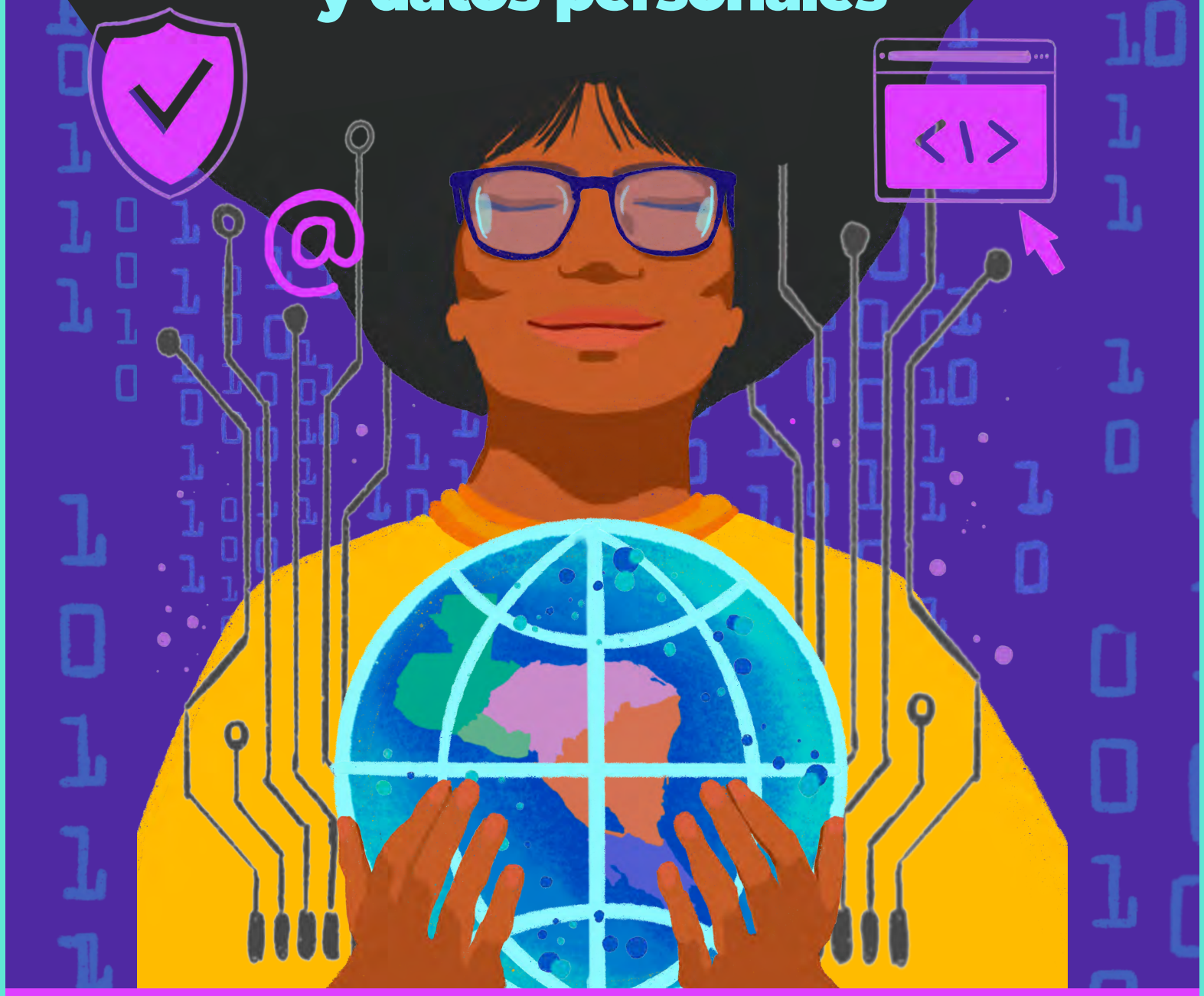
FUNDACIÓN Acceso

Informe sobre los marcos legales vigentes de Centroamérica en materia de vigilancia tecnológica, privacidad y datos personales



Temáticas principales:

vigilancia tecnológica, privacidad, datos personales.

índice

Introducción

El presente informe tiene por objetivo realizar un análisis comparativo de los marcos normativos nacionales de Guatemala, El Salvador, Honduras, Nicaragua y Costa Rica que se refieren a la regulación de los derechos de uso de la tecnología en relación con lzos derechos fundamentales de las personas. De esta forma, se hará énfasis en la regulación de cada país en cuanto a la protección de la privacidad, inviolabilidad de comunicaciones, protección de datos personales, delitos informáticos, leyes de inteligencia y vigilancia tecnológica.

El uso de tecnologías para la vigilancia ilegal pone en amenaza varios derechos humanos, entre ellos el derecho a la privacidad y a la protección de la información; también pone en riesgo la integridad y seguridad de las personas en general, y, en particular, de aquellas que ejercen el periodismo o realizan activismo en la promoción y defensa de los derechos humanos.

Se trata de técnicas de vigilancia a las personas y organizaciones que son de naturaleza invasiva, que permiten tener acceso total a la información como leer, escuchar, rastrear, crear perfiles o utilizar cualquier información a la que se tenga acceso a través de las tecnologías de la información y las redes sociales (Ramírez, 2018).

El objetivo es presentar una visión amplia y comparativa de los marcos jurídicos de los cinco países que sirva como guía para identificar vacíos normativos que distintos actores de la sociedad civil, la academia y personas que toman decisiones puedan relevar y subsanar dichas legislaciones para que, a futuro, cumplan con los estándares internacionales en estas materias.
Finalmente, el anexo 1 de este informe incluye una tabla comparativa respecto del cumplimiento de ciertos estándares que permita una comparación visual clara y sencilla.

Glosario de términos

Convenio de Budapest:

es un tratado internacional que pacta sobre delitos cometidos a través de internet, redes o tecnologías de la información y la comunicación. También, establece competencias y procedimientos para la investigación de delitos y la evidencia electrónica, entre las cuales están la interceptación de comunicaciones privadas. Únicamente Costa Rica ha ratificado dicho convenio.

Datos personales:

cualquier información relativa a una persona identificada o identificable.

Persona defensora de derechos humanos:

el proceso de aplicar técnicas de codificación para convertir la representación original de la información en una forma alternativa de información llamada texto cifrado.

Se trata de una técnica de seguridad de la información que busca resguardar su confidencialidad y privacidad; también, que la información solo se pueda accesar por las personas que cuentan con la debida autorización.

Vigilancia:

el monitoreo realizado tanto por entes públicos como privados a las actividades o la información de las personas, usualmente argumentando razones de seguridad. La vigilancia puede ser legal o ilegal, dependiendo de si se cuenta con una orden judicial que la autorice y se cumplan ciertos principios como el de proporcionalidad, legalidad, idoneidad y necesidad.

Privacidad:

el derecho fundamental de toda persona de mantener ciertos aspectos de su vida libre de intromisiones externas y, por tanto, expresarse de forma privada.

Derechos ARCO

(acceso, rectificación, cancelación y oposición):

corresponden a las siglas de derechos que tiene las personas para ejercer control sobre su información personal, ya sea mediante su acceso, rectificación, solicitud de cancelación o eliminación, u oposición al uso de los datos personales en bases de datos físicas o en formato digital.

Cifrado o criptografía:

el proceso de aplicar técnicas de codificación para convertir la representación original de la información en una forma alternativa de información llamada texto cifrado.
Se trata de una técnica de seguridad de la información que busca resguardar su confidencialidad y privacidad; también, que la información solo se pueda accesar por las personas que cuentan con la debida autorización.

Auto-determinación informativa:

es el poder de control que tienen las personas respecto de sus datos personales, en particular, su uso y destino, con el propósito de impedir su tráfico ilícito y dañino para la dignidad y derechos de la persona afectada. En algunas legislaciones es considerada un derecho fundamental vinculado a la protección de datos personales, mientras que en otras es considerada un derecho derivado de la privacidad.

Guatemala

Resumen de la situación a escala país

Guatemala cuenta con un reconocimiento parcial de la autodeterminación informativa; este término significa que las personas ciudadanas tienen el poder de controlar como son tratados sus datos personales cuando se cede su tratamiento. Este derecho solo está resguardado respecto de la información en manos de organismos públicos. El anonimato está amenazado por leyes que obligan a los usuarios a entregar su identidad al momento de adquirir planes telefónicos y no existen leyes que promuevan el uso del cifrado o de protección. Si bien existe legislación (insuficiente) que regula las actividades de vigilancia, han sido evidentes distintos casos de compra de herramientas de espionaje informático, utilizado para espiar a los oponentes políticos.

Nivel normativo de los tratados de derechos humanos

Guatemala ha confirmado varios tratados internacionales en materia de derechos humanos que —de acuerdo al artículo 46 de la Constitución Política de Guatemala— tienen preferencia respecto al contenido del derecho interno. Del mismo modo, el artículo 149 también establece que Guatemala normará sus relaciones con otros Estados de acuerdo con los principios y prácticas internacionales.

