la contratación de servicios de seguridad privada[18]. Según cifras provistas por la Gerencia de Movilidad Urbana a la prensa, 188 comunidades de Tegucigalpa participaban en esta iniciativa en 2017.

Bertha Oliva, coordinadora del Comité de Familiares de Desaparecidos de Honduras (COFADEH), señala que esta situación ha propiciado que las empresas tengan una gran cantidad de información privada de las ciudadanas y los ciudadanos, que podría estar siendo utilizada – o ser utilizada en el futuro – para desarrollar acciones de vigilancia. Se trata de un riesgo importante ya que no existen mecanismos para evitar este tipo de abusos[19].

Es de destacar, que las empresas de seguridad privada están reguladas por la Ley Orgánica de la Policía Nacional (Decreto N° 67/2008)[20], y el Reglamento para el Control de los Servicios de Seguridad Privada (Acuerdo N° 013/2009)[21].

Según la Ley de 2008, la entidad responsable de la administración, control y vigilancia del sector

16 Luis Hernández, «En Honduras las empresas de seguridad privada son un buen negocio», *Once Noticias*, 5 de noviembre de 2018, https://www.oncenoticias.hn/en-honduras-las-empresas-de-seguridad-privada-son-un-buen-negocio/.
17 Ibíd.
18 «Barrios Seguros», *El Heraldo,* acceso el 9 de diciembrede 2019, https://www.elheraldo.hn/opinion/720871-368/barrios-seguros
19 Bertha Oliva, Entrevista realizada en diciembre de 2018.
20 Ley Orgánica de la Policía Nacional De Honduras, 31 de octubre de 2008, Decreto 67-2008, https://www.acnur.org/fileadmin/Documentos/BDL/2016/10610.pdf.
21 Reglamento para el control de los servicios privados de seguridad, 11 de enero de 2010, Acuerdo 013-2009, https://www.tsc.gob.hn/web/leyes/Reglamento%20para%20el%20control%20de%20los%20servicios%20privados%20de%20seguridad.pdf.

privado es la Unidad de Control de los Servicios de Seguridad Privada (UCSSP). Esta unidad operaría, según dicha ley, bajo la Dirección Nacional de Servicios Especiales Preventivos. Sin embargo, el reglamento aprobado un año más tarde estableció que la UCSSP estaría vinculada directamente a la Secretaría de Estado, mediante la Dirección Nacional de Seguridad Privada. Este cambio dejó a la UCSSP en manos más políticas que técnicas. Un informe presentado en 2018 por el centro de análisis Diálogo Interamericano reporta que en Honduras hay varios cientos de empresas que operan sin licencia. Esto permite a dichas compañías evadir la obligación de reportar los antecedentes penales de sus empleados[22].

No se ha logrado identificar cuánto es el presupuesto total que el Estado hondureño dedica a la contratación de servicios de las empresas de seguridad privada. Sin embargo, la información disponible evidencia que las licitaciones públicas son una importante fuente de ingresos para estas empresas.

2.3 Relación de actores estatales o políticos con las directivas de empresas de seguridad

2.3.1 Nivel de relación del Estado con empresas de seguridad privada

Investigaciones periodísticas han revelado los estrechos vínculos entre algunas empresas y altos cargo del Gobierno.

Según reportes de prensa, la seguridad privada en Honduras, al igual como sucede en El Salvador y Guatemala, está en manos de exmilitares[23]. Además, investigaciones periodísticas han revelado los estrechos vínculos entre algunas empresas y altos cargos del Gobierno. El caso más difundido en medios ha sido la relación entre el presidente Juan Orlando Hernández con dos empresas de seguridad privada. En este sentido, una investigación publicada en mayo de 2019 señala que Hernández tiene vinculación con las empresas Servicios de Seguridad Lempira (SERSEL) y Servicios de Seguridad y Asociados, Sociedad Anónima (SSA)[24].

22 Sarah Kinosian y James Bosworth, «Security for Sale», The Dialogue, 2018, https://www.thedialogue.org/wp-content/uploads/2018/03/Security-for-Sale-FINAL-ENGLISH.pdf
23 «700 compañías de seguridad privada existen en Honduras», *Diario El Heraldo*, 7 de abril de 2014, https://www.elheraldo.hn/pais/581306-214/700-companias-de-seguridad-privada-existen-en-honduras.
24 «Sersel: la seguridad favorita del Gobierno», Expediente Público, 2019, 10 de septiembre de 2019,https://expedientepublico.org/sersel-la-seguridad-favorita-del-gobierno/

Según esta misma fuente, Hernández fue uno de los constituyentes de SERSEL cuando la empresa fue creada en 1991. Asimismo, la misma fuente ha revelado que el actual presidente aparece como constituyente de la empresa SSA en 2004[25].

Desde 2006 hasta la fecha a SERSEL se le han otorgado 38 contratos estatales, por un monto de 12.6 millones de dólares. Es importante señalar además que Wilfredo Calderón, subdirector de Migración, también es socio de esta empresa.

Según medios de prensa, la empresa se habría beneficiado de contrataciones realizadas por mecanismos excepcionales, al margen de la Ley de Contrataciones del Estado. Concretamente, le fue otorgado un contrato por 8 millones de dólares para brindar servicios de 149 guardias de seguridad entre 2017 y 2019 al Instituto Hondurenos de Seguridad Social (IHSS). Como ya se ha señalado para otorgar esta licitación no se siguieron los procedimientos establecidos por ley, ya que - argumentando que se trataba de una situación de emergencia - se realizó una licitación privada en la que se invitó directamente a determinadas empresas[26].

2.4 Planes de Gobierno en vigencia en materia de seguridad nacional

2.4.1 Planes de gobierno vigentes relacionados con la seguridad nacional y ciberseguridad que protegen o vulneran la privacidad

El Ejecutivo hondureño incluye objetivos y acciones relativas a la seguridad nacional en varios de su planes y políticas. En este sentido, uno de los más generales es el Plan Estratégico de Gobierno 2018-2022[27]. Este plan establece entre sus objetivos específicos "Garantizar mayores niveles de seguridad, para la convivencia sana y pacífica de la población hondureña, y el desarrollo pleno de la actividad productiva".

25 Ibíd.
26 Ibíd.
27 «Plan Estratégico de Gobierno 2018-2022», Secretariade Coordinación General del Gobierno, 2018, http://www.scgg.gob.hn/es/node/108.

Además, cuenta con la Política Integral de Convivencia y Seguridad Ciudadana para Honduras 2011 – 2022[28]. Esta política define las siguientes seis líneas estratégicas de acción: la creación del Sistema Nacional de Seguridad Ciudadana, la creación de un Consejo Nacional de Seguridad Ciudadana, reingeniería policial, el fortalecimiento institucional de la Secretaría de Seguridad, la reingeniería policial, el papel de los gobiernos locales en la seguridad, y participación de la ciudadanía y del sector privado en materia de convivencia y seguridad ciudadana.

El plan también prevé el desarrollo de diferentes programas y proyectos entre los que destaca el Sistema de Información de Violencia y Delincuencia. Las acciones previstas en este marco apuntan a: administrar e implementar un sistema de información estadística útil para la Secretaría de Seguridad, la Dirección General de la Policía Nacional y sus Direcciones Policiales; sistematizar de manera centralizada la información y documentación sobre la actividad delictiva del país; planificar, coordinar, ejecutar y evaluar la generación de informes estadísticos periódicos; mantener estrecha relación de colaboración con las oficinas de planeamiento de las Direcciones, Metropolitanas y Jefaturas Departamentales; procesar la información depurándola hasta transformarla en reportes ejecutivos; y mantener canales de comunicación y colaboración con el Observatorio de la Violencia e instancias internacionales que manejan información de interés policial[29].

El resguardo de la privacidad no es una prioridad en los planes de gobierno vigentes. Por otro lado, la información disponible con respecto a los planes no permite identificar si dichos planes podrían vulnerar el derecho a la privacidad.

En el ámbito de la ciberseguridad, el país carece de una política nacional de o algún otro instrumento similar.

2.5 Relación de los planes de seguridad nacional y ciberseguridad con la privacidad

2.5.1 Nivel de protección o vulneración de la privacidad de los planes de gobierno vigentes relacionados con la seguridad nacional y ciberseguridad

El análisis incluido en el punto anterior evidencia que el resguardo de la privacidad no es una prioridad en los planes de gobierno vigentes. Por otro lado, la información disponible con

28 «Política integral de convivencia y seguridad ciudadana para Honduras 2011-2022», 2011, http://www.hn.undp.org/content/dam/honduras/docs/publicaciones/Politica_Integral_Convivencia_Seguridad_2011_2022.pdf.
29 Ibíd.

respecto a los planes no permite identificar si dichos planes podrían vulnerar el derecho a la privacidad.

2.6 Uso de tecnológicas de vigilancia como evidencia o caso para criminalizar o judicializar

2.6.1 Casos en los que se usan evidencias de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos que ejercen sus derechos humanos y civiles

Un estudio de las interacciones en twitter realizado por la investigadora Erin Gallagher reveló que desde cuentas falsas se realizó una campaña de desprestigio contra la defensora hondureña Berta Cáceres, tres meses antes de su asesinato

La mayoría de los ataques reportados por las personas entrevistadas fueron de acoso y deslegitimación en redes sociales. Si bien no se puede demostrar el origen de estos intentos de deslegitimación algunos estudios han aportado información relevante sobre este tipo de dinámicas. En este sentido, un estudio de las interacciones en twitter realizado por la investigadora Erin Gallagher reveló que desde cuentas falsas se realizó una campaña de desprestigio contra la defensora hondureña Berta Cáceres, tres meses antes de su asesinato. Dicho estudio identificó varias decenas de cuentas falsas, creadas prácticamente de manera simultánea cuya única actividad estaba vinculada a criminalizar y desprestigiar al COPINH y a la defensora hondureña Berta Cáceres[30].

2.6.2 Identificación de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos que ejercen sus derechos humanos y civiles

Con respecto al uso de tecnologías de vigilancia para criminalizar, deslegitimar o amenazar a personas y colectivos que ejercen sus derechos humanos y civiles, en algunos casos se han denunciado este tipo de prácticas, pero solo un caso fue denunciado públicamente por un ex-diputado y miembro de la Alianza de Oposición a la dictadura. Concretamente, denunció que una conversación privada con una persona de confianza sobre la situación en Venezuela había sido grabada[31] sin su consentimiento y distribuida en redes sociales[32].

30 Erin Gallagher, «Fake Twitter Hondureño: La campaña digital contra Berta Cáceres y COPINH, 2017», https://medium.com/@erin_gallagher/fake-twitter-hondure%C3%B1o-la-campa%C3%B1a-digital-contra-berta-c%C3%A1ceres-y-copinh-3911ad7db456
31 «Rafael Alegría dice que fue lenguaje coloquial», *Diario La Tribuna Honduras*, 1 de agosto de 2017, http://www.latribuna.hn/2017/08/01/rafael-alegria-dice-fue-lenguaje-coloquial/.
32 Nos queda claro, *Así se expresa miembro de la Alianza, Rafael Alegría sobre la constituyente en Venezuela*, 2017, https://www.youtube.com/watch?v=mRl6hjydbLg.

Antes de ello, en 2015, miembros de la Junta Nominadora del Poder Judicial 2016-2020, denunciaron que eran vigilados mediante grabaciones telefónicas y monitoreo por medio de cámaras ocultas[33].

2.7 Acuerdos bilaterales y multilaterales de cooperación en materia de seguridad

2.7.1 Existencia de acuerdos bilaterales y multilaterales de cooperación en materia de seguridad

Honduras cuenta con diferentes acuerdos bilaterales o multilaterales en materia de seguridad. Uno de los más recientes es el Acuerdo marco de cooperación entre el gobierno de la República de Honduras y el gobierno del Estado de Israel, adoptado en 2016[34].