Privacidad y protección de datos personales

Guatemala no tiene una ley especial para la protección de datos personales, pero existe protección a la privacidad y a la protección de datos en algunas leyes especiales, como tratados internacionales ratificados, y, principalmente, en el texto de la Constitución Política de Guatemala, que protege el derecho a la intimidad y a la privacidad como un derecho fundamental de su ciudadanía.

La Corte de Constitucionalidad ha interpretado que el derecho a la intimidad y la privacidad se encuentran relacionados con los artículos 23, 24 y 25 de la Constitución, respectivamente, los que hacen referencia a la inviolabilidad de la vivienda, la correspondencia, los documentos y los libros, así como respecto del registro de personas y vehículos[1].

Con base en el artículo 31 de la Constitución, el reconocimiento al derecho a la protección de datos personales y a los derechos ARCO se da únicamente respecto de aquellos datos personales contenidos en archivos, documentos o registros estatales o públicos. En otras palabras, el derecho a la autodeterminación informativa en Guatemala está garantizado únicamente, respecto del ámbito público.

[1] La Sentencia de la Corte de Constitucionalidad dictada dentro del expediente N° 1356-2006 el 11 de octubre de 2006 se transformó en la primera sentencia en que la Corte tuteló jurisdiccionalmente el derecho a la protección de datos, incluso utilizando el término derecho a la autodeterminación informativa.

A pesar de lo anterior, existe doctrina legal que ha reconocido la obligación de obtener el consentimiento de la persona titular para el tratamiento de sus datos personales (De Mata, 2020), así como un fallo de la Corte Constitucional que establece que mientras persista el vacío legal respecto a organismos privados se deberá obtener el consentimiento de la persona interesada para procesar sus datos y utilizarlos con un propósito compatible con aquello para lo que se obtuvieron[2].

El *habeas data* es una garantía legal que se encuentra regulado en los artículos 30 al 35 de la Constitución Política de Guatemala; al ejercer este mecanismo legal la ciudadanía puede conocer, acceder y controlar la información, en general, y los datos personales contenidos en registros públicos y en manos de autoridades u otros sujetos obligados de acuerdo con la Ley de Acceso a la Información Pública, así como también para ejercer los derechos ARCO. Algunas normativas sectoriales pueden ofrecer ciertas protecciones limitadas (Contraloría General de Cuentas, 2002). En 2018, el congresista Ronald Arango presentó un recurso de amparo (habeas data) contra Infornet por la comercialización de datos personales de la población, alegando que esta práctica va en contra de la prohibición de la Corte Constitucional al respecto (Gordillo, 2020).

Guatemala podría estar cerca de aprobar una ley especial en materia de protección de datos personales. En el Congreso se han presentado dos iniciativas de leyes (Congreso de la República, 2021), en 2021 y, recientemente, en 2024 las que vendrían a regular el tratamiento de

[2] Sentencia de la Corte de Constitucionalidad dictada dentro del expediente N° 1356-2006 el 11 de octubre de 2006.

los datos en el sector público y privado, así como los principios, conceptos y obligaciones de quienes procesen o resguarden datos personales en bases de datos.

No existe ninguna norma de rango legal o constitucional que promueva la utilización del cifrado o el anonimato en Guatemala. Por el contrario, la Ley de Equipos Terminales Móviles de 2013[3] obliga a los usuarios que quieran adquirir una tarjeta SIM a "proporcionar al vendedor una copia física o electrónica de su documento legal de identificación personal" (artículo 3), lo que implica una importante amenaza al derecho de comunicarse de forma anónima, especialmente, para personas defensoras de derechos humanos y periodistas de investigación. Esta misma ley, en su artículo 9 también prohíbe a las empresas de telecomunicaciones "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." Respecto del cifrado, la normativa sobre firma y comunicaciones electrónicas, sí se establece la criptografía asimétrica, que es un sistema de seguridad que cuenta con dos claves, una privada y otra pública, como uno de los mecanismos que los certificadores de firma electrónica avanzada podrán implementar para asegurar la confidencialidad de estas transacciones, aunque no lo establece como obligatorio[4].

[3] Decreto 08-2013 del 2 de octubre de 2013.
[4] Artículo 46 del Decreto 47-2008

A pesar de no contar con una ley especial en Guatemala, existen las siguientes leyes secundarias que hacen referencia a la protección de los datos personales o privacidad:

El Código Penal de Guatemala

define acciones sobre las cuales se les asigna una pena respecto de ciertos delitos relacionados con la violación de la privacidad y la protección de datos. Entre ellos se incluyen la divulgación indebida de datos, la usurpación de identidad, el acceso no autorizado a sistemas informáticos y —bajo ciertas circunstancias— el delito de pánico financiero (quien divulgue información falsa que desprestigie una institución financiera).

El Decreto 39-2022, Ley de Prevención y Protección Contra la Ciberdelincuencia

tiene como objetivo sancionar y regular la prevención de la ciberdelincuencia que es un delito contra la seguridad de empresas o personas a través de tecnologías digitales; además, la ley también tiene como objetivo definir las conductas delictivas, mejorar la protección de los datos personales; también, establece normas para la incorporación de medios de pruebas digitales que es la información digital para acreditar los hechos en un proceso judicial.

La Ley de Acceso a la Información Pública de Guatemala. Decreto 57-2008[5]

establece parámetros generales para el manejo de los datos personales en registros públicos o estatales y, por parte de entidades públicas, dejando por fuera la protección de datos personales en manos de entes privados. Dicha ley también se ha utilizado para impedir la transparencia o la rendición de cuentas,

[5] https://transparencia.gob.gt/wp-content/uploads/2019/03/Decreto-57-2008.....pdf

así como para no entregar información pública referente al uso o transferencia de datos biométricos de personas migrantes, es decir, que reconozcan sus características físicas a través de un escáner (Access Now, 2023).

La Ley General de Telecomunicaciones de Guatemala[6]

no cuenta con un capítulo específico que regule la protección de datos, pero, como norma secundaria, se rige por los principios constitucionales y por lo establecido en otras normas secundarias como la Ley de Acceso a Información Pública, normas penales y otras aplicables. Algunos aspectos relevantes son:

- Se consideran confidenciales los datos que consten en archivos estatales, por ejemplo, los registros de personas usuarias de servicios de telecomunicaciones; únicamente, pueden ser revelados con el consentimiento informado de la persona titular de los datos o por medio de orden judicial.
- Las empresas de telecomunicaciones y toda entidad privada deben respetar los principios de licitud, finalidad, proporcionalidad, calidad, seguridad y responsabilidad; además, deben obtener el consentimiento previo, expreso e informado de la persona titular para la recolecta, almacenamiento o procesamiento de datos personales.
- Para la interceptación, grabación o difusión de datos personales transmitidos por medios electrónicos, como el correo electrónico, redes sociales, o las aplicaciones móviles, únicamente, puede realizarse por medio de la obtención del consentimiento o por orden judicial como una garantía de protección al derecho de intimidad y honor.
- Se reconocen los derechos ARCO respecto del procesamiento de datos personales de las personas titulares; de la misma manera, se le reconoce el derecho a la protección de sus datos y a conocer si son procesados de manera automatizada o manual en bases de datos de instituciones públicas o privadas.

[6] https://sit.gob.gt/gerencia-juridica/leyes-y-reglamentos/

- Se establece que las personas responsables del tratamiento de los datos personales deben adoptar medidas técnicas, administrativas y jurídicas necesarias para garantizar la seguridad, integridad y confidencialidad de los datos, como una manera de prevenir la alteración, pérdida, acceso o uso no autorizado de los datos personales.
- Se establecen sanciones, penas de prisión o inhabilitaciones a quienes causen algún daño o incurran en faltas a la protección de datos personales respecto de las obligaciones establecidas por la normativa en materia de telecomunicaciones.

La intervención de las comunicaciones es posible ejecutarla aplicando la Ley contra la Delincuencia Organizada, Decreto 21-2002, que reforma al Código Procesal Penal y que establece los requisitos y procedimientos para que el Ministerio Público pueda solicitar al juez o la jueza competente la autorización para interceptar, grabar, registrar o divulgar las comunicaciones que se realicen por cualquier medio, cuando existan indicios racionales de la comisión de un delito grave que afecte la seguridad del Estado, la paz pública, la vida, la libertad o la integridad de las personas.

La ley tiene como objetivo prevenir y sancionar los delitos cometidos por grupos del crimen organizado, así como fortalecer la cooperación judicial y policial entre autoridades nacionales e internacionales, facilitar la persecución y enjuiciamiento de este tipo de delincuentes. La solicitud de intervención debe estar

debidamente fundada y motivada por parte del Ministerio Público, puede solicitarse ante la comisión de delitos públicos graves que puedan afectar al Estado o la ciudadanía en general.

La intervención debe ser proporcional, temporal y limitada, respetando la intimidad y el secreto de las comunicaciones, tal como lo establece el artículo 24 de la Constitución. Por otro lado, la Ley de Control y Prevención del Lavado de Dinero utiliza un lenguaje particularmente amplio, al autorizar el uso de cualquier medio tecnológico disponible para la investigación de cualquier delito para facilitar su esclarecimiento (Electronic Frontier Foundation, 2021).

Vigilancia tecnológica

En los últimos años ha habido varias denuncias sobre la compra estatal y uso de tecnología para atacar, vigilar y rastrear de manera ilegal a la ciudadanía por medio del uso de programas de espionaje, interceptación ilegal de comunicaciones, ataques a correos electrónicos, redes sociales, hostigamiento y criminalización hacia personas defensoras de derechos humanos y periodistas.

En 2013, una investigación del Citizen Lab de Toronto mostró que Guatemala se encontraba entre los 83 países que habían adquirido y ejecutado los dispositivos denominados PacketShaper y ProxySG de la empresa Blue Coat Systems, los que pueden ser utilizados para activar restricciones por motivos políticos al acceso a la información, así como monitorear y registrar comunicaciones privadas (Marquis-Boire, 2013).

De modo similar, en julio de 2017, la Dirección General de Inteligencia Civil del Ministerio de Gobernación —a través de una adjudicación directa— compró el programa Magnet Axiom a la empresa ITD (Guatecompras 2017). Dicho programa cumple la función de herramienta forense para realizar exfiltración de datos, como robar información, analizar la actividad de una red y, en particular, permitir la recuperación de información borrada de distintos dispositivos.

Más grave aún es que durante 2018 la publicación Nuestro Diario (Sas y Orantes, 2018) (Díaz, 2018), reveló que en Guatemala podrían existir prácticas autoritarias de espionaje ilegal al adquirir "las versiones más avanzadas de Pen-Link, Conceptus, Circles, Citer 360, Avatar, Pegasus, Laguna, entre otros". La compra de tecnología para la vigilancia autoritaria representaría un retroceso en la garantía con respeto a los derechos humanos en Guatemala desde la firma de los acuerdos de paz en 1996.

Uno de los casos más destacados, en cuanto a hechos ilícitos de vigilancia, es el denominado caso Tigo en el que la Comisión Internacional Contra la Impunidad en Guatemala (CICIG), entregó los resultados de diferentes casos investigados, entre ellos de uno nombrado como "Tigo". En este caso se vincula al ministro de Economía de la época y al exgerente de la empresa Tigo, Acisclo Valladares Urruela, de dirigir un sistema de espionaje a personas opositoras políticas, personas empresarias y a su propia exesposa (Oliva, 2021). De acuerdo con la denuncia realizada (CIGIC, 2019), se concluyó que del resultado del allanamiento efectuado en el inmueble donde residía el señor Valladares, existían indicios relevantes y significativos que permiten inferir la práctica de seguimientos, escuchas e intervenciones de teléfonos celulares sin la debida orden judicial, por parte del funcionario de la empresa telefónica Tigo, cuyos resultados eran reportados al señor Valladares.

Honduras

Resumen de la situación a escala país

Honduras no cuenta con una ley específica de protección de datos personales que proteja la autodeterminación informativa de su ciudadanía y solo cuenta con un procedimiento parcial de habeas data establecido de forma reglamentaria. No existen normas que promuevan o limiten el anonimato y el cifrado.

En materia de vigilancia, la existencia de una Unidad de Intervención de las Comunicaciones, que no cuenta con los controles y contrapesos habituales en un estado de derecho, implica una falta de protección en las garantías constitucionales de la ciudadanía.

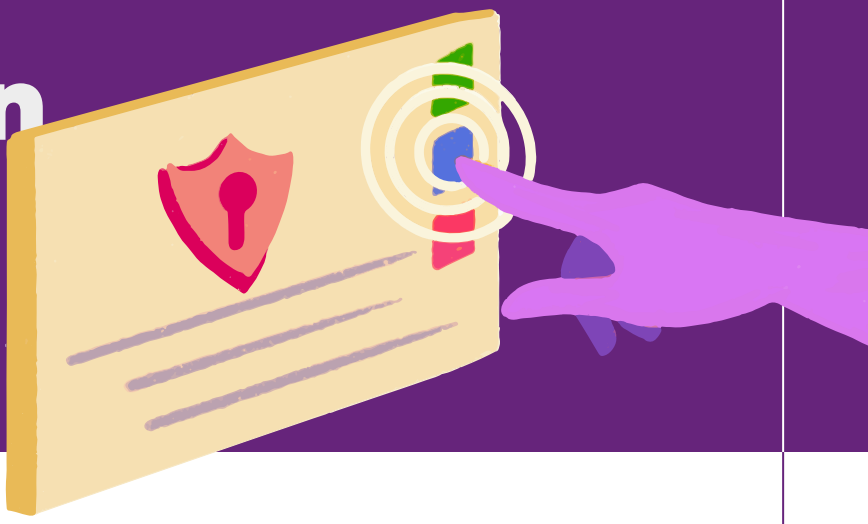
Nivel normativo de los tratados de derechos humanos

Honduras ha ratificado los principales tratados internacionales en materia de derechos humanos; además, cuenta con una serie de normas respecto a la protección de la privacidad digital, entre las que se destaca La Ley de Intervención de las Comunicaciones aprobada por el Congreso Nacional el 8 de diciembre de 2011[7]. Esta disposición establece un marco legal de regulación procedimental o de procedimientos de la intervención de las comunicaciones, el que dejó sin efecto las normas del Código Procesal Penal en la materia. No obstante, el derecho a la privacidad relacionado con la privacidad digital, la vigilancia y la vulneración de derechos digitales han sido escasamente tratados en el país.

En cuanto a la fuerza normativa de los tratados internacionales de derechos humanos en el sistema jurídico hondureño, el artículo 16 de la Constitución de Honduras establece que "los tratados internacionales celebrados por Honduras con otros estados, una vez que entran en vigor, forman parte del derecho interno".

[7] https://www.tsc.gob.hn/biblioteca/index.php/leyes/127-ley-especial-sobre-intervencion-de-las-comunicaciones-privadas

Privacidad y protección de datos personales



La Constitución Política de la República de Honduras de 1981 en el artículo 57 garantiza el derecho a la intimidad personal, familiar y a la propia imagen. Así, el derecho a la privacidad, cualquiera que sea su esfera, se le denomina “derecho a la intimidad”, tanto en las normas como en la jurisprudencia, entendida como el conjunto de sentencias judiciales de las que se extrae una norma que influya en la decisión de casos futuros. La Sala de lo Penal de la Corte Suprema de Justicia Hondureña complementa el contenido del derecho estableciendo algunas de las esferas de la privacidad que merecen protección, como el derecho a la intimidad digital, la autodeterminación informativa y la inviolabilidad o protección de domicilio, incluyendo la inviolabilidad de las comunicaciones privadas.

No existe ninguna norma legal o constitucional que regule la promoción ni las limitaciones al cifrado o al anonimato. Una mención al cifrado puede encontrarse en el acuerdo SO-098-2019 del Instituto de Acceso a la Información Pública[8] donde se establecen los lineamientos aplicables a la gestión documental ejecutada por las instituciones obligadas por la Ley de

[8] https://www.tsc.gob.hn/web/leyes/Acuerdo-SO-098-2019.pdf

Transparencia y Acceso a la Información Pública. En dicho documento se define “criptografía” y se señala como aquellas medidas que pueden ser utilizadas para resguardar el Patrimonio Documental de la Nación.

El artículo 99 de la Constitución de la República elabora algunas maneras de limitar el derecho a la inviolabilidad del domicilio: a) el consentimiento de la persona que lo habita; b) por “resolución de autoridad competente, y c) sin consentimiento, ni resolución de autoridad competente en caso de urgencia, para impedir la comisión o impunidad de delitos o evitar daños graves a la persona o a la propiedad. A reglón seguido, el artículo 100 de la Constitución de la República establece como requisito para la limitación del derecho a la inviolabilidad y al secreto de las comunicaciones que se haga mediante resolución judicial.

Honduras cuenta con una Unidad de Intervención de las Comunicaciones, órgano de la Dirección Nacional de Investigación e Inteligencia (como ente encargado de ejecutar las políticas públicas en materia de defensa y seguridad) y, esta a su vez, es la plataforma de la operatividad del Consejo Nacional de Defensa y Seguridad, el que está conformado por el presidente de la República que lo preside, el presidente del Congreso Nacional, el presidente de la Corte Suprema de Justicia, el fiscal general, el secretario de Estado en el Despacho de Seguridad y el secretario de Estado en el Despacho de Defensa Nacional, y c (Argueta, 2020).

Existen tres mecanismos de acceso a la justicia en el contexto de la vigilancia por violación a derechos fundamentales desarrollados anteriormente. Estos son: 1) el recurso de amparo contenido en el artículo 183 de la Constitución, 2) el

recurso de habeas data: la finalidad de la acción es que la información se pueda actualizar, rectificar y/o suprimir, el que conoce y resuelve la Sala de lo Constitucional de la Corte Suprema de Justicia, después de agotarse el procedimiento administrativo ante el Instituto de Acceso a la Información Pública, y 3) el recurso de inconstitucionalidad contenido en el artículo 184 de la Constitución de la República. Este recurso puede ser interpuesto por quien se considere lesionado en su interés directo, personal y legítimo, a fin de que se declare la nulidad total o parcial de una ley vigente nacional.