Dicho acuerdo tiene como objetivo "asegurar que las Fuerzas Armadas de Honduras dispongan de los recursos necesarios para cumplir su función constitucional de proteger la soberanía nacional"[35]. Para ello, el acuerdo prevé la ejecución de varios proyectos. En este sentido, el acuerdo incluye aspectos como "repotenciar los aviones F5 y A37, así como la flota de helicópteros que posee actualmente la Fuerza Aérea Hondureña"[36]. En cuanto a la defensa marítima, el acuerdo incluye la construcción de una embarcación con capacidad de para aterrizaje y despegue de helicópteros.

Por otro lado, el convenio incluye acciones como la creación de un nuevo sistema de comunicación con cobertura nacional, impulsar la mejora del sistema de comando y control,

33 «Honduras: Junta Nominadora denuncia escuchas telefónicas ilegales», *El Libertador,* acceso el 14 de marzo de 2019, http://www.web.ellibertador.hn/index.php/justicia/922-honduras-junta-nominadora-denuncia-escuchas-telefonicas-ilegales.
34 «Seguridad y Defensa Israel y Honduras suscriben acuerdo para potenciar las Fuerzas Armadas», Consejo de Secretarios de Estado, acceso 20 de septiembre de 2018, http://www.consejosecretariosdeestado.gob.hn/content/seguridad-y-defensa-israel-y-honduras-suscriben-acuerdo-para-potenciar-las-fuerzas-armadas; «Honduras suscribe acuerdo con Israel: Estos son los proyectos a desarrollar en las Fuerzas Armadas», *Diario El Heraldo*, 8 de diciembre de 2016, https://www.elheraldo.hn/pais/1024750-466/honduras-suscribe-acuerdo-con-israel-estos-son-los-proyectos-a-desarrollar-en; y «Acuerdo marco de cooperación entre el gobierno de la República de Honduras y el gobierno del Estado de Israel», 6 de diciembre de 2016.
35 «Seguridad y Defensa Israel y Honduras suscriben acuerdo para potenciar las Fuerzas Armadas», Consejo de Secretarios de Estado, acceso 20 de septiembre de 2018, http://www.consejosecretariosdeestado.gob.hn/content/seguridad-y-defensa-israel-y-honduras-suscriben-acuerdo-para-potenciar-las-fuerzas-armadas
36 Ibíd.

implementar 3 sistemas de vigilancia y reconocimiento no tripulada mediante 6 drones, fortalecer el sistema informático del Estado[37] y crear el Centro de Respuesta a Emergencias Informáticas (CERT)[38].

Otro de los tratados relevantes adoptados en los últimos años es la Alianza para la Prosperidad del Triángulo Norte. Se trata de una iniciativa tripartita en la que participan los gobiernos de Guatemala, Honduras y El Salvador, en colaboración con el Banco Interamericano de Desarrollo (BID). Esta Alianza surgió como una estrategia para frenar la migración irregular hacia Estados Unidos. Entre las medidas planteadas en el marco de esta iniciativa destacan algunas relativas al campo de la seguridad[39].

Otro de los tratados relevantes adoptados en los últimos años es la Alianza para la Prosperidad del Triángulo Norte. Se trata de una iniciativa tripartita en la que participan los gobiernos de Guatemala, Honduras y El Salvador, en colaboración con el Banco Interamericano de Desarrollo (BID).

En el marco de esta Alianza, Honduras ha recibido 27,4 millones de dólares por concepto de fondos no reembolsables y 826,8 millones de dólares por concepto de préstamos. En el ámbito de la seguridad, el país ha invertido parte de estos fondos en desarrollar un programa de convivencia ciudadana y mejoramiento de barrios que ha tenido 720,000 beneficiarios; en capacitar a 7,000 agentes de policía; en graduar 800 nuevos policías; y crear consejos de seguridad en 3 municipalidades[40].

3 Dimensión Económica

3.1 Presupuestos nacionales destinados a seguridad y gastos reservados

3.1.1 Total de presupuesto en líneas de los presupuesto nacionales destinados a gastos reservados

Aunque no sean nombrados explícitamente de esta forma, son varios los textos normativos que permiten el uso de fondos reservados en Honduras. Así, la ley de la Dirección Nacional de

37 Ibíd.
38 «Acuerdo marco de cooperación entre el gobierno de la República de Honduras y el gobierno del Estado de Israel», 6 de diciembre de 2016.
39 «Plan de la Alianza para la Prosperidad del Triángulo Norte - Hondurasl», Banco Interamericano de Desarrollo, acceso el 16 de octubrede 2019, https://www.iadb.org/es/alianza-para-la-prosperidad/honduras
40 Ibíd.

Investigación e información (DNII) establece que esta instancia está "obligada a rendir cuentas de sus operaciones; sin embargo, las actuaciones financiadas con fondos reservados serán respaldadas y sustituidas por un certificado de cumplimento de la normativa jurídica en materia de fiscalización vigente, que se remitirá al Tribunal Superior de Cuentas (TSC)." (Artículo 17).

Por otro lado, la aprobación en 2014 de la Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional favoreció la posibilidad de manejar presupuestos públicos de forma opaca.

Por otro lado, la aprobación en 2014 de la Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional favoreció la posibilidad de manejar presupuestos públicos de forma opaca. Esta norma introdujo un nuevo sistema para la reserva de documentos, creando cuatro categorías: reservado, confidencial, secreto y ultra secreto. Asimismo, amplía los plazos de desclasificación. Anteriormente, se contemplaba que la reserva podía tener una duración de hasta 10 años. Sin embargo, la Ley de Clasificación otorga un plazo de reserva de 15 años a los documentos calificados como secretos, y de 25 años para los ultra secretos, prorrogables en ambos casos[41].

Al amparo de esta ley, también en 2014, el Consejo de Seguridad aprobó una resolución clasificando como reservada la

> "Información proveniente de al menos 16 instituciones, entre las cuales se cuentan la Dirección Ejecutiva de Ingresos (ahora Servicio de Administración de Rentas), el Registro Nacional de las Personas, el Instituto Hondureño de Seguridad Social, el Instituto de la Propiedad, la Dirección de la Marina Mercante, la Dirección de Aeronáutica Civil, la Empresa Nacional de Energía Eléctrica y el Servicio Autónomo Nacional de Acueductos y Alcantarillados, las que guardan poca relación directa y evidente con la seguridad nacional"[42].

Es importante señalar además, que la resolución – también clasificada como secreta – no es clara a la hora de establecer si el carácter reservado es aplicable a toda la información generada por dichas instituciones o si se limita a "aquella cuya revelación pudiese ocasionar daños a la seguridad y defensa"[43].

41 «Derecho de Acceso a la información e intereses legítimos de defensa y seguridad en Honduras: La búsqueda del balance en un estado democrático y constitucional de derecho», MACCIH - OEA, julio de 2017, https://www.oas.org/en/spa/dsdsm/maccih/new/docs/20170705_MACCIH_5.pdf
42 Ibíd.
43 Ibíd.

En este escenario, fuentes de prensa reportan que tanto organizaciones de la sociedad civil como sectores de la oposición han denunciado que el Ejecutivo está empleando esta ley para ocultar cómo está gastando el presupuesto y qué procedimientos se está empleando para la realización de licitaciones, compras y contrataciones del Estado[44].

3.1.2 Total del presupuesto nacional destinado a seguridad

A la hora de analizar el comportamiento del presupuesto destinado en Honduras a la seguridad, es necesario realizar algunas consideraciones sobre el comportamiento presupuestario en general. En este sentido, un informe realizado en 2019 por el Fondo Social de Deuda Externa y Desarrollo de Honduras (FOSDEH) señala importantes debilidades, derivadas principalmente de las diferencias entre el presupuesto aprobado, el vigente y el ejecutado. Esto es signo, según dicho informe, tanto de debilidades en la planificación como de indisciplina presupuestaria[45].

En el caso concreto del presupuesto destinado a seguridad, FOSDEH señala que el conflicto existente entre Secretarías de Seguridad (SESSEGU) y Defensa (SEDENA) ha implicado una mayor erogación de recursos destinados a esta última área, sin que esto se haya traducido en una mejora en la percepción ciudadana con respecto a la inseguridad[46]. En importante señalar además, que entre 2002 y 2013 la SESSEGU contaba con un mayor presupuesto. Sin embargo, a partir de 2014 hubo un cambio en esta tendencia, de manera que en el último cuatrienio ha sido la SEDENA la que ha contado con más fondos[47].

FOSDEH señala que el conflicto existente entre Secretarías de Seguridad (SESSEGU) y Defensa (SEDENA) ha implicado una mayor erogación de recursos destinados a esta última área, sin que esto se haya traducido en una mejora en la percepción ciudadana con respecto a la inseguridad

Según FOSDEH este aumento a la SEDENA se relaciona, entre otros factores, por gastos extraordinarios realizados por esta entidad en los últimos años.

> "Es oportuno señalar que durante este periodo, además de dársele a las fuerzas armadas la potestad de realizar funciones en el marco de seguridad pública, también el conflicto

44 «Ley de Secretos es un escudo para los corruptos», Criterio.hn, 10 de Julio de 2017, https://criterio.hn/2017/07/10/ley-secretos-escudo-los-corruptos/
45 «¿Cuál es el costa de la seguridad y la defensa en Honduras?», FOSDEH, 2019, http://www.fosdeh.com/2019/01/cual-es-el-costo-de-la-seguridad-y-la-defensa-en-honduras/#prettyPhoto
46 Ibíd.
47 Ibíd.

político y social posterior a la celebración de Elecciones Generales en noviembre de 2017, provocó costos financieros no presupuestados a esta institución"[48].

Según muestra la tabla 1 para 2018 el presupuesto total destinado a seguridad fue de más de 14,000 millones de lempiras[49]. Este presupuesto ha tenido en los últimos cuatro años un aumento importante, ya que en 2014 era de 8,500 millones.

La mayor parte del presupuesto se destina al pago de salarios del personal en ambas secretarías. Esto incluye salarios de policías a cargo de la SESSEGU, de militares de la SEDENA y de personal civil de ambas instituciones. La priorización del área de defensa también se evidencia si se considera la planilla de cada una de las secretarías. Así, Seguridad cuenta con 15,820 personas empleadas, mientras que defensa tiene 25,615 personas contratadas.

La mayor parte del presupuesto se destina al pago de salarios del personal en ambas secretarías. Esto incluye salarios de policías a cargo de la SESSEGU, de militares de la SEDENA y de personal civil de ambas instituciones.

Tabla 1. Presupuesto nacional aprobado a las secretarías de Seguridad y de Defensa (2014-2018)

	Secretaría de Seguridad	Secretaría de Defensa	Total
2014	3,959,488,288.00	4,551,901,320.00	8,511,389,608.00
2015	3,867,197,685.00	5,418,822,357.00	9,286,020,042.00
2016	5,952,735,239.00	6,712,434,642.00	12,665,169,881.00
2017	6,276,603,158.00	6,997,720,092.00	13,274,323,250.00
2018	6,583,476,835.00	7,958,582,485.00	14,542,059,320.00

Fuente: Elaboración propia a partir de presupuestos nacionales.

Por otro lado, también es importante señalar que en 2014 fue creado mediante un decreto ejecutivo el Gabinete de Seguridad y Defensa, añadiendo una nueva instancia a la estructura institucional nacional de seguridad. La finalidad del Gabinete es coordinar las funciones de

48 «Seguimiento y Evaluación del Gasto Público en Seguridad y Defensa 2002 - 2018», Foro Social de la Deuda Externa y Desarrollo de Honduras, julio de 2018, http://che.hn/wp-content/uploads/2018/08/Seguimiento-y-Evaluacion-Gasto-Publico-en-Seguridad-y-Defensa-2002-2018.pdf

49 Aproximadamente 593 millones de dólares.

instituciones como la Secretaría de Seguridad, la Secretaría de Defensa o el Instituto Nacional de Migración, entre otras. A pesar que desde su creación cuenta con presupuesto asignado, su ejecución ha sido muy irregular. Por ejemplo, entre 2014 y 2017 la ejecución presupuestaria fue de 0%. Sin embargo, aunque el presupuesto no se haya utilizado, la mayoría de los años la asignación ha sido aumentada. A este respecto FODEH plantea que

> "Esta conducta presupuestaria da indicios de bajos niveles de operatividad técnica y por ende una débil coordinación y articulación de metas y resultados de las instituciones adscritas al mismo, asimismo refleja la ausencia de planificación entre presupuesto y actividades programáticas"[50].

Otro de los aspectos a tomar en consideración en el caso de Honduras es que la Ley de Seguridad Poblacional de 2011, creó un Fondo de Protección y Seguridad Poblacional y un fideicomiso para su manejo. Este fondo se financia a partir de impuestos especiales, "con montos superiores a los 120 mil lempiras; del 1% de los ingresos brutos mensuales de la telefonía móvil; del 2% de las actividades de exportación minera; del 0.5% sobre ingresos brutos de las comidas rápidas; del 1% sobre ingresos totales de los casinos y máquinas tragamonedas y del 3.6 % sobre los excedentes netos anuales del sector cooperativo"[51].

Esta tasa se creó inicialmente para un periodo de 5 años, pero en 2018 pasó a ser de carácter permanente mediante un Decreto Legislativo (N. 31-2018). Desde su creación los fondos recaudados se han dirigido principalmente a la SESSEGU y la SEDENA, en menor medida a proyectos de prevención[52].

Según concluye la investigación realizada por FODEH la transparencia y la rendición de cuentas por parte del Fideicomiso ha sido deficiente. De hecho, esta misma fuente reporta que en 2015 parte de los fondos se destinaron a cubrir deudas de la Empresa Nacional de Energía Eléctrica.

50 «¿Cuál es el costa de la seguridad y la defensa en Honduras?», FOSDEH, 2019, http://www.fosdeh.com/2019/01/cual-es-el-costo-de-la-seguridad-y-la-defensa-en-honduras/#prettyPhoto
51 «Tasa de seguridad en Honduras», ASJ, 2017, http://asjhonduras.com/webhn/tag/tasa-de-seguridad-honduras/
52 «¿Cuál es el costa de la seguridad y la defensa en Honduras?», FOSDEH, 2019, http://www.fosdeh.com/2019/01/cual-es-el-costo-de-la-seguridad-y-la-defensa-en-honduras/#prettyPhoto

Esta información, conforme a dicho informe, se mantuvo oculta al amparo de la Ley para la Clasificación de Documentos Públicos relacionados con la Seguridad y Defensa Nacional[53].

3.1.3 Instituciones Estatales que tienen líneas de presupuesto destinadas a seguridad y gastos reservados

Como ya se ha señalado, al amparo de la Ley para la Clasificación de Documentos Públicos Relacionados con la Seguridad y Defensa Nacional, el presupuesto de al menos 16 instituciones es considerado secreto. Se trata de una situación excepcional en la región, ya que son amplias las líneas presupuestarias que manejan con opacidad.

3.1.4 Montos de contratos relacionados con compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

Aunque es posible encontrar algunos contratos de compras de equipo en materia de seguridad, la información que ofrece el portal de compras públicas (Honducompras), es limitada e insuficiente para conocer montos exactos de la inversión o detalle de los equipos adquiridos. Una vez más, esto es consecuencia de la opacidad que permite la normativa hondureña con respecto a las compras y los presupuestos. Habida cuenta de esta situación, las compras de este tipo que se han podido identificar son escasas.

A mediados de 2016, con dinero de un préstamo al Banco Interamericano de Desarrollo (Programa BID-Préstamo 2745/BL/HO), la "adquisición de Equipo para Laboratorios de Policía Científica y Criminalista de la Dirección Policial de Investigaciones –DPI", pero es imposible saber qué empresas obtuvieron el contrato, qué equipamiento compraron, toda vez que el concurso no detalla claramente el equipo sin que se limita a describirlos como Equipo informático, equipo audiovisual y hasta equipos misceláneos[54] o el concurso para la "Adquisición de equipo y software para laboratorios de informática forense de la DPI", del mismo préstamo, cuya descripción del

53 Ibíd.

54 «Expediente SS-PICSC-LPI-007-2016», Honducompras, 6 de mayo de 2016, http://sicc.honducompras.gob.hn/HC/Procesos/ProcesoHistorico.aspx?Id0=NwAAADEAAAA3AAAA-Fq0Qhrwnpd0%3D&Id1=MQAAAA%3D%3D-OFoziWLXW%2Fg%3D&Id2=UwAAAFMAAAAtAAAAUAAAAEkAAABDAAAAUwAAAEMAAAAtAAAATAAAAFAAAABJAAAALQAAADAAAAAwAAAANwAAAC0AAAAyAAAAMAAAADEAAAA2AAAA-ZchExUJxgK0%3D.

equipo es un "Software de sistema experto", que incluía Estación de Trabajo Forense, un servidor de datos y un software de análisis forense[55].

De la autopromoción que hace el Consejo Técnico del Fidecomiso de la Tasa de Seguridad se puede conocer algunas inversiones en líneas gruesas. Según su página web, se gastaron 62.89 millones de lempiras en la creación y fortalecimiento de la Agencia Técnica de Investigación Criminal entre 2014 y 2015[56]; 33.57 millones de lempiras en construcción y reconstrucción de capacidades de la unidad de medicina forense del Ministerio público[57]; y 264.71 millones de lempiras Radares para la Fuerza Aérea Hondureña (FAH) para el combate al narcotráfico[58].

3.1.5 Instituciones encargadas de los contratos relacionados con compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

Debido a las limitaciones ya señaladas, tampoco se ha logrado información detallada con respecto a este punto. Sin embargo, puede inferirse que cualquier institución cuenta con las posibilidades económicas de comprar este tipo de bienes y servicios.

3.2 Empresas proveedoras de bienes y servicios en materia de tecnologías de vigilancia

3.2.1 Empresas que tienen los contratos relacionados de compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

Como ya se ha señalado, las limitaciones para acceder a los contratos que realiza el Estado son numerosas, debido a la normativa que califica con secreto de Estado buena parte de los

55 «Expediente SS-PICSC-LPI-015-2018», Honducompras, 1 de junio de 2018, http://sicc.honducompras.gob.hn/HC/Procesos/ProcesoHistorico.aspx?Id0=NwAAADEAAAA3AAAA-Fq0Qhrwnpd0%3D&Id1=MQAAAA%3D%3D-OFoziWLXW%2Fg%3D&Id2=UwAAAFMAAAAtAAAAUAAAAEkAAABDAAAAUwAAAEMAAAAtAAAATAAAAFAAAABJAAAALQAAADAAAAAxAAAANQAAAC0AAAAyAAAAMAAAADEAAAA4AAAA-DDGicaqHWvs%3D.

56 «Fortalecimiento de Capacidad Institucional de la ATIC», Tasa de Seguridad Poblacional - Honduras, 20 de enero de 2014, https://www.tasadeseguridad.hn/proyecto.php?p=5.

57 «Adquisición de Equipo para Medicina Forense», Tasa de Seguridad Poblacional - Honduras, 1 de junio de 2017, https://www.tasadeseguridad.hn/proyecto.php?p=2.

58 «Escudo Aéreo Marítimo y Terrestre», Tasa de Seguridad Poblacional - Honduras, 20 de junio de 2017, https://www.tasadeseguridad.hn/proyecto.php?p=4.

presupuestos de las instituciones. En consecuencia, no es posible contar con un panorama general de la situación. Sin embargo, sí se ha logrado recabar información puntual con respecto a alguna empresa que provee al Estado servicios de videovigilancia. En este sentido, se pudo identificar que la compañía Cablecolor, brinda servicio de videovigilancia al Proyecto Centro Cívico, en construcción, según contrato firmado con la Secretaría de Defensa Nacional[59].

3.2.2 Nivel de posibilidad de contrataciones o interés de contratar bienes y servicios en tecnologías de vigilancia

Como se evidencia en el apartado 4 de este documento, existe evidencia de que el Estado Hondureño ha adquirido tecnologías de vigilancia. Se trata además de contrataciones realizadas mediante prácticas opacas que evitan la obligación de rendir cuentas a la ciudadanía.

4. Dimensión Tecnológica

4.1 Utilización de malware o spyware dentro del país

4.1.1 Evidencias de ataques o uso de malware, spyware, phishing u otras

Hacking Team fue contratado por es Estado hondureño(...) la DNII había gastado 355,000 euros en realizar compras a esta empresa en el año 2014.

En 2015 la empresa Hacking Team sufrió una ataque digital a partir del cual sus correos electrónicos y archivos se hicieron públicos. La organización Derechos Digitales realizó una investigación con base a los documentos filtrados mostrando que Hacking Team fue contratado por el Estado hondureño[60]. Este mismo estudio logró mostrar que la DNII había gastado 355,000 euros en realizar compras a esta empresa en el año 2014. La compra la habría realizado a través de la empresa Nice representada en la región por Ori Zoller[61]. El artículo no detalla cuál fue el tipo de software adquirido por Honduras.

59 «Contrato de Servicio entre Negocios Corporativos Cable Color y Secretaría de Defensa Nacional», 8 de julio de 2015, https://portalunico.iaip.gob.hn/archivos/SecretariadeDefensaNacional/Planeacion%20y%20rendicion%20de%20cuentas/Contrataciones/2017/contrato.pdf.
60 Pérez de Acha, Gisela, «Hacking Team Malware para la Vigilancia en América Latina», Derechos Digitales, marzo de 2016, https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf.
61 Ibíd.

Adicionalmente, es importante señalar que según reveló en 2018, el diario inglés The Guardian el gobierno Británico aprobó dos "licencias que permitían la exportación abiertas de una amplia gama de componentes militares y de telecomunicaciones, como programas, 'sensibles a las escuchas ilegales'" a Honduras[62]. Según esta misma fuente, la venta – de más 400.000 dólares - se habría realizado previo a la elección general de 2017, e incluiría tecnología que podría ser empleada para interceptar, monitorear y rastrear correos electrónicos, teléfonos móviles y servicios de mensajería en línea como WhatsApp[63].

The Guardian publicó que el gobierno Británico aprobó dos "licencias que permitían la exportación abiertas de una amplia gama de componentes militares y de telecomunicaciones, como programas, 'sensibles a las escuchas ilegales'" a Honduras

4.2 Escuchas telefónicas dentro del país

4.2.1. Casos en los que se evidencia el uso de escuchas telefónicas

La información relativa a la cantidad de solicitudes de escuchas telefónicas por año, al amparo de la Ley Especial sobre la Intervención de las Telecomunicaciones no está disponible[64]. Sin embargo, la autoridades hacen alarde del éxito de esta estrategia y de los resultados positivos que ha permitido obtener[6566].

Por otro lado, es importante señalar que en algunas ocasiones el Estado ha evidenciado que los controles y mecanismos para custodiar y resguardar la información intervenida son ineficaces. Por ejemplo, en 2016 el Ministerio Público detuvo a un funcionario de la Unidad de Intervenciones de las Comunicaciones, por vender información derivada de escuchas a un grupo de narcotraficantes[67].

62 Nina Lakhani, «UK Sold Spyware to Honduras Just before Crackdown on Election Protesters», *The Guardian*, 8 de febrero de 2018, sec. World news, https://www.theguardian.com/world/2018/feb/08/uk-sold-spyware-to-honduras-just-before-crackdown-on-election-protesters.
63 Ibíd.
64 Ley Especial sobre Intervención de las Comunicaciones Privadas, 12 de diciembre de 2011, Decreto 243.2011.
65 «Gobierno de Honduras califica de herramienta útil escuchas telefónicas», *Diario La Tribuna Honduras*, 12 de noviembre de 2015, http://www.latribuna.hn/2015/11/12/gobierno-de-honduras-califica-de-herramienta-util-escuchas-telefonicas/.
66 «BOLETIN INFORMATIVO 25 - 04 - 2018 Tribunal con Jurisdicción Nacional Declara Culpables a Dos Ciudadanos por el Delito de Secuestro.» (Poder Judicial de Honduras), accedido 17 de marzo de 2019, http://www.poderjudicial.gob.hn/CSJ-2016-2023/Juzgados-Tribunales/Documents/05042018-SalaIJN-Secuestro.pdf.
67 «Tegucigalpa: Cae empleado del MP por vender información confidencial», *Tiempo.hn | Noticias de última hora y sucesos de Honduras. Deportes, Ciencia y Entretenimiento en general.*, 17 de diciembre de 2016, Tiempo digital edición, https://tiempo.hn/tegucigalpa-cae-empleado-del-mp-vender-informacion-confidencial/.