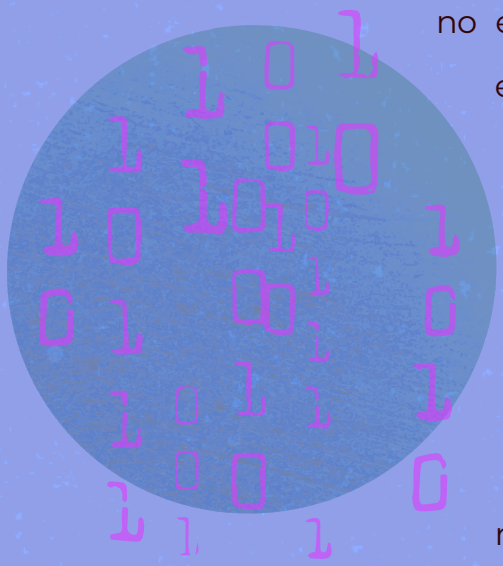
La misma Sala de lo Constitucional de la Corte Suprema es la responsable de su conocimiento y fallo.

Al igual que Guatemala y El Salvador, en Honduras las normas relativas a la reserva de la información y la confidencialidad se han utilizado para impedir la transparencia o la rendición de cuentas, así como para no entregar información pública referente al uso o transferencia de datos biométricos de personas migrantes (Access Now, 2023).

Actualmente, Honduras no cuenta con una legislación que regule, específicamente, la protección de los datos personales de titulares; sin embargo, existe otra legislación que regula algunos aspectos en la materia:

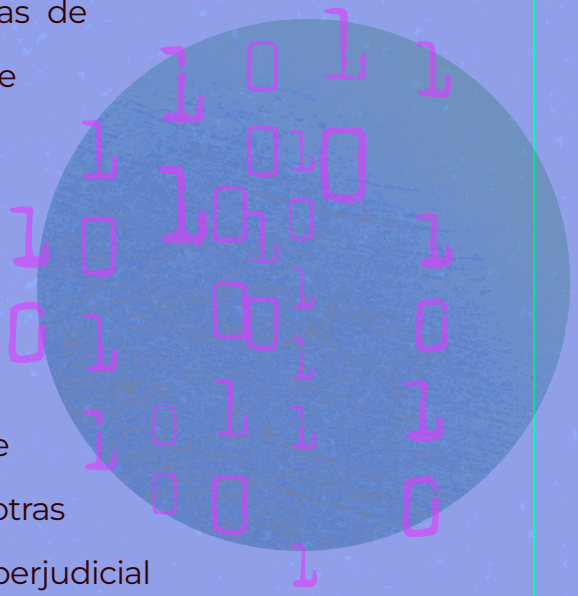
La Ley del Instituto de Acceso a la Información Pública y su reglamento establecen una sucinta regulación en la materia. Así, el artículo 23 de dicha ley consagra la existencia de un procedimiento de habeas data, a través el cual el titular puede reclamar, por sí o a través del Comisionado Nacional de Derechos Humanos el

tratamiento indebido de sus datos personales ante la Sala de lo Constitucional de la Corte Suprema de Justicia. El artículo 24 señala sucintamente que "los datos personales serán protegidos siempre" y que el acceso a los datos personales procederá únicamente por decreto judicial o a petición de la persona cuyos datos personales se contienen en dicha información. Por último, el artículo 25 establece que ninguna persona podrá obligar a otra a proporcionar datos personales que puedan originar discriminación, causar daños, riesgos patrimoniales o morales de las personas. Lamentablemente, se trata de una legislación extremadamente mínima y somera, que no reconoce efectivamente el derecho al acceso, rectificación, cancelación y oposición de las personas titulares de datos personales, no establece los principios rectores de la legislación, no establece categorías especiales de datos o regula cuáles son las bases legales para el tratamiento de datos personales ni la forma y casos en que pueden ser recolectados, almacenados y procesados por terceros. Del mismo modo, no establece cuáles son las herramientas con las que cuentan las personas titulares en caso de infracción de sus derechos ni un régimen de sanciones ante dicho incumplimiento.



A empresas proveedoras de telecomunicaciones se les ha impuesto la obligación legal de colaboración con las autoridades de la Unidad de Intervención de las Comunicaciones y la Comisión Nacional de Telecomunicaciones en las actividades de vigilancia, a través del registro de clientes, colaborando en la interceptación de las comunicaciones y con la retención de datos de conexión por un plazo de cinco años.

Adicionalmente, la Ley de Intervención de las Comunicaciones contiene un capítulo completo dedicado a las obligaciones de las personas naturales y jurídicas que prestan servicios de comunicación (capítulo VI) y cuyo incumplimiento conlleva sanciones económicas costosas, con multas de 5000 a 10 000 salarios mínimos, hasta la cancelación de la licencia.



Del mismo modo, se encuentra en las últimas etapas de tramitación la llamada "Ley SIM"[9] que establece la obligación del registro de clientes de telecomunicaciones, así como registro y entrega de otras formas de telecomunicación, lo que puede resultar perjudicial para las personas defensoras de derechos humanos y para el ejercicio del derecho de comunicarse de forma anónima, es decir, esta "Ley SIM" puede implicar la identificación de todas aquellas personas que se comuniquen a través de dispositivos móviles; además, existe el temor de que sea utilizada en contra de personas opositoras políticas al gobierno de turno (Ortez, 2023).

[9] El artículo 23 de esta propuesta establece que "Los registros técnicos referidos en este apartado son: registros de llamadas telefónicas, videollamadas, mensajes de voz, mensajes de texto cursados en terminal o cursados vía internet, registros de ocupación de direcciones IP, así como otros tipos de registros de servicios de telecomunicaciones que a futuro se implementen".

En junio de 2020 entró en vigencia el nuevo Código Penal de Honduras, estos son algunos aspectos relevantes:

- **En los delitos de injurias y calumnias, se verá agravada la pena en aquellas declaraciones realizadas "utilizando sitios web de divulgación colectiva o redes sociales a través de internet". Esto incumple el principio de proporcionalidad, puesto que establece un agravante solo por el medio utilizado para expresarla.**
- **Establece penas de cárcel para quien intercepte telecomunicaciones sin consentimiento de la persona titular.**
- **Sanciona con multas a las empresas proveedoras de servicios de telecomunicaciones por la falta u omisión de registro o identificación de clientes.**

La publicación de un nuevo Código Penal en 2019 incluye la tipificación de una serie de delitos informáticos. Entre ellos se incluye el delito de acceso no autorizado (artículo 398), el delito de daños a datos y sistemas informáticos (artículo 399). La redacción de la mayoría de estos delitos sigue de cerca la redacción establecida en el Convenio de Budapest; sin embargo, la legislación no incluye una excepción en favor de personas investigadoras de seguridad informática o docentes en esta materia, quienes muchas veces prueban la seguridad de los sistemas con el fin de reportar vulnerabilidades

informáticas o como forma de enseñar a su estudiantado la forma correcta de detectarlos. El delito de acceso no autorizado solo exige que se ingrese sin permiso al sistema informático, lo que podría implicar que, eventualmente, se criminalice la actividad legítima de investigación y docencia en materias relacionadas con la seguridad informática (Rodríguez, et al., 2018).

La ley sobre Intervención de las Comunicaciones, vigente desde 2011, establece el marco legal de regulación procedimental de la intervención de las comunicaciones. En su artículo 5 establece cinco principios para la intervención de las comunicaciones: proporcionalidad, necesidad e idoneidad, confidencialidad, reserva judicial y temporalidad. De igual forma, permite intervenir comunicaciones entre personas presentes, entre llamadas telefónicas, correos electrónicos y, finalmente, en su artículo 40 establece "sobre cualquier otra información", dejando la puerta abierta a otros medios de comunicación no contemplados en la ley, como las redes sociales. La manera como regula los requisitos y las formas para efectuar la intervención de comunicaciones privadas es vaga y con poca precisión respecto de qué se entiende como espacio público, o qué se entiende por "mera sospecha de comisión de delito" que habilitan el registro de domicilios, generan debate respecto de la posibilidad de la comisión de arbitrariedades o medidas desproporcionadas que lesionen los derechos de la población. Del mismo modo, han existido reportes de una utilización indebida de escuchas telefónicas sin una orden judicial (Proceso digital, 2015).

Honduras se adhirió en 2006 a la Convención Interamericana sobre Asistencia Mutua en Materia Penal (MLAT, por su sigla en inglés); además, cuenta con tratados de asistencia judicial con todos los países centroamericanos, México y Brasil. Este convenio permite al país extender la persecución penal fuera de sus fronteras, incluyendo los delitos mencionados en este apartado.

Vigilancia tecnológica

En la aplicación de normas sobre vigilancia, principalmente a propósito de la persecución penal del crimen organizado, aparecen situaciones de vulneración a personas defensoras de derechos humanos, sobre todo a partir del golpe de estado de 2009.

En 2013 se creó un nuevo Sistema Nacional de Inteligencia, coordinado por la Dirección Nacional de Investigación e Inteligencia, que cuenta con un Consejo Nacional de Defensa y Seguridad con sus propios agentes de inteligencia y vigilancia. Del mismo modo, este cuerpo legal entrega importantes atribuciones invasivas a las agencias de inteligencia, sin control respecto de su funcionamiento, ya sea de carácter jurisdiccional (por parte del Poder Judicial) o control de carácter democrático (por parte del Poder Legislativo).