4.3 Peticiones de información del gobierno sobre usuarios de servicios de Internet

Plataformas de Internet como Facebook[68], Google[69] y Twitter[70] publican informes semestrales de transparencia con información relativa a las solicitudes de información de datos sobre sus usuarios que realizan los diferentes gobiernos. En esta sección se realiza un análisis de la información recabada de estas fuentes desde el primer semestre de 2016 hasta el primer semestre de 2018.

4.3.1 Número de peticiones de información sobre usuarios de servicios de Internet por parte del gobierno

Las solicitudes que realizan los gobiernos puede afectar a una o más cuentas de usuarios. En la siguiente tabla se ve el resumen de solicitudes (S) y las cuentas de usuarias afectadas (U).

En el caso de Honduras se puede ver que son muy limitadas las capacidades del Gobierno de solicitar información. En en el caso de Google, este país ni siquiera está listado entre los proveedores.

La tabla 2 evidencia que en Honduras son muy limitadas las capacidades del Gobierno de solicitar información. En en el caso de Google, este país ni siquiera está listado entre los proveedores.

Tabla 2. Solicitudes de información realizadas por Honduras a Facebook, Google y Twitter (2016 - 2018)

	2016				2017				2018	
	1er semestre		2do semestre		1er semestre		2do semestre		1er semestre	
	S	U	S	U	S	U	S	U	S	U
Facebook	2	2	0	0	2	2	0	0	0	0
Google	-	-	-	-	-	-	-	-	-	-
Twitter	0	0	0	0	1	1	0	0	0	0

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

68 *Requests For User Data - HN*, acceso el 4 de marzo de 2019, https://transparency.facebook.com/government-data-requests/country/HN.
69 «Solicitudes de información sobre usuarios – Informe de transparencia de Google», Google, accedido 4 de marzo de 2019, https://transparencyreport.google.com/user-data/overview.
70 *Information Requests*, accedido 4 de marzo de 2019, https://transparency.twitter.com/en/information-requests.html.

4.3.2 Naturaleza de las peticiones de información sobre usuarios de servicios de Internet por parte del gobierno

La tabla 3 muestra las solicitudes generadas por semestre según el tipo de solicitud. La información de cada semestre se divide en el total de solicitudes (T), las solicitudes de carácter legal (L) y las de tipo de emergencia (E). Es importante señalar, que las solicitudes de tipo legal requieren que se haya establecido una solicitud legal en el país, mientras que las solicitudes de emergencia proveen la información cuando sucede una emergencia. En el caso de Twitter, esta empresa pública información relativa al tipo de solicitud.

Tabla 3. Solicitudes realizadas por Honduras a Facebook, Google y Twitter según tipo de solicitud (2016 - 2018)

	2016						2017						2018		
	1er semestre			2do semestre			1er semestre			2do semestre			1er semestre		
	T	L	E	T	L	E	T	L	E	T	L	E	T	L	E
Facebook	2	1	1	0	0	0	2	1	1	0			0		
Google	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Twitter	0	-	-	0	-	-	1	-	-	0	-	-	0	-	-

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

4.3.3 Peticiones aceptadas por las empresas

Los informes también registran el porcentaje de solicitudes que generan datos. Se entiende que cuando una solicitud genera datos, significa que las empresas han provisto información a las agencias estatales que lo han solicitado.

Según los informes disponible, el Estado hondureño recibió la información solicitada tan solo en un caso.

Tabla 4. Solicitudes realizadas por Honduras a Facebook, Google y Twitter aceptadas (2016 - 2018)

	2016				2017				2018	
	1er semestre		2do semestre		1er semestre		2do semestre		1er semestre	
Facebook	2	0%	0	0%	2	50%	0	0%	0	0%
Google	-	-	-	-	-	-	-	-	-	-
Twitter	0	0%	0	0%	1	0%	0	0%	0	0%

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

Por otro lado, también algunas de las empresas proveedoras de servicios de Internet y telefonía (IPS por sus siglas en inglés) publican en sus informes de transparencia información relativa a la solicitudes de información que realizan los Estados. Entre las empresas que operan en Honduras solo se han encontrado disponibles los informes de Millicom (Tigo).

Según reporta el informe de Millicom del año 2018, los datos agregados de Honduras, Costa Rica, El Salvador y Guatemala muestran que las solicitudes de metadatos en el conjunto de estos cuatro países se han reducido entre entre 2016 y 2018. Así, se pasó de 16.758 a 11.278 solicitudes[71]. A pesar, de la reducción en el último bienio, la cifra da cuenta de una importante demanda de este tipo de información. Sin embargo, el hecho de que los datos no están desagregados por país, impide conocer cuál ha sido el comportamiento en cada caso. Es más, aunque la cifra global se haya reducido podría haber aumentado en alguno de los países si se considera individualmente.

4.4 Vigilancia en Internet

4.4.1 Evidencia de Vigilancia en Internet por parte del gobierno

El Estado hondureño ha adquirido en los últimos años diferentes herramientas tecnológicas que, sin los controles adecuados, podrían emplearse para realizar acciones de vigilancia.

71 «2018 Millicom GroupLaw Enforcement Disclosure (LED) Report, Millicom», 2018, https://www.millicom.com/AnnualReport-2018Millicom/pdf/Millicom-2018-LED-Report.pdf

Según reporta el artículo de investigación "Herramientas de Vigilancia Digital Identificadas en Centroamérica"[72] la empresa Verint está registrada como empresa contratante para el Estado de la Oficina Normativa de Contratación del Estado (ONCAE) desde enero de 2016 . Por otro lado, hay evidencia de que que German Allan McNiel Rueda, Subdirector Nacional del Instituto Nacional Penitenciario (INP), realizó una visita a Trinidad y Tobago para ver una demostración del uso de estos sistemas en ese país. La tecnología que suministra esta empresa incluye videovigilancia y reconocimiento facial. Además, varias de sus herramientas se caracterizan por tener capacidades de vigilancia masiva[73]. Es importante señalar, que no se cuenta con el detalle de las herramientas concretas que el país podría haber adquirido. Por otro lado, el hecho de contar con las herramientas tampoco significa que se está haciendo un uso ilegítimo de ellas. Sin embargo, habida cuenta de la opacidad con la que se maneja este tipo de información, es esencial conocer los riesgos que podrían implicar.

El Estado hondureño ha adquirido en los últimos años diferentes herramientas tecnológicas que, sin los controles adecuados, podrían emplearse para realizar acciones vigilancia.

Por otro lado, también hay evidencia de que Honduras ha adquirido herramientas forenses para extraer información de celulares de la empresa Cellebrite y herramientas Encase[74].

Tabla 5. Herramientas de vigilancia y empresas proveedoras presentes en Honduras

	Recolección de información				Análisis de información
	Red	Internet/OSINT	Malware	Forense	
Verint	X	X			X
Cellebrite				X	X
Encase				X	X

Fuente: Bonifaz, R. (2019). "Herramientas de Vigilancia Digital Identificadas en Centroamérica".

72 Rafael Bonifaz. «Herramientas de Vigilancia Digital Identificadas en Centroamérica». Fundación Acceso, 2020, http://acceso.or.cr/assets/files/Art_Herramientas_Vigilancia_CA-mayo2020.pdf
73 Ibíd.
74 Ibíd.

4.5 Tecnologías de Reconocimiento Biométrico

4.5.1 Capacidad instalada en uso de tecnologías de reconocimiento biométrico

En el ámbito de la uso de tecnologías para el reconocimiento biométrico, es importante señalar que en los últimos años se han instalado cientos de cámaras en las principales ciudades del país. Así en 2017 se instalaron en Tegucigalpa 1.300 cámaras, cuya cobertura que permitía vigilar el 65% de la ciudad[75]. De forma similar en 2016 se instalaron 2.300 cámaras en diferentes ciudades del valle de Sula como Choloma, Villanueva y San Pedro[76].

En esta línea, en 2018 el portal de noticias de seguridad Secure Week promocionaba que el gobierno de Honduras instaló 3.800 cámaras adicionales en San Pedro Sula y Tegucigalpa. En este caso además se reporta que el sistema cuenta con una plataforma que recopila todos los incidentes reportados al 911, incluyendo los detectados por la red de cámaras[77]. El equipo instalado es resistente a la intemperie y el vandalismo. Además, logra captar imágenes de alta calidad (full HD) y cuenta con tecnología XDNR que permite eliminar el ruido visual aún en pobres condiciones de luz[78].

En el ámbito de la uso de tecnologías para el reconocimiento biométrico, es importante señalar que en los últimos años se han instalado cientos de cámaras en las principales ciudades del país.

4.6 Drones y globos de Vigilancia

4.6.1 Capacidad de los modelos de drones y globos de vigilancia utilizados

No se ha identificado información detallada acerca de la cantidad y el tipo de drones de los que disponen la autoridades de seguridad pública. Sin embargo, hay evidencia de que se cuenta con este tipo de tecnología. En este sentido, publicaciones de diferentes medios tradicionales y alternativos han reportado uso de drones en operaciones de seguridad ante protestas o

75 «Sistemas de cámaras de seguridad invaden Tegucigalpa», *Diario La Prensa*, 19 de febrero de 2017, https://www.laprensa.hn/sucesos/1045925-410/sistemas-de-cámaras-de-seguridad-invaden-tegucigalpa.
76 «Honduras: Echan a andar masivo proyecto de videovigilancia», *Tiempo.hn | Noticias de última hora y sucesos de Honduras. Deportes, Ciencia y Entretenimiento en general.*, 24 de agosto de 2015, Tiempo Digital edición, https://tiempo.hn/honduras-echan-a-andar-masivo-proyecto-de-videovigilancia/.
77 SecureWeek, «Hondureños disfrutan de calles más seguras con las cámaras de seguridad de Sony», SecureWeek, 19 de julio de 2018, https://www.secureweek.com/2018/07/18/hondurenos-disfrutan-de-calles-mas-seguras-con-las-camaras-de-seguridad-de-sony/.
78 «Sistema Nacional de Emergencias 911», Tasa de Seguridad Poblacional - Honduras, accedido 17 de marzo de 2019, https://www.tasadeseguridad.hn/proyecto.php?p=9.

actividades multitudinarias. Este es el caso, por ejemplo, del desalojo de manifestantes de la Universidad Autónoma de Honduras realizado en junio de 2018[79], de numerosos encuentros deportivos[80] y de operativos de seguridad[81].

También es importante señalar, que medios de prensa han revelado que Honduras ha adquirido drones Skykark 3, de la empresa israelí Elbit Systems. Se trata de aeronaves no tripuladas que disponen de armamento. Además, cuentan con antenas de rastreo satelital, envían video de alta definición en tiempo real y cuentan con visión nocturna. Según señalan responsables de las Fuerzas Armadas estos drones están destinados a la vigilancia fronteriza para extremar los controles ante el crimen organizado, terrorismo y narcotráfico[82].

4.7 Georeferenciación

4.7.1 Capacidad de georeferenciación

El teléfono móvil sigue siendo la forma más fácil de hacer seguimiento de georreferenciación. No hay registros de uso de tecnología celular para dar seguimiento a una persona en especial. Sin embargo, como ya se ha señalado, la Ley especial de Intervenciones a las Comunicaciones obliga a las operadoras de telefonía celular a tener un registro por cinco años de datos que podrían contribuir a la georeferenciación.

Paralelamente a ello, algunas ciudades hondureñas han instalado en los últimos años semáforos inteligentes que permiten la identificación. Ambas herramientas tecnológicas utilizadas de buena forma permiten una vigilancia permanente en caso de robo o hurto, pero sin los debidos controles también podrían prestarse para abusos.

79 «Jefe de Policía Nacional de Honduras planificó desalojo en el que torturaron a defensores de Derechos Humanos», Pasos de Animal Grande, accedido 17 de marzo de 2019, http://www.pasosdeanimalgrande.com/index.php/de/especiales/protesta-social-unah/item/2166-jefe-de-policia-nacional-de-honduras-planifico-desalojo-en-el-que-torturaron-a-defensores-de-derechos-humanos.
80 «Policía Nacional vigila el Motagua-Marathón con drones en el estadio Nacional», *Diez - Diario Deportivo*, 11 de febrero de 2018, https://www.diez.hn/liganacionaldehonduras/1151316-498/policia_nacional-estadio_nacional-motagua_marathon.
81 Redacción La Tribuna, «Seguridad emplea el "monitoreo aéreo" con drones y videocámaras», *Diario La Tribuna Honduras*, 24 de noviembre de 2017, http://www.latribuna.hn/2017/11/24/seguridad-emplea-monitoreo-aereo-drones-videocamaras/.
82 Xiomara Orellana, «Honduras vigilará fronteras con seis drones israelíes», *Diario La Prensa*, 6 de agosto de 2018, https://www.laprensa.hn/honduras/1204356-410/drones-honduras-skylark-narco-crimen-violencia-.

Nicaragua

FUNDACIÓN Acceso

Nota: Los capítulos de Guatemala, Honduras y El Salvador evidencian una opacidad y cultura del secreto generalizada en cuanto a las acciones de vigilancia del Estado. Esta situación es particularmente acentuada en el caso de Nicaragua, razón por la cual no se ha logrado contar con información suficiente en muchos de los apartados de este capítulo.

1. Jurídico-Legal

1.1 Protección de la privacidad a nivel constitucional

1.1.1 Nivel de protección de la privacidad en el país a nivel constitucional Protección de la privacidad en el país a nivel constitucional

La Constitución reconoce en su artículo 26 el derecho a la protección y respeto de la vida privada. Concretamente, este artículo señala que

La Constitución reconoce en su artículo 26 el derecho a la protección y respeto de la vida privada.

> "Toda persona tiene derecho: 1) A su vida privada y a la de su familia. 2) A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo. 3) Al respeto de su honra y reputación. 4) A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información" (Art. 26).

Por otro lado, el texto constitucional consigna en su artículo 45 el derecho al amparo señalando que

> "Las personas cuyos derechos constitucionales hayan sido violados o estén en peligro de serlo, pueden interponer el Recurso de Exhibición Personal o de Amparo, según el caso y de acuerdo con la Ley de Amparo" (Art. 45).

En este sentido, es importante destacar que en 2013 la Asamblea Nacional aprobó una reforma a la Ley de Amparo que agregó la figura de *habeas data*. Esto implica, que la ciudadanía puede

presentar recursos ante la Sala Constitucional cuando su derecho a la privacidad haya sido vulnerado o el uso de sus datos personales haya sido inapropiado[1].

1.2 Tratados y Convenciones Internacionales

1.2.1 Nivel de implicación de instrumentos internacionales - como tratados, acuerdos convenciones y otros - firmados por el país con relación a la privacidad

Según dispone el artículo 182 de la Constitución nicaragüense los tratados internacionales tienen un rango infraconstitucional. Es decir, en los casos en los que la Constitución y un instrumento internacional se contradicen, prevalece lo dispuesto en la Carta Magna. Concretamente, dicho artículo señala que:

> "La Constitución Política es la carta fundamental de la República; las demás leyes están subordinadas a ella. No tendrán valor alguno las leyes, tratados, decretos, reglamentos, órdenes o disposiciones que se le opongan o alteren sus disposiciones".

Según dispone el artículo 182 de la Constitución nicaragüense los tratados internacionales tienen un rango infraconstitucional. Es decir, en los casos en los que la Constitución y un instrumento internacional se contradicen, prevalece lo dispuesto en la carta magna.

El marco normativo internacional relativo a la privacidad vinculante en Nicaragua, considerando siempre las limitaciones derivadas del rango de dichos instrumentos en el país, es amplio. Retomando los planteamientos que realiza el documento "Privacidad y Acceso a la información pública en línea para Defensores y Defensoras de Derechos Humanos"[2], el primer texto normativo internacional relativo a los derechos humanos en espacios digitales es la Declaración Universal de Derechos Humanos, adoptada por la Organización de Naciones Unidas (ONU) en 1948. Esta declaración ya reconocía algunos aspectos fundamentales, según recogen los siguientes artículos:

> Artículo 12: "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. Toda persona

1 Daniel López, «Análisis de la normativa nicaragüense en materia de protección de datos», blog, 14 de marzo de 2019. http://dlcarballo.com/2019/03/14/analisis-de-la-normativa-nicaraguense-en-materia-de-proteccion-de-datos/

2 José Osorio, «Privacidad y Acceso a la información pública en línea para Defensores y Defensoras de Derechos…», Fundación Acceso - Medium (blog), 5 de septiembre de 2018, https://medium.com/@facceso.ca/privacidad-y-acceso-a-la-informaci%C3%B3n-p%C3%BAblica-en-l%C3%ADnea-para-defensores-y-defensoras-de-derechos-5690330c3762.

tiene derecho a la protección de la ley contra tales injerencias o ataques".

Artículo 19: "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas sin limitación de fronteras, por cualquier medio de expresión".

Artículo 29: "1. Toda persona tiene deberes respecto a la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad.

2. En el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática.

3. Estos derechos y libertades no podrán, en ningún caso, ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas".

También es relevante el Pacto Internacional de Derechos Civiles y Políticos. Dicho Pacto data de 1966 y fue ratificado por Nicaragua en 1980. Esta norma establece que los Estados deben garantizar a cada persona el disfrute de sus derechos civiles y políticos, incluyendo sus derechos económicos, sociales y culturales. Impone a los Estados la obligación de promover el respeto universal y efectivo de los derechos y libertades humanos, inclusive en la utilización de medios digitales donde la persona titular de los mismos pueda emitir expresiones que vayan en favor de las libertades de las personas y del interés general.

Posteriormente, en 1969, a nivel regional, se suscribió el Pacto de San José o la Convención Americana de Derechos Humanos (CADH). Este instrumento entró en vigor en 1978 y fue ratificado por Nicaragua en 1979. Entre las disposiciones más relevantes de la CADH destacan las siguientes:

Artículo 13: Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda

índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a. el respeto a los derechos o a la reputación de los demás, o

b. la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

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.

Artículo 14: Derecho de Rectificación o Respuesta, toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentada y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.

En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiese incurrido.

Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial.

La 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.

Principio 5, Declaración de Principios sobre la Libertad de Expresión

Adicionalmente, la Comisión Interamericana de Derechos Humanos ha desarrollado la Declaración de Principios sobre Libertad de Expresión. Se trata de un instrumento de gran relevancia ya que desarrolla algunos principios básicos en materia de libertad de expresión y privacidad:

Principio 1: La libertad de expresión, en todas sus formas y manifestaciones, es un derecho fundamental e inalienable, inherente a todas las personas. Es además, un requisito indispensable para la existencia misma de una sociedad democrática.

Principio 5: La 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.

Principio 10: Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas.

1.3 Leyes, reglamentos, decretos y normativas nacionales

1.3.1 Nivel de aplicación, transparencia y control de leyes, reglamentos, decretos y normativas relacionados con el derecho a la privacidad (leyes de telecomunicaciones, leyes ciberseguridad, inteligencia de Estado (secreto de Estado), leyes antiterroristas, o reformas de ley con artículos que indican prácticas que protegen o vulneran la privacidad

Son varias las leyes que en Nicaragua regulan aspectos vinculados con el derecho a la privacidad. Una de ellas es la Ley 787, de Protección de Datos Personales, aprobada en 2012. Esta ley se acompaña de un reglamento que fue aprobado ese mismo año.

El artículo 3 de la ley define los datos personales como aquella información sobre una persona natural o jurídica "que la identifica o la hace identificable". Este mismo artículo brinda una definición de datos personales informáticos señalando que se trata de "los datos personales tratados a través de medios electrónicos o automatizados" (Art., 3)[3]. Además, considera como datos personales sensibles:

> "toda información que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicos financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación" (Art. 3).

"El titular de los datos tiene derecho a solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros" Ley de Protección de Datos Personales Art. 10.

Por otro lado, esta ley establece en su artículo 9 lo relativo al tratamiento de los datos. Así, señala que – salvo en las excepciones previstas por ley – todo tratamiento estará sujeto al consentimiento de la persona titular de los datos.

El artículo 10 por su parte, se refiere al derecho al olvido digital, señalando que:

> "El titular de los datos tiene derecho a solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros" (Art. 10).

También es relevante la Ley 621 de Acceso a la Información Pública. Esta ley aprobada en 2007 define el ya mencionado *hábeas data* como:

> "La garantía de la tutela de datos personales privados asentados en archivos, registros, bancos de datos u otros medios técnicos, sean éstos públicos o privados, cuya publicidad constituya una invasión a la privacidad personal y familiar, que tenga relevancia con respecto a datos sensibles de las personas, su vida íntima, incluyendo sus asuntos familiares, que se encuentren en poder de las entidades especificadas en el Art. 1" (Art. 4).

3 Ley 787, de Protección de Datos Personales, 21 de marzo de 2012, Diario Oficial n. 61 del 29 de marzo de 2012, http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d

De igual manera, el *habeas data* garantiza el acceso de toda persona a la información que puede tener cualquier entidad pública sobre ella, así como el derecho a saber por qué y con qué finalidad tienen esa información (Art. 4)[4].

Otra norma relevante es la Ley 200, Ley General de Telecomunicaciones y Servicios Postales[5], en su artículo 2, numeral 6, se establece el deber de "garantizar y proteger la privacidad y la inviolabilidad de la correspondencia y las comunicaciones y la seguridad de la información transmitida". Asimismo, artículo 82 considera como infracciones muy graves:

> "interferir o interceptar intencionalmente los servicios de telecomunicaciones, afectar su funcionamiento e incumplir intencionalmente las leyes, reglamentos, tratados, convenios o acuerdos internacionales de telecomunicaciones en los cuales Nicaragua es parte, siempre y cuando se compruebe dolo manifiesto". (Art. 82)

en Nicaragua no hay una ley específica dedicada a la regulación de la intervención de las comunicaciones. La Constitución Política establece algunos de los supuestos en los que la intervención es permitida.

Finalmente, es importante señalar que, a diferencia de otros países de la región, en Nicaragua no hay una ley específica dedicada a la regulación de la intervención de las comunicaciones. La Constitución Política establece algunos de los supuestos en los que la intervención es permitida. Dichos supuestos se detallan y amplían la Ley 735, de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados. Esta norma establece que la comunicaciones podrán interceptarse a solicitud expresa y fundada del Fiscal General de la República o de la Dirección General de la Policía Nacional. Asimismo, un juez penal podrá tanto interceptar una comunicación telefónica, como "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"[6].

4 Ley 621 de Acceso a la Información Pública, 16 de mayo de 2007, Diario Oficial n. 118 del 22 de junio de 2007, http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/675A94FF2EBFEE9106257331007476F2

5Ley 200, Ley General de Telecomunicaciones y Servicios Postales, 22 de diciembre de 2005, https://www.telcor.gob.ni/MarcoLegal.asp?Accion=VerRecurso&REC_ID=178.

6 Mireia Zepeda, «¿Privacidad digital para defensores y defensoras de derechos humanos en Nicaragua?» https://www.ieepp.org/blog/Privacidad-digital-para-defensores-y-defenso ras-de/

En esta misma línea, el Código Procesal Penal, establece en los artículos 213 y 214 algunos delitos considerados graves que podrían dar lugar a la intervención de las comunicaciones. Se trata de delitos como:

> "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" (Art. 213)[7].