Tanto la Ley de Intervención de las Comunicaciones como el resto de legislación hondureña carecen en absoluto de disposiciones normativas legales que obliguen a las entidades, que llevan a cabo estas actividades, a informar periódicamente del número, tipo y ámbito de las que llevan a cabo. Podrían aplicarse las normas generales de la ley de Transparencia y Acceso a la Información Pública, sin embargo, los datos que se generan en la Unidad de Intervención de las Comunicaciones tienen la categoría de “información de Inteligencia” y, por consiguiente, gozan de carácter reservado. Respecto a la supervisión pública, no existe un órgano

de supervisión independiente ni tampoco mecanismos internos de revisión.

La vigilancia en internet y en las telecomunicaciones en Honduras forma parte de una política en materia de seguridad pública que fueron agrupados temas relativos a seguridad, defensa e inteligencia. Se ha implementado bajo el supuesto de que, para lograr una sociedad segura, es necesario crear las herramientas jurídicas e institucionales para el combate a la violencia y la delincuencia organizada y, quien no está a favor de las medidas restrictivas, está a favor de la "delincuencia"; en otras palabras, se plantea una falsa disyuntiva entre libertades fundamentales y seguridad.

Un ejemplo de adquisición de tecnología de vigilancia intrusiva, que afecta los derechos a una persona investigada, referencia a la plataforma WkeLeaks Honduras, consultada en 2028, *https://1.bp.blogspot.com/-5lFP4WcVyeo/VZ8nk7UJ65I/AAAAAAAAAYA/W53jSz69bCs/s1600/pachecompra.jpg* se dio en 2015, año en el que Honduras compró a la empresa italiana Hacking Team un softreferencia a la plataforma WkeLeaks Honduras, consultada en 2028, *https://1.bp.blogspot.com/-5lFP4WcVyeo/VZ8nk7UJ65I/AAAAAAAAAYA/W53jSz69bCs/s1600/pachecompra.jpg* ware espía por un total de 355 000 euros.

Este sistema de espionaje conocido como "Galileo" tiene la capacidad de descifrar archivos, correos cifrados, grabar llamadas, entre otras comunicaciones (WekeLeaks, 2018). Dicho de otra manera, se trata de un programa destinado a ser utilizado a través de una infección de malware, que es un programa malintencionado, cuyo nivel de intrusión es difícil de justificar bajo el marco normativo hondureño.

El Salvador

Resumen de la situación a escala país

El Salvador no cuenta con una ley de protección de datos personales y algunas de las iniciativas para legislar en esta materia han sido censuradas por el actual presidente Nayib Bukele, sin embargo, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición han sido reconocidos por la jurisprudencia. Tampoco existen normas que promuevan o limiten el anonimato y el cifrado. En materia de vigilancia tecnológica se ha podido constatar la compra de programas de vigilancia, así como la utilización de malware para espiar a activistas y periodistas.

Nivel normativo de los tratados de derechos humanos

El Salvador ha ratificado tratados internacionales en materia de derechos humanos que tienen fuerza vinculante, es decir con obligación de cumplirlos si no se aplica una sanción; además, tienen la misma fuerza legal que las normas secundarias vigentes en el ámbito interno de acuerdo con el tratado confirmado por el país los que tienen una fuerza vinculante en las relaciones entre Estados y el ámbito interno.

Según el artículo 144 de la Constitución de la República los tratados internacionales celebrados por El Salvador con otros estados o con organismos internacionales, constituyen leyes de la República al entrar en vigor, conforme a las disposiciones del mismo tratado y de la Constitución. Al gozar de la misma fuerza legal, una ley no puede modificar o derogar el contenido de lo acordado por un tratado internacional.

Privacidad y protección de datos personales

El derecho a la privacidad esta regulado en el artículo 2 de la Constitución salvadoreña de 1983; se garantiza el derecho al honor a la intimidad personal y familiar y a la propia imagen. El mismo artículo es la base sobre la que se ha interpretado, vía jurisprudencial, el derecho a la autodeterminación informativa.

El Salvador no cuenta con una ley de protección de datos personales ni tampoco considera alguna norma constitucional que regule la promoción ni las limitaciones al cifrado o al anonimato. En la Asamblea Legislativa se han discutido varias iniciativas de ley relacionadas que regularían, en el sector privado, el tratamiento de los datos personales. Un ejemplo fue el Decreto Legislativo 875, presentado el 28 de abril de 2021 por la Asamblea Legislativa, que buscaba proteger los datos personales en el ámbito público y privado. Sin embargo, fue vetado en mayo del mismo año por el presidente Bukele, por considerarlo inadecuado para el marco legal salvadoreño, con el argumento adicional de falta de presupuesto y experiencia técnica de la institución a cargo de su aplicación (Rodríguez M., 2021).

Los derechos de privacidad y protección de datos personales se pueden defender a través de tres mecanismos: el primero es el amparo constitucional que es un mecanismo contra la restricción, omisión o amenaza contra los derechos constitucionales; el segundo, es el recurso de inconstitucionalidad que

es un control de compatibilidad con la Constitución y; tercero, el proceso de amparo que es una protección de los derechos constitucionales de la ciudadanía. No existe propiamente la figura del habeas data.

Mediante procesos de amparo el derecho a la autodeterminación informativa y derechos ARCO han sido reconocidos, vía jurisprudencia de la Sala de lo Constitucional de la Corte Suprema de Justicia de El Salvador; específicamente, en las sentencias de los amparos 934-2007 y 142-2012 de la Sala de lo Constitucional de la Corte Suprema de Justicia. En dichas sentencias se reconocieron los principios relacionados con el derecho a la autodeterminación informativa y se interpretó que ese derecho se deriva de la garantía de seguridad, contenida en el artículo 2 de la Constitución de 1983.

Además, se interpretó que el derecho debe asegurarse y entenderse desde dos facetas: una primera, material y preventiva relacionada con la libertad y la autonomía del individuo; la segunda, instrumental que hace referencia a las acciones encaminadas a la protección, control y reparación de los datos personales contenida en bancos de datos o ficheros.

Dichos procesos de amparo representan también dos casos emblemáticos en la materia; las solicitudes de amparo fueron interpuestos por el presidente y representante legal de la Asociación Salvadoreña para la Protección de Datos e Internet (Indata) en contra de las empresas Dicom Centroamérica y General Automotriz y, en un segundo proceso, contra Infornet (Adesa, 2011). En ambos procesos se aludía a que, en sus operaciones, las empresas violaban el derecho constitucional a la autodeterminación informativa.

En el caso contra Dicom se alegó la falta de actualización en los registros y

bases de datos personales y, en el caso contra Infornet, se señaló que recopilaba y comercializaba, de forma ilegítima, información personal, crediticia, judicial, mercantil y de prensa sin consentimiento de las personas titulares. Ambos amparos fueron favorables para Indata, lo que confirmó la interpretación de la Constitución de que el derecho a la autodeterminación informativa es uno de los reflejos del derecho a la seguridad y que, por lo tanto, los datos informáticos deben ser protegidos y el acceso a la información personal limitado a lo estrictamente permitido por cada titular.

A pesar de no contar con leyes específicas respecto a la protección de datos, sí existen algunas leyes secundarias que hacen referencia a la protección de los datos personales o privacidad, entre ellas:

La Ley de Acceso a la información Pública de El Salvador contiene un breve capítulo relativo a la protección de datos personales en bases de datos, archivos físicos o documentos en posesión de entidades públicas sujetas a la ley, dejando sin regulación el manejo de datos personales por sujetos privados. Las normas relativas a la reserva de la información y la confidencialidad se han utilizado para impedir la transparencia o la rendición de cuentas, así como para no entregar información pública referente al uso o transferencia de datos biométricos de personas migrantes (Access Now, 2023).

El Código Penal de 1997 y el código procesal penal regulan lo relativo al allanamiento, requisa, posesión ilegal de comunicaciones escritas, documentos confidenciales o personales, calumnia, difamación, entre otros delitos que pueden aplicar en el ámbito virtual como presencial. Al igual que Honduras, El Salvador se ha adherido a la Convención Interamericana sobre Asistencia Mutua en Materia Penal.

Ley de telecomunicaciones, regula en el artículo 29 “b” el derecho al secreto de las comunicaciones y a la confidencialidad de los datos personales no públicos, teniendo en cuenta lo mencionado en el título v-bis, capítulo único de la ley (referente a la colaboración con las autoridades para compartir información o bases de datos con autoridades e instituciones del sistema de justicia para investigar hechos punibles). Los proveedores de servicios de telecomunicación tienen la obligación legal de llevar un registro de clientes con sus documentos de identificación en relación con su respectivo número telefónico o tarjeta SIM.