1.4 Normativa de seguridad nacional y ciberseguridad

1.4.1 Existencia de legislación relacionada con seguridad nacional y ciberseguridad

Lo relativo a la seguridad nacional se regula en Nicaragua mediante la Ley 919 de Seguridad Soberana de 2015. Esta Ley define el concepto de seguridad soberana como:

> "la existencia de paz y unidad permanente, dando tranquilidad y estabilidad a las y los nicaragüenses en su vida, en el trabajo, en la salud, en la educación, en la superación de la pobreza y la pobreza extrema, y en la promoción del desarrollo humano sostenible, en el que se garantiza el respeto a la Constitución Política, las Leyes de la República, prevaleciendo el poder del soberano.
>
> Esta contempla todos los ámbitos de la seguridad humana, seguridad ciudadana, seguridad alimentaria, seguridad agropecuaria, seguridad ambiental, seguridad interna y externa, es decir la seguridad de las personas, la familia, la comunidad y la nación.
>
> Es el fortalecimiento a la producción, trabajo, estudio de todas y todos los nicaragüenses, materializado a través de las responsabilidades compartidas entre la familia, comunidad, trabajadores y trabajadoras, productores y trabajadoras y el empresariado con el Estado, Ejército de Nicaragua y la Policía Nacional" (Art. 5, numeral 3)[8].

7 Ley 406, Código Procesal Penal, 13 de noviembre de 2001, Diario Oficial 243-244 del 21 y 24 de diciembre de 2001, http://legislacion.asamblea.gob.ni/Normaweb.nsf/%28$All%29/5EB5F629016016CE062571A1004F7C62
8 Ibíd.

Entre los objetivos de esta ley, enunciados en el artículo 6, destacan algunos como la preservación de la soberanía, la independencia y la integridad territorial; la protección de la vida y de la democracia; el mantenimiento del orden constitucional y el estado de derecho; la defensa del país frente a agresiones extranjeras; la lucha contra el narcotráfico y el crimen organizado transnacional; y la protección de la nación nicaragüense.

En su capítulo 2, la ley establece la creación del Sistema Nacional de Seguridad Soberana, que estará conformado por instituciones como el Ejército de Nicaragua; la Policía Nacional; el Sistema Nacional para la Prevención, Mitigación y Atención de Desastres; el Ministerio Público; la Procuraduría General de la República; los ministerios de Estado que tienen competencia en la seguridad alimentaria y nutricional; y otras instituciones, que en el ejercicio de sus funciones de ley, obtienen, generan y procesan información en el ámbito de la seguridad nacional (Art. 10).

Con respeto al derecho a la privacidad el artículo 13 dispone que las instituciones que conforman el Sistema Nacional de Seguridad Soberana no podrán:

> "1) Ejercer actividades de espionaje político.
>
> 2) Realizar actividades que impliquen el uso de la fuerza o la intimidación, durante el proceso de recolección, análisis y producción de información.
>
> 3) Obtener información o almacenar datos sensibles sobre personas por el motivo de nacimiento, nacionalidad, credo político, raza, sexo, idioma, religión, opinión, origen, posición económica o condición social, pertenencia a organizaciones o movimientos partidarios, sociales, sindicales o de cualquier otra índole, así como por cualquier actividad que desarrollen en el marco de la Constitución Política y la Ley.
>
> 4) Revelar o divulgar cualquier tipo de información adquirida en el ejercicio de sus funciones, mientras no sea ordenada por la autoridad competente, de acuerdo a las leyes de la materia.
>
> 5) Interceptar e intervenir comunicaciones telefónicas, postales, electrónicas o de cualquier otro sistema de transmisión de información, así como archivos, registros y documentos privados, sin la autorización expresa otorgada por la instancia judicial competente en los términos y formalidades establecidas por la Ley.

6) Simular como reales situaciones de orden ficticio, con el objeto de justificar y facilitar la acción represiva del Estado.

7) Transgredir los derechos y garantías establecidas en la Constitución Política de la República de Nicaragua y los derechos humanos reconocidos en los instrumentos internacionales aprobados y ratificados por Nicaragua según la Constitución Política". (Art. 13).

Organizaciones de la sociedad civil, como el Instituto de Estudios Estratégicos y Políticas Públicas (IEEPP), manifestaron su rechazo a esta ley ya que se enmarca en un proceso de reforma que habría tenido como objetivo "profundizar un modelo donde los cuerpos armados predominan sobre las instituciones civiles, manteniendo su subordinación únicamente al Presidente de la República"[9]. En este sentido, se plantea la preocupación por la falta de mecanismos de control civil.

Organizaciones de la sociedad civil (...) manifestaron su rechazo a esta Ley ya que se enmarca en un proceso de reforma que habría tenido como objetivo "profundizar un modelo donde los cuerpos armados predominan sobre las instituciones civiles, manteniendo su subordinación únicamente al Presidente de la República"

La ley fue criticada por la introducción de un nuevo concepto – el de seguridad soberana – que no cuenta con ningún tipo de respaldo en el marco jurídico internacional. Por otro lado, quienes se opusieron a la norma, también señalaron que la falta de precisión al definir dicho concepto podría propiciar discrecionalidad en su aplicación[10].

En el ámbito de la seguridad también es importante mencionar, la Ley 748 de la Defensa Nacional de la República de Nicaragua[11]. En dicha norma, la seguridad nacional se entiende como:

> "la condición permanente de soberanía, independencia, integridad territorial, paz y justicia social dirigida a preservar la integridad, estabilidad y permanencia del Estado de Nicaragua, sus instituciones, el orden democrático, estado social de derecho, el bien común, protección de las personas y sus bienes, frente a cualquier amenaza, riesgo o agresión, en apego a la Constitución Política de la República de Nicaragua, los derechos humanos, los convenios y tratados de los que Nicaragua es Parte en esta materia." (Art. 3, numeral 2)

En el artículo 5 se enuncian los 9 objetivos que busca alcanzar la ley. Entre ellos destacan la garantía de la soberanía y la independencia nacional; la garantía del Estado de Derecho, el orden

9 IEEPP. «10 peligros de la Ley de Seguridad Soberana». https://www.envio.org.ni/articulo/5121
10 Ibíd.
11 Ley 748, de Defensa Nacional de la República de Nicaragua, 13 de diciembre de 2010, Diario Oficial n. 244, 22 de diciembre de 2010, http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/9F1F361C509ED3F706257825004FE9BC?OpenDocument.

constitucional y la democracia; la protección de la vida y los bienes de la población; la preservación del medio ambiente y de los recursos estratégicos; el fortalecimiento y la promoción de la relaciones pacíficas con otras naciones, en particular con las centroamericanas; la contribución a la promoción de la paz y la seguridad regional; la garantía sin restricciones del respeto a los derechos humanos; el fomento del desarrollo humano sostenible; y la modernización del ejército.

Finalmente, es importante señalar que Nicaragua no cuenta con normativa específica relativa a la ciberseguridad. Además, el país no es firmante del Convenio de Budapest sobre ciberdelincuencia.

2. Dimensión Política

2.1 Relación entre Estado, empresas y cámaras de telecomunicaciones

2.1.1 Nivel de relación entre el Estado, empresas y cámaras de telecomunicaciones

2.1.2 Nivel de representación en cuanto a la relación entre el Estado, las empresas y las cámaras de telecomunicaciones

En 2013 el mercado de telefonía celular se distribuía entre dos operadoras: Enitel y Movistar. La primera contaba con el 53,89% del mercado, mientras que la segunda el 46,11%

La opacidad que prevalece en el accionar del Estado nicaragüense se evidencia también en la falta de fuentes e información relativa a la relación del Estado con empresas de telecomunicaciones.

El ente regulador de este ámbito es el Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR). La escasez de cifras oficiales provistas por esta entidad con respecto al sector da cuenta de la situación de falta de transparencia ya mencionada. De hecho, las cifras estadísticas disponibles en la página web de la entidad solo contemplan datos hasta 2013[12]. Según dichas cifras, en 2013 el mercado de telefonía celular se distribuía entre dos operadoras: Enitel y Movistar. La primera contaba con el 53,89% del mercado, mientras que la segunda el 46,11%. Los datos

12 «Estadísticas», TELCOR, acceso el 15 de enero de 2020, https://www.telcor.gob.ni/Desplegar.asp?PAG_ID=53

disponible también hace referencia a Sercom, señalando que no se cuenta con información para el caso de esa empresa[13].

Las cifras relativas a los servicios de Internet son aún más antiguas, datan de 2011, y evidencian que la empresa Claro controlaba en aquel momento gran parte del mercado (65,74%). Laparticipación de Movistar era de 8,76% y la de Yota de 11,21%. El 14,29% restante se distribuía entre otras empresas de menor envergadura[14]. El informe de Transparencia de Telefónica del 2019 no incluye Nicaragua, ya que a fecha de publicación de dicho informe Telefónica estaba finalizado el proceso de desinversión[15].

La cámara que reúne a la empresas del sector es la Cámara Nicaragüense de Internet y Telecomunicaciones (CANITEL). Desde 2015 CANITEL es además miembro del Consejo Superior de la Empresa Privada (COSEP). CANITEL integra a empresas como Movistar, Tigo o Claro, entre otras.

2.2 Contratos entre el Estado y las empresas de seguridad privada

El peso de las empresas de seguridad privada en Nicaragua es, según reportan fuentes de prensa, menor que en otros países de la región como El Salvador, Honduras o Guatemala.

2.2.1 Nivel de impacto de los contratos establecidos entre el Estado y empresas de seguridad privada

Tampoco ha sido posible acceder a información detallada acerca de las contrataciones de seguridad privada realizadas por parte del Estado Nicaragüense. Sin embargo, es importante señalar que el peso de las empresas de seguridad privada en Nicaragua es, según reportan fuentes de prensa, menor que en otros países de la región como El Salvador, Honduras o Guatemala. Así, el Nuevo Diario reportaba en 2015 que en Nicaragua había en aquel momento 160 empresas dedicadas a las seguridad privada. Las actividades realizadas por estas empresas implicaban un gasto anual de 124 millones de dólares, muy por debajo de los montos invertidos en los países del Triángulo Norte, que van de los 200 a 460 millones de dólares[16]. En cualquier caso, información

13 Ibíd.
14 Ibíd.
15 «Informe sobre transparencia en las comunicaciones», Telefónica, 2019, https://www.telefonica.com/documents/153952/183394/Informe-Transparencia-Comunicaciones-2019.pdf/00cb6cba-dbe7-df8d-64d1-df8510830960
16 Ricardo Guerrero. «Nicaragua con menos gasto en seguridad privada». Nuevo Diario. 23 de marzo de 2015. https://www.elnuevodiario.com.ni/economia/355993-nicaragua-menos-gastos-seguridad-privada/

brindada también por fuentes de prensa evidencia que el peso de estas empresas en el país no es menor, ya que en 2014 empleaban a 18.000 personas, mientras que la fuerza policial era de 12.000 agentes[17].

También hay otros indicios que permiten estimar la relevancia de estas empresas en el país. En este sentido, destaca que el país es la sede del Instituto Centroamericano de Seguridad Privada (INCASAPRI)[18]. Este instituto está a cargo de la realización del evento Expo Seguridad, una feria dedicada a la promoción de los productos y servicios brindados por las empresas de seguridad privada. Dicho evento fue realizado en 2014 en Nicaragua. El entonces Presidente del Instituto Centroamericano de Seguridad Privada, Luis González, señaló en el marco de este evento que el desarrollo de esta industria estaba relacionado en Nicaragua más con el crecimiento económico del país que con el aumento de la inseguridad[19].

2.3 Relación de actores estatales o políticos con las directivas de empresas de seguridad

2.3.1 Nivel de relación del Estado con empresas de seguridad privada

La información relativa a los posibles nexos entre actores estatales y las empresas de seguridad también se ha obtenido a partir de fuentes periodísticas. Un artículo de investigación publicado por el periódico La Prensa en 2010 señala que José Jorge Mojica Mejía, cercano a Daniel Ortega y el FSLN, era el propietario de la empresa de seguridad El Goliat[20]. Dicha empresa había obtenido contratos millonarios por parte del Estado a partir de octubre de 2009[21]. Según recoge este medio de comunicación el ejecutivo de Ortega manejó la información relativa a El Goliat de manera poca transparente, tratando de ocultar quiénes eran sus propietarios.

17 Octavio Enríquez. El pastel de la seguridad privada. El Confidencial. 1 de diciembre de 2014. https://confidencial.com.ni/archivos/articulo/20318/el-pastel-de-la-seguridad-privada

18 «Nosotros», Instituto Centroamericano de Seguridad Privada, acceso el 23 de marzo de 2019, https://www.incaspri.com/inicio/nosotros/.

19 «El negocio de la seguridad privada en Nicaragua», Central America Data, 3 de marzo de 2014, https://www.centralamericadata.com/es/article/home/El_negocio_de_la_seguridad_privada_en_Nicaragua.

20 Octavio Enríquez, «Pistas de El Goliat apuntan a empleado del Presidente», La Prensa, accedido 23 de marzo de 2019, https://www.laprensa.com.ni/2010/06/19/nacionales/28383-pistas-de-el-goliat-apuntan-a-empleado-del-presidente.

21 «La fortuna de un empleado de Ortega - La Prensa». https://www.laprensa.com.ni/2010/06/20/nacionales/28474-la-fortuna-de-un-empleado-de-ortega

La investigación realizada por La Prensa plantea además, que se trataría de contrataciones irregulares, ya que por mandato constitucional las instituciones no podría otorgar adjudicaciones a empresas vinculadas al partido de Gobierno. Por otro lado, en algunos casos – como el de un contrato realizado por la alcaldía de Managua – la adjudicación se habría realizado de manera directa sin que mediara un concurso. Esto también habría implicado una irregularidad, ya que no habría ninguna justificación para la no realización del concurso[22].

2.4 Planes de Gobierno en vigencia en materia de seguridad nacional

2.4.1 Planes de gobierno vigentes relacionados con la seguridad nacional y ciberseguridad que protegen o vulneran la privacidad

Nicaragua desarrolló durante la década del 2000 una Estrategia de Seguridad Ciudadana. Dicha estrategia fue construida en el marco del programa de gobernabilidad democrática y respeto a los derechos humanos del PNUD y en alianza con el Ministerio de Gobernación. Se trató de un proceso "participativo de diálogo, concertación y formulación de Líneas Estratégicas para el desarrollo de nuevas políticas públicas sobre la prevención social del delito"[23]. A partir de dichas líneas estratégicas se formularon el Plan Nacional de Lucha contra las Drogas (2002-2006), el Plan Nacional de Prevención de la Violencia IIntrafamiliar y Sexual (2001-2006), el Programa de Desarrollo Integral para la Prevención de la Violencia Juvenil, el Programa Nacional de Seguridad Ciudadana, el Proyecto Fortalecimiento de la Seguridad Ciudadana en el Sistema Penitenciario Nacional, entre otros, con un fuerte enfoque en prevención[24].

Es importante señalar, sin embargo, que dicha estrategia no está vigente y que no se ha encontrado ningún plan o política de seguridad nacional que se esté implementando en la actualidad. Sin embargo, como ya se ha señalado, el país sí cuenta con una ley específica en esta

22 Octavio Enríquez, «Pistas de El Goliat apuntan a empleado del Presidente», La Prensa, accedido 23 de marzo de 2019, https://www.laprensa.com.ni/2010/06/19/nacionales/28383-pistas-de-el-goliat-apuntan-a-empleado-del-presidente.
23 PNUD. Nicaragua. «Seguridad Ciudadana. Evaluación de proyecto». https://www.resdal.org/Archivo/le-cap1.htm
24 RESDAL. «Líneas Estratégicas de Seguridad Ciudadana en Nicaragua». https://www.resdal.org/Archivo/le-cap1.htm

materia. Se trata de la Ley 919 de Seguridad Soberana en Nicaragua. En un recurso de amparo el Centro Nicaragüense de Derechos Humanos (CENIDH) planteó sus preocupaciones con respecto a esta ley. En primer lugar, la ley le estaría atribuyendo soberanía a la seguridad, un concepto sin duda poco ortodoxo, que implicaría darle a la seguridad un estatus superior a otros ámbitos y desconocería, al mismo tiempo, que la soberanía reside en el pueblo:

> "la ley atribuye a la seguridad el carácter de soberana, cuando la Constitución otorga la soberanía al pueblo y hace referencia al soberano sin especificar a quien se está refiriendo. La preeminencia que se le da a la seguridad sobre otros derechos predetermina a quienes aplicarán la Ley, invadiendo funciones propias de la justicia y compromete la ponderación de derechos que corresponde hacer en cada caso concreto"[25].

La ley propiciaría la discrecionalidad atentando contra derechos como "el derecho de manifestación, la libertad de expresión, el derecho de reunión, el derecho de asociación, el derecho mismo de defender derechos humanos que es fundamental para el ejercicio de este derecho; tener la posibilidad de expresarse libremente y de participar en manifestaciones"

Por otro lado, la ley propiciaría la discrecionalidad atentando contra derechos como "el derecho de manifestación, la libertad de expresión, el derecho de reunión, el derecho de asociación, el derecho mismo de defender derechos humanos que es fundamental para el ejercicio de este derecho; tener la posibilidad de expresarse libremente y de participar en manifestaciones"[26].

Ya se ha señalado que en Nicaragua no existe una política expresa en materia de ciberseguridad. Sin embargo, es importante señalar que a partir de 2018 se han realizado intentos de aprobar una "ley mordaza" con el objetivo de regular las redes sociales. Dicha normativa se justificó apelando a la necesidad de proteger a la niñez y las familias de la mala influencia de la redes sociales. No obstante, diferentes actores, han denunciado que se trataba de una estrategia para silenciar a la oposición[27].

Finalmente, es importante señalar que el Código Penal de Nicaragua contiene algunos artículos que permiten penalizar algunas formas de delincuencia cibernética. Por ejemplo, el artículo 198 sanciona "Quien, sin la debida autorización, utilice los registros informáticos de otro, o

25 CENIDH. «CENIDH presenta recurso por inconstitucionalidad contra la Ley de Seguridad Soberana». https://www.cenidh.org/noticias/871/
26 Ibíd.
27 Fundación Acceso. «Encuentro Centroamericano de Seguridad Digital» y Gloria Argüello, «La prevención del ciber crimen permite a Nicaragua tener una de las tasas más bajas de este delito», Consejo Nicaragüense de Ciencia y Tecnología, 27 de abril de 2016, http://conicyt.gob.ni/index.php/2016/04/27/la-prevencion-del-ciber-crimen-permite-a-nicaragua-tener-una-de-las-tasas-mas-bajas-de-este-delito/..

ingrese, por cualquier medio, a su banco de datos o archivos electrónicos".

2.5 Relación de los planes de seguridad nacional y ciberseguridad con la privacidad

2.5.1 Nivel de protección o vulneración de la privacidad de los planes de gobierno vigentes relacionados con la seguridad nacional y ciberseguridad

Según se menciona en el punto anterior, en los últimos años se han impulsado reformas legales en lo relativo a la seguridad nacional tales como la ley "mordaza" o reformas al Código Penal. Como ya se ha señalado, dichas reformas implican importantes riesgos para la privacidad. De hecho, organizaciones de la sociedad civil han denunciado que las reformas propiciarían la violación del derecho de manifestación, la libertad de expresión, el derecho de reunión, el derecho de asociación o el derecho a defender derechos humanos[28].

2.6 Uso de tecnológicas de vigilancia como evidencia o caso para criminalizar o judicializar

2.6.1 Casos en los que se usan evidencias de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos que ejercen sus derechos humanos y civiles

No se han identificado evidencias reportadas en fuentes de investigación o prensa que den cuenta del uso de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas o colectivos. Tampoco en las entrevistas realizadas se han recibido denuncias de este tipo.

2.6.2 Identificación de tecnologías de vigilancia para criminalizar, deslegitimar y amenazar a personas y colectivos que ejercen sus derechos humanos y civiles

En el contexto ola represiva desatada a raíz de la crisis política de 2018, numerosas personas defensoras han denunciado el uso de tecnologías de vigilancia para controlar a la población en

28 CENIDH. «CENIDH presenta recurso por inconstitucionalidad contra la Ley de Seguridad Soberana». https://www.cenidh.org/noticias/871/

general y en particular a quienes defienden los derechos humanos en el país[29]. Sin embargo, no se cuenta con evidencia que respalde esta sospecha.

2.7 Acuerdos bilaterales y multilaterales de cooperación en materia de seguridad

2.7.1 Existencia de acuerdos bilaterales y multilaterales de cooperación en materia de seguridad

Nicaragua cuenta con diversos acuerdos bilaterales y multilaterales en materia de seguridad. Entre ellos destacan las relaciones de cooperación bilateral con Rusia. En este sentido, ambos países firmaron en 2014 un acuerdo de cooperación que permite el atraque de navíos militares rusos en puertos nicaragüenses. El entonces ministro de Defensa de Rusia, Serguéi Shoigu, y su homólogo nicaragüense, Julio César Avilés, concretaron una cooperación técnica y militar que según palabras de Shoigu "formaliza jurídicamente nuestras tradicionales relaciones de amistad"[30].

En esta misma línea, fuentes de prensa reportan que en 2017 se instaló en el suroeste de Managua la estación terrestre del Sistema Global de Navegación por Satélite (Glonass). Se trata de una infraestructura similar al GPS estadounidense y el Galileo europeo. También la prensa, señala que el hermetismo de ambos gobiernos con respecto al proyecto ha sido total[31].

Este hermetismo ha generado desconfianza entre la sociedad civil, ya que se percibe que - aunque se ha tratado de justificar señalando que su objetivo es la lucha contra el narcotráfico - se trata de una fachada para esconder un centro de espionaje[32].

29 Fundación Acceso, «Encuentro Centroamericano de Seguridad Digital, 2019.
30 «Rusia y Nicaragua firman acuerdos de cooperación», Telesur, 12 de febrero de 2015, https://www.telesurtv.net/news/Rusia-y-Nicaragua-firman-acuerdos-de-cooperacion-20150212-0055.htm
31 Leire Ventas, «La Enigmática Estación Satelital Que Rusia Instaló En Nicaragua Para "Combatir El Narcotráfico" y Que Inquieta a EE.UU.», 23 de junio de 2017, sec. América Latina, https://www.bbc.com/mundo/noticias-america-latina-40352903; «La base de vigilancia de Rusia en Nicaragua que preocupa a la región», Infobae, 1 de julio de 2017, https://www.infobae.com/america/america-latina/2017/07/01/la-base-secreta-de-espionaje-de-rusia-en-nicaragua-que-preocupa-a-la-region/; Emili Blasco, «Rusia hace de Nicaragua su Cuba del siglo XXI», ABC, 14 de agosto de 2017, https://www.abc.es/internacional/abci-rusia-hace-nicaragua-cuba-siglo-201708141811_noticia.html; y «¿Hay un centro de espionaje ruso en Nicaragua?», Revista Estrategia & Negocios, 24 de abril de 2017, https://www.estrategiaynegocios.net/lasclavesdeldia/1065359-330/hay-un-centro-de-espionaje-ruso-en-nicaragua.
32 «¿Hay un centro de espionaje ruso en Nicaragua?», Revista Estrategia & Negocios, 24 de abril de 2017, https://www.estrategiaynegocios.net/lasclavesdeldia/1065359-330/hay-un-centro-de-espionaje-ruso-en-nicaragua.

3. Dimensión Económica

3.1 Presupuestos nacionales destinados a seguridad y gastos reservados

3.1.1 Total de presupuesto en líneas de los presupuesto nacionales destinados a gastos reservados

En la clasificación por objeto de gasto del presupuesto del Estado nicaragüense existe un renglón de gasto reservados. Se trata de una práctica de opacidad presupuestaria muy difundida en América Latina. En Nicaragua, los gastos reservados se incluyen en rubro de *otros servicios*. Dentro de este rubro general se contemplan "servicios no personales no especificados en los rubros anteriores, tales como atenciones sociales, servicios de vigilancia y gastos reservados, etcétera"[33]. Sin embargo, no se ha encontrado información que de cuenta del monto que se dedica anualmente a este tipo de gastos.

3.1.2 Total del presupuesto nacional destinado a seguridad

El gasto destinado en Nicaragua a seguridad puede estimarse considerando lo asignado en los presupuestos nacionales al Ministerio de Defensa y a la Policía Nacional. Es importante señalar, que los presupuestos más recientes – de 2015 a 2018 – consignan el presupuesto destinado a la Policía Nacional, considerándola una institución independiente. En los presupuestos previos, sin embargo, dicho gasto estaba integrado en el presupuesto del Ministerio de Gobernación bajo el rubro "Mantenimiento del orden público, protección ciudadana, prevención e investigación del delito".