Ley de protección al consumidor. El artículo 18 “f” y “g” prohíbe la difusión o publicación de datos personales o información confidencial y crediticia: f) realizar gestiones de cobro difamatorias o injuriantes en perjuicio del deudor, codeudor, fiador o sus familiares; utilizar medidas de coacción física o morales para tales efectos; así como publicar por cualquier medio de comunicación nombres, datos personales o fotografías de personas naturales o jurídicas por incumplimiento de sus obligaciones crediticias. Esta prohibición también es aplicable a las personas naturales o jurídicas que se dediquen a gestiones de cobro; g) compartir información personal y crediticia del consumidor, ya sea entre proveedores o a través de entidades especializadas en la prestación de servicios de información, sin la debida autorización del consumidor.

La Ley de Delitos Informáticos de El Salvador tipifica la utilización de datos personales sin autorización y a través de las TIC (Tecnologías de Información y Comunicaciones) en el artículo 24; así como la revelación indebida de datos o de información confidencial en el artículo 26. La ley, sin embargo, en sus conceptos, posee lenguaje amplio e impreciso.

La Ley Especial para la Intervención de las Telecomunicaciones, Decreto 285, tiene como objetivo fortalecer los procedimientos y mecanismos para la persecución y combate de la criminalidad, obtención, ofrecimiento y producción de prueba en un proceso judicial; de esta manera, la intervención de las comunicaciones se convierte en una excepción que la ley permite ante la comisión de delitos graves que afecten la seguridad, la paz, la vida, la libertad o la integridad de las personas; debe estar autorizada por un juez o una jueza competente, solicitada previamente y de manera fundada y motivada por parte de la fiscalía general. Tanto la ley de intervención de las comunicaciones como las recientes reformas al código penal y procesal penal, el Estado ha regulado de manera vaga y con un alcance bastante amplio el uso de agentes digitales encubiertos (Pisanu, 2022) y ha adoptado medidas para patrullar las redes sociales como parte de las técnicas de investigación de delitos.

Vigilancia tecnológica

La falta de regulación respecto a temas de privacidad y protección de datos toman especial relevancia en el contexto actual de El Salvador, pues existe una suspensión de los derechos constitucionales y garantías procesales que inició en marzo de 2022, situación que se ha prolongado por más de dos años consecutivos, bajo el argumento de velar por la seguridad pública y para el combate de las maras (pandillas). Organizaciones salvadoreñas e internacionales defensoras de derechos humanos han emitido informes evidenciando los efectos derivados del régimen de excepción instaurado desde hace dos años (Cristosal, 2023), tales como "detenciones arbitrarias, desapariciones forzadas y muertes bajo custodia" (Human Rights Watch, 2022), abusos a los derechos humanos. Recientemente se aprobaron una serie de reformas legales en materia penal y procesal penal que, de acuerdo con la Relatoría Especial para la Libertad de Expresión, pueden representar riesgos de criminalización al ejercicio legítimo de la libertad de expresión, libertad de prensa y acceso a la información (OEA, 2022).

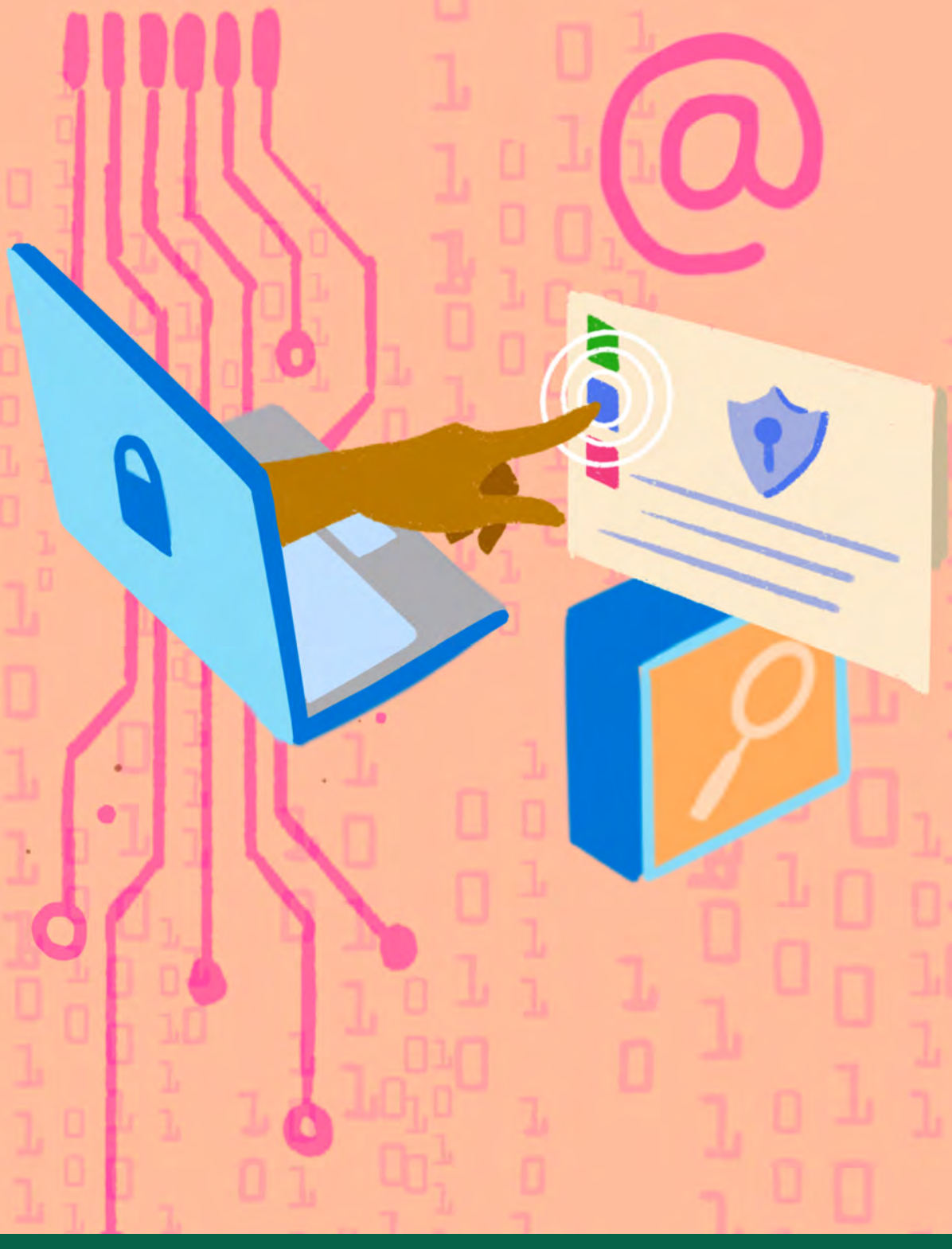
En enero de 2022 se dio a conocer mediante un informe de Citizen Lab, con la colaboración de varias organizaciones de derechos digitales y seguridad informática, acerca de la adquisición y uso del software de vigilancia Pegasus en contra de

periodistas, activistas y miembros de la sociedad civil en El Salvador (Scott-Railton, 2022). A lo anterior, se le suman varios reportes de agresiones a periodistas por parte de la Asociación de Periodistas de El Salvador (Apes) (Sandoval, 2024), hostigamiento por redes sociales, y constantes violaciones a derechos humanos; además, utilización de mecanismos de censura por parte del Gobierno salvadoreño.

El uso del software israelí Pegasus del grupo NSO dirigido a diferentes periodistas de distintos medios de comunicación y personas de la sociedad civil salvadoreña, es un claro ejemplo de la invasión a la privacidad y vigilancia ilegal. No existe información sobre el estado de las investigaciones por parte del Ministerio Público e incluso y, a pesar de que la Apes interpusiera dos avisos a la Fiscalía General de la República para que investigue el uso de software espía (Bernal, 2022), el Comisionado Presidencial para los Derechos Humanos, Andrés Guzmán Caballero, recientemente, negó que existieran ataques a la prensa en El Salvador (Infodemia, 2024).

A raíz de este caso, el Comisión Interamericana de Derechos Humanos (CIDH) llamó a una audiencia pública, llevada a cabo el 16 de marzo de 2023, donde citó a representantes del Estado salvadoreño con el fin de abordar las inquietudes y preguntas respecto a las pruebas presentadas por las organizaciones de la sociedad civil con relación al espionaje estatal. Los representantes de El Salvador negaron categóricamente cualquier ejercicio de "persecución, hostigamiento o estigmatización hacia personas o entidades críticas a la gestión del Gobierno" y que han sido activos en investigar lo sucedido. Es más, declaran que funcionarios de Gobierno también sufrieron vulneración de sus dispositivos. Además, también admitieron el uso de agentes encubiertos digitales, pero mencionaron que son para perseguir delitos contra menores (Gavarrete, 2022).

Nicaragua



Resumen de la situación a escala país

Nicaragua cuenta con una ley de protección de datos personales, así como un organismo a su cargo (Dirección de Protección de Datos Personales). El ordenamiento jurídico nicaragüense no aborda la promoción o limitación del cifrado y el anonimato, excepto en el ámbito del comercio electrónico. En materia de vigilancia tecnológica destaca la ausencia del principio de transparencia en la realización de interceptación de comunicaciones, así como el peligroso proyecto que el presidente Daniel Ortega busca aprobar para obligar a las empresas telefónicas a suministrar información de sus usuarios al ente regulador de telecomunicaciones.