Por otro lado, la tabla 1 muestra que entre 2012 y 2014 el presupuesto dedicado a Defensa fue superior al destinado a la Policía Nacional. Sin embargo, a partir de 2015 se ha destinado más fondos a la Policía Nacional todos los años, salvo en 2018.

33 «Clasificador por Objeto del Gasto» (Ministerio de Hacienda y Crédito Público, 2012), http://www.hacienda.gob.ni/documentos/presupuesto/estudio/actualizacion%202012%20Clasificador%20por%20objeto%20del%20gasto.pdf.

Tabla 1. Presupuesto votado para los ramos de Defensa Nacional y Policía Nacional Nicaragua (2012-2018)

	Ministerio de Defensa Nacional		Policía Nacional		Total	
	Abs.	%	Abs.	%	Abs.	%
2012	1,548,556,214	3,66%	1,453,439,999	3,44%	3,001,996,213	7,1%
2013	2,104,031,221	4,41%	1,694,132,000	3,55%	3,798,163,221	7,95%
2014	2,151,798,000	3,86%	2,059,641,000	3,69%	4,211,439,000	7,55%
2015	1,952,177,889	3,2%	2,292,179,034	3,76%	4,244,356,923	6,95%
2016	2,076,628,000	2,89%	2,834,767,281	3,94%	4,911,395,281	6,83%
2017	2,509,586,292	3,14%	3,367,890,845	4,91%	5,877,477,137	7,35%
2018	3,681,646,014	4,23%	2,577,613,711	2,96%	6,259,259,725	7,18%

Fuente: Elaboración propia con base a datos públicos del presupuesto de la República en cada año. Montos en córdobas.

Entre 2012 y 2014 el presupuesto dedicado a Defensa fue superior al destinado a la Policía Nacional. Sin embargo, a partir de 2015 se ha destinado más fondos a la Policía Nacional todos los años, salvo en 2018.

3.1.3 Instituciones Estatales que tienen líneas de presupuesto destinadas a seguridad y gastos reservados

La mayoría de las instituciones del Estado cuentan con un rubro destinado a seguridad o vigilancia. Sin embargo, no se ha logrado información suficiente para detallar un listado de las instituciones que en efecto incluyen este gasto.

3.1.4 Montos de contratos relacionados con compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

El portal de compras estatal Nicaragua Compra incluye al menos ocho tipos de bienes y servicios con número de catálogo relacionados con la seguridad y las tecnologías de vigilancia:

- Avión de reconocimiento y vigilancia (25131707).
- Software de vigilancia de redes (43232801).
- Equipo de vigilancia y detección (46171600).

- Grabadoras de sonido o vídeo de vigilancia (46171621).
- Servicios de seguridad y protección personal (92120000).
- Servicios de sistemas de seguridad (92121700).
- Vigilancia o mantenimiento o control de alarmas (92121701).
- Mantenimiento o control de sistemas de vigilancia de reclusión (92121704)[34].

No fue posible identificar en dicho portal adjudicaciones realizadas para la compra de este tipo de bienes o servicios.

3.1.5 Instituciones encargadas de los contratos relacionados con compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

No ha sido posible acceder a la información necesaria para analizar los aspectos previstos para este apartado.

3.2 Empresas proveedoras de bienes y servicios en materia de tecnologías de vigilancia

3.2.1 Empresas que tienen los contratos relacionados de compra de bienes y servicios en materia de seguridad que incluyan tecnologías de vigilancia

No ha sido posible acceder a la información necesaria para analizar los aspectos previstos para este apartado.

3.2.2 Nivel de posibilidad de contrataciones o interés de contratar bienes y servicios en tecnologías de vigilancia

Tomando en cuenta la oferta privada de seguridad privada existente en el país, la contratación de este tipo de servicios por parte del Estado no es improbable. Sin embargo, no ha sido posible acceder a la información necesaria para analizar dichos aspectos.

34 «Inicio», Nicaragua Compra, acceso el 24 de marzo de 2019, http://www.nicaraguacompra.gob.ni/.

4. Dimensión Tecnológica

4.1 Utilización de malware o spyware dentro del país

4.1.1 Evidencias de ataques o uso de malware, spyware, phishing u otras

No se han identificado evidencias de uso de malware en Nicaragua. Las filtraciones e investigaciones que han evidenciado el uso malware como Galileo o Pegasus en países de la región como Honduras o Guatemala no han señalado que hayan sido empleados en este país[35].

4.2 Escuchas telefónicas dentro del país

4.2.1. Casos en los que se evidencia el uso de escuchas telefónicas

No se ha logrado acceder a información que de cuenta de las escuchas telefónicas realizadas dentro de los supuestos permitidos en la legislación nacional. Sin embargo, es importante señalar que representantes de la sociedad civil han denunciado en diferentes momentos que este tipo de prácticas se realizan de manera ilegal.

El Diario La Prensa publicó en 2013 un reportaje en el que líderes de la oposición y líderes religiosos denunciaban haber sido víctimas de espionaje ilegal.

En este sentido, el Diario La Prensa publicó en 2013 un reportaje en el que líderes de la oposición y líderes religiosos denunciaban haber sido víctimas de espionaje ilegal. En dicho artículo un ex-diputado afirmó tener fundadas sospechas de que su telefóno estaba siendo intervenido. De la misma manera, un obispo católico manifestó haber sufrido una situación similar[36]. El Ejecutivo nicaragüense rechazó estas denuncias[37].

35 Rafael Bonifaz. «Herramientas de Vigilancia Digital Identificadas en Centroamérica». Fundación Acceso, http://acceso.or.cr/assets/files/Art_Herramientas_Vigilancia_CA-mayo2020.pdf

36 «El gran ojo que espía», La Prensa, 3 de noviembre de 2013, https://www.laprensa.com.ni/2013/11/03/reportajes-especiales/168521-el-gran-ojo-que-espia.

37 Vladimir Vásquez, «Telcor niega espionaje telefónico en Nicaragua - La Prensa», La Prensa, 4 de noviembre de 2013, https://www.laprensa.com.ni/2013/11/04/nacionales/168699-telcor-niega-espionaje-telefonico-en-nicaragua.

4.3 Peticiones de información del gobierno sobre usuarios de servicios de Internet

Empresas proveedoras de servicios de Internet como Google, Facebook o Twitter publican de forma semestral informes sobre solicitudes de información realizadas por gobiernos. Según los informes que dan cuenta de este tipo de solicitudes, entre 2016 y el primer semestre de 2018, a diferencia de otros países de la región, Nicaragua no solicitó información a estas empresas en ninguna ocasión[38].

4.4 Vigilancia en Internet

4.4.1 Evidencia de Vigilancia en Internet por parte del gobierno

Según un estudio realizado por Citizenlab en 2013, en Nicaragua se descubrió que servidores ejecutaban el software PacketShapper de la empresa Bluecoat en redes públicas. Este software permitiría tanto el análisis del tráfico de la red como el bloqueo de sitios de Internet[39].

Según un estudio realizado por Citizenlab en 2013, en Nicaragua se descubrió que servidores ejecutaban el software PacketShapper de la empresa Bluecoat en redes públicas. Este software permitiría tanto el análisis del tráfico de la red como el bloqueo de sitios de Internet

Por otro lado, según un artículo sobre herramientas de vigilancia en Centroamérica, también existen posibilidades que el Estado haya adquirido o esté interesado en adquirir software de la empresa Verint[40]. Esta empresa cuenta con herramientas de videovigilancia y reconocimiento facial. Además, ofrece productos que realizan "Inteligencia en Redes" (Network Intelligence) y que permiten recolectar el tráfico de una red a cualquier escala. De forma adicional a la interceptación, los productos de esta empresa pueden analizar la información tanto en tiempo real como de manera retrospectiva. Si bien no se cuenta con evidencias de que el gobierno haya comprado herramientas de esta empresa, se sabe que Verint se registró como marca en este país en diciembre de 2011. Dicho registro tiene una validez de 10 años[41].

38 Rafael Bonifaz , «Herramientas de Vigilancia Digital Identificadas en Centroamérica», Fundación Acceso, 2020.
39 Ibíd.
40 Ibíd.
41 Ibíd.

También existen evidencias que el Estado Nicaragüense ha mostrado interés en la adquisición de licencias de Encase y otros sistemas de vigilancia[42]. Encase se emplea para análisis forense y provee un conjunto de herramientas de software y hardware para investigaciones policiales. Permite copiar el contenido íntegro de dispositivos de almacenamiento.

El siguiente cuadro, tomado del artículo "Herramientas de Vigilancia Digital Identificadas en Centroamérica", sintetiza la información acerca de las herramientas identificadas en Nicaragua[43].

Tabla 2. Herramientas de vigilancia y empresas proveedoras presentes en Nicaragua

	Recolección de información				Análisis de información
	Red	Internet/OSINT	Malware	Forense	
BlueCoat	X				
Verint	X	X			X
Encase				X	X

4.5 Tecnologías de Reconocimiento Biométrico

4.5.1 Capacidad instalada en uso de tecnologías de reconocimiento biométrico

No se pudo acceder a datos específicos sobre este indicador. Si bien existen sistemas de reconocimiento biométrico en aeropuertos y otros puntos de migración, no contamos con evidencias o indicios de inversiones municipales o estatales en este aspecto.

Sin embargo, si se logró identificar que en Managua se cuenta desde 2017 con un un proyecto de semáforos inteligentes. Estos semáforos poseen cámaras para regular el tráfico[44].

42«Pliego de cláusulas administrativas particulares», 23 de marzo de 2017, 6, https://www.policia.gob.ni/wp-content/uploads/2017/03/PLIEGO-L.P.-06-2017-Compra-de-Equipamiento-Especializado-TICs.pdf.
43 Rafael Bonifaz , «Herramientas de Vigilancia Digital Identificadas en Centroamérica», Fundación Acceso, 2020.
44 «Semáforos inteligentes para todas las intersecciones capitalinas», La Voz del Sandinismo, 28 de abril de 2017, https://www.lavozdelsandinismo.com/nicaragua/2017-04-28/semaforos-inteligentes-todas-las-intersecciones-capitalinas/.

4.6 Drones y globos de Vigilancia

4.6.1 Capacidad de los modelos de drones y globos de vigilancia utilizados

El uso de drones por parte de particulares está prohibido en territorio nicaragüense. Dicha prohibición fue establecida por el Instituto Nicaragüense de Aeronáutica Civil en 2014[45].

Por otro lado es importante señalar, según reportan diferentes medios de prensa, periodistas han denunciado públicamente el uso de drones como forma de intimidación y vigilancia. Ese es el caso del periodista Miguel Mora que denunció que un dron vigilaba su residencia el 25 de noviembre de 2018[46]. En esta misma línea, en diciembre de ese mismo año otro dron fue visto vigilando las instalaciones del canal 100% Noticias[47].

4.7 Georeferenciación

4.7.1 Capacidad de georeferenciación

El teléfono móvil sigue siendo la estrategia para la georeferenciación más sencilla. También es accesible el reconocimiento OCR de matrículas, que permite triangular la ubicación de una persona en el territorio. Por otro lado, no hay pruebas técnicas que den cuenta del uso de aparatos GPS para dar seguimiento a personas específicas.

45 «Restricción para uso de Drones en Nicaragua», INAC, 29 de noviembre de 2014, http://www.inac.gob.ni/2014/11/restriccion-para-uso-de-drones/.
46 «Paramilitares sandinistas envían dron a vivienda de Miguel Mora», 100% Noticias, 25 de noviembre de 2018, https://100noticias.com.ni/nacionales/94868-dron-casa-miguel-mora/.
47 «Dron de paramilitares sandinistas espían y asedian instalaciones de 100% Noticias», 100% Noticias, 7 de diciembre de 2018, https://100noticias.com.ni/nacionales/95205-dron-espia-100-noticias/.