Nivel normativo de los tratados de derechos humanos

La salvaguarda del derecho a la privacidad en Nicaragua se fundamenta en los tratados internacionales ratificados por el país, los que tienen fuerza vinculante en las relaciones entre estados y el ámbito interno. Según el artículo 138 de la Constitución, los instrumentos internacionales aprobados por la Asamblea Nacional adquieren efectos legales tanto dentro como fuera del país una vez que han entrado en vigor a escala internacional.

Privacidad y protección de datos personales

El artículo 26 de la Constitución Política de la República de Nicaragua dispone que toda persona tiene derecho:

1. **A su vida privada y a la de su familia.**
2. **Al respeto de su honra y reputación.**
3. **A conocer toda información que sobre ella se haya registrado en las entidades de naturaleza privada y pública, así como el derecho de saber por qué y con qué finalidad se tiene esa información.**
4. **A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo.**

El contenido normativo de este precepto constitucional aborda el derecho a la vida privada desde un punto de vista más amplio al tradicional, en el que las libertades públicas para crear un espacio libre de injerencias no solo aplican para las que provienen desde particulares.

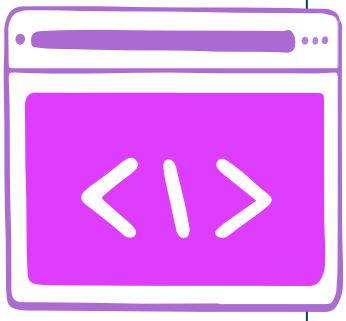
El artículo 26 de la Constitución de Nicaragua busca además proteger la privacidad y la inviolabilidad del domicilio, la correspondencia y las comunicaciones. Además, el artículo 34 garantiza el derecho al debido proceso, incluyendo no ser procesado por actos que no están claramente tipificados como condenables en la ley al momento de cometerse.

A raíz del Caso Infornet, que afectó a Nicaragua, Panamá, El Salvador y

Guatemala, en el que, sin consentimiento de las personas, se obtenían datos sobre su solvencia económica y se comercializaban a empresas para que ofrecieran sus productos (Durón, 2005), se decidió aunar esfuerzos y legislar sobre el tema de la protección de datos personales. De esta forma, el 21 de marzo de 2012 se aprueba la Ley N.° 787 de Protección de Datos Personales, cuyo principal objetivo es "promover y garantizar el bien común, asumiendo la tarea de promover el desarrollo humano protegiéndolo de todo tipo de explotación, discriminación y exclusión".

La legislación nicaragüense no aborda detalladamente la protección del cifrado y el anonimato, salvo en el ámbito del comercio electrónico. Aunque no hay una disposición constitucional específica sobre el cifrado, el precepto constitucional número 26 podría ofrecer cierta protección. Aunque no se menciona expresamente el cifrado en la constitución, el artículo 32, indirectamente, permite el cifrado al establecer que los ciudadanos nicaragüenses no están obligados a hacer lo que la ley no prescribe ni prohibidos de hacer lo que ella no prohíbe, relacionando este derecho con la libertad de expresión reconocida en el artículo 30.

La Ley N.° 787 de Protección de Datos Personales de Nicaragua (La Gaceta, 2012), en su artículo 8, determina cuatro categorías de datos: datos personales sensibles, datos personales relativos a la salud, datos personales informáticos y datos personales comerciales, las que tendrán diferentes características y su recolección y procesamiento girará en dependencia del caso.



La presentación de solicitudes de protección de datos personales debe realizarse ante la Dirección de Protección de Datos Personales (Diprodap). Una vez recibida la solicitud, se enviará al responsable del archivo de datos, quien tendrá un plazo de quince días hábiles para responder, proporcionar pruebas pertinentes y expresar por escrito sus comentarios.

El recurso constitucional del habeas data, diseñado para salvaguardar el derecho a la privacidad, enfrenta desafíos en su ejercicio efectivo. Sin embargo, en Nicaragua podrían aplicarse leyes secundarias relativas a la protección de datos personales y a la privacidad. Por ejemplo, el Código Penal, que tipifica y penaliza aquellas acciones que constituyen delito, dedica un capítulo a los delitos contra la vida privada y contra las intromisiones ilegítimas en la privacidad:

- **Sustracción, desvío o destrucción de comunicaciones: se castigará con prisión a aquel que, con conocimiento o suposición del contenido, ilegalmente se apropie, destruya o desvíe una comunicación ajena.**
- **Captación indebida de comunicaciones ajenas: se establece una pena de prisión.**
- **Acceso y uso no autorizado de información: se prevé una sanción con prisión.**
- **Denegación de acceso a la información pública: se establece pena de prisión y la inhabilitación para ejercer empleo o cargo público.**
- **Divulgación de información por parte de autoridades, funcionarios o empleados públicos: se contempla una pena de prisión y la inhabilitación para el ejercicio de empleo o cargo público.**
- **La orden de allanamiento debe llevarse a cabo de 6 a. m. a 6 p. m., salvo consentimiento del morador o en casos sumamente graves y urgentes, donde los jueces o las juezas resolverán en una hora solicitudes de la fiscalía o jefe policial. Se debe registrar la urgencia en la resolución que autoriza el**

allanamiento. La solicitud debe especificar las razones, el lugar y lo que se espera encontrar en el allanamiento, secuestro o detención. La resolución judicial que autoriza el allanamiento, secuestro o detención deberá contener: a) el nombre del juez o de la jueza y la identificación de la investigación, b) la dirección exacta del inmueble, c) el nombre de la autoridad que practicará el registro, d) La hora y la fecha en que deba practicarse la diligencia, e) el motivo del allanamiento. Respecto a las formalidades de allanamiento, se requiere una copia de la resolución judicial que autoriza el allanamiento y el secuestro.

- **La interceptación de comunicaciones requiere una solicitud expresa y fundamentada del fiscal general de la República o del director general de la Policía Nacional. Ambos deben evaluar los antecedentes y justificar la intervención, especificando la duración y las personas con acceso. La destrucción del material grabado se ordena tras el sobreseimiento o la sentencia de no culpabilidad firme. En casos de desestimación, falta de mérito o archivo, también se procede a la destrucción del material.**

En 16 de mayo de 2007 se aprueba la Ley de Acceso a la Información Pública, la cual se crea para fortalecer el ejercicio de la democracia, visto desde la promoción de la participación ciudadana activa. Estos son algunos de los principales alcances que esta ley reforzó: 1) el habeas data; 2) el principio de transparencia, y 3) el principio de acceso a la información pública[10].

[10] http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/675A94FF2EBFEE9106257331007476F2

En cuanto a las agencias relevantes respecto al control de las comunicaciones, la Ley N.º 1810, aprobada el 12 de febrero de 2014 y que reforma el Código Militar de Nicaragua establece en su artículo 2 inciso 15 que el Ejército de Nicaragua debe cumplir la función de "participar, en coordinación con las instituciones competentes, en la protección a los sistemas de datos, registros informáticos, espectro radioeléctrico y satelital, para evitar alteraciones o afectaciones a los sistemas de comunicación nacional y lo dispuesto para los fines de defensa nacional"[11].

De la misma manera, el artículo 68 de la Ley General de Telecomunicaciones[12], aprobada el 21 de julio de 1995, considera como infracción muy grave quien interfiera o intercepte intencionalmente los servicios de telecomunicaciones, afecte su funcionamiento e incumpla las leyes, reglamentos, tratados, convenios o acuerdos internacionales de telecomunicaciones en los que Nicaragua es parte.

Vale la pena mencionar que Nicaragua atraviesa una crisis sociopolítica que debilita el Estado de Derecho y la Independencia de Poderes, por lo que, si bien algunas leyes creadas en el pasado protegen datos personales, ahora han sido, frecuentemente, violentadas por el mismo gobierno en el poder. Es decir, las leyes que persiguen la violación de la privacidad tanto de los datos personales, de las telecomunicaciones y de los delitos Informáticos, están débilmente aplicadas.

[11] http://legislacion.asamblea.gob.ni/normaweb.nsf/b92aaea87dac762406257265005d21f7/ec53e953cf146ff806257c9f005e9567?OpenDocument
[12] http://legislacion.asamblea.gob.ni/normaweb.nsf/($All)/E19D0A4FF53C43320625715A00587598?OpenDocument

Vigilancia tecnológica

En 1987, el constituyente nicaragüense reconoce el derecho en el Título IV de la Constitución, Capítulo I, referente a los "Derechos, deberes y garantías del pueblo nicaragüense". Este capítulo incluye los "derechos de la personalidad", entendidos como aquellos que otorgan poder a las personas para proteger la esencia del ser humano y sus cualidades más importantes. El artículo 26 de la Constitución Política de Nicaragua establece el derecho humano a la inviolabilidad del domicilio, la correspondencia y las comunicaciones, lo que lleva a examinar detalladamente este principio en relación con las intervenciones telefónicas.

En materia de vigilancia de las comunicaciones, el ordenamiento jurídico nicaragüense no especifica el principio de transparencia. En relación con la interferencia de los proveedores de servicios, las empresas deben mantener un registro oficial de usuarios o clientes. Estos registros pueden ser solicitados por la autoridad competente para investigaciones, persecuciones y procesos penales. Esta legislación es sumamente peligrosa para la privacidad de las comunicaciones y podría, eventualmente, ser usada para persecución política y otras violaciones a los DD. HH. (Infobae, 2024).

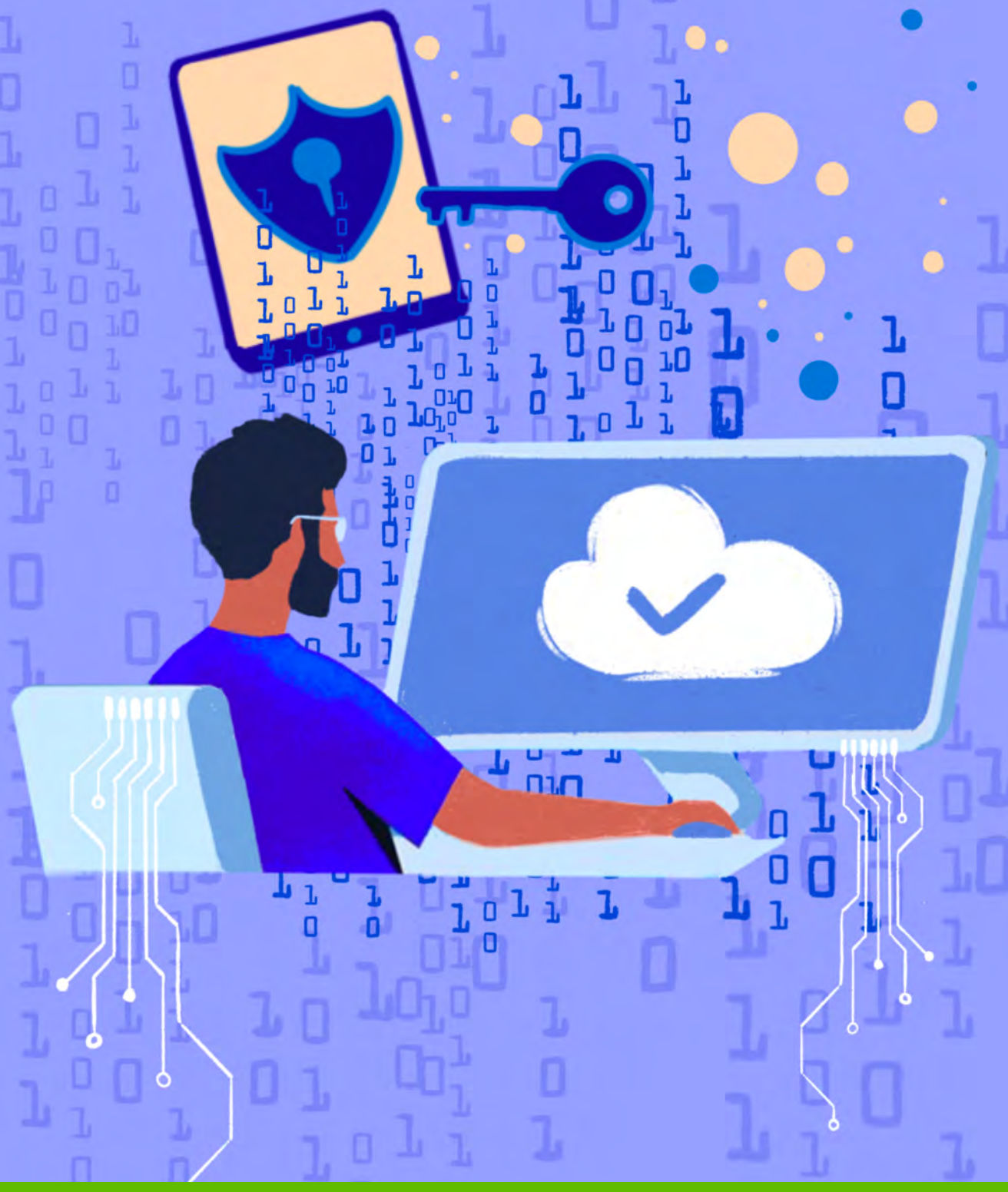
Un ejemplo de la escasa aplicación de las leyes de protección de los datos es el caso de Fake Antenna Detection Project, publicado por el medio alemán Deutsche Welle (DW, 2022) en 2022, que reveló el uso de falsas antenas de

comunicaciones en grandes ciudades de Nicaragua, utilizadas, presuntamente, para la vigilancia electrónica de medios de comunicación que, además, incluye rastreo de llamadas, mensajes de texto y ubicación de teléfonos. El medio comunicó que al menos existían 39 dispositivos de vigilancia, dejando en evidencia como la infraestructura de tecnologías de información del país está siendo vulnerada y utilizada para la recolección ilegal de datos privados.

Dado el contexto de represión de toda oposición al gobierno, la existencia de las falsas antenas/dispositivos de vigilancia toma mayor gravedad. Estas prácticas de vigilancia vulneran la intimidad y la privacidad de todas las personas, no solo de aquellas que pueden estar siendo perseguidas. Al poder ser utilizadas de manera masiva, toda la población que está expuesta a estas falsas antenas puede ser foco de vigilancia y espionaje ilegal.

Si bien no se ha verificado que los dispositivos hayan sido instalados por parte de las fuerzas armadas o autoridades civiles, sus operaciones deberían ser del conocimiento del Instituto Nicaragüense de Telecomunicaciones y Correos (Telcor), ente regulador de las telecomunicaciones, como parte de su monitoreo regular de las antenas operativas de las distintas empresas de telecomunicaciones. Esto da espacio a la sospecha, pues Telcor está dirigido actualmente por Nahima Janett Díaz Flores, hija del jefe de la Policía Nacional, Francisco Díaz Madriz, quien a su vez es consuegro del presidente de Nicaragua, Daniel Ortega, su hija Blanca Díaz Flores está casada con Maurice Ortega Murillo, séptimo hijo del mandatario (Swissinfo, 2022).

Costa Rica



Resumen de la situación a escala país

Costa Rica cuenta con una abundante legislación de protección de datos personales, así como la Agencia de Protección de Datos de los Habitantes, una agencia encargada de su observancia. No existen normas de rango legal que promuevan o limiten el anonimato y el cifrado, salvo una resolución del Consejo de la Superintendencia de Telecomunicaciones de 2012. Costa Rica cuenta con una regulación de altos estándares en materia de vigilancia e interceptación de comunicaciones y ha sido unos de los primeros países en hacer un llamado a establecer una prórroga de la tecnología de vigilancia.

Nivel normativo de los tratados de derechos humanos

Costa Rica ha ratificado los principales tratados internacionales en materia de derechos humanos, entre los que se encuentran la Convención Americana sobre Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales. Por otra parte, el artículo 7 de la Constitución Política de Costa Rica establece que *"los tratados públicos, los convenios internacionales y los concordatos, debidamente aprobados por la Asamblea Legislativa, tendrán desde su promulgación o desde el día que ellos designen, autoridad superior a las leyes"*, fijando explícitamente que existe una superioridad normativa de los tratados internacionales respecto de la ley nacional, la Constitución de Costa Rica impide que se pueda argumentar que en una materia de derechos fundamentales pueda primar una disposición de derecho interno que sea contraria a los estándares internacionales de derechos humanos.

Privacidad y protección de datos personales

La Constitución Política de Costa Rica cuenta con distintas disposiciones y artículos que reconocen derechos vinculados estrechamente con el derecho a la privacidad de la ciudadanía, el ejercicio de la autodeterminación informativa, el uso de las tecnologías y otros derechos digitales. Así, el artículo 23 de la constitución reconoce la inviolabilidad del domicilio, al establecer que "[e]l domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante, pueden ser allanados por orden escrita del juez o de la jueza competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley".

Por otro lado, el artículo 24 reconoce el derecho a la privacidad y la inviolabilidad de las comunicaciones, señalando que "se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones". Por último, el artículo 25 reconoce el derecho a la libertad de expresión de la siguiente manera "todos pueden comunicar sus pensamientos de palabra o por escrito, y publicarlos sin previa censura; pero serán responsables de los abusos que cometan en el ejercicio de este derecho, en los casos y del modo que la ley establezca".

No existen normas que regulen explícitamente la utilización de herramientas de tecnología de cifrado o anonimato. Lo anterior implica que no existen disposiciones legales que

reconozcan el derecho de las personas a utilizar este tipo de medidas para resguardar su privacidad, proteger sus comunicaciones o salvaguardar su anonimato. Como contrapartida, también es posible dar cuenta de que no existen disposiciones legales que, por el contrario, sancionen la utilización de herramientas de cifrado o anonimato, criminalicen su distribución o establezcan su utilización como un agravante de la responsabilidad penal.[13]

Costa Rica podría convertirse en el primer país en Centroamérica en constitucionalizar el derecho a la protección de datos personales (Ramos, 2023). Actualmente, la Constitución, en su artículo 24, reconoce el derecho a la intimidad. Este derecho tiene como objetivo asegurar a cada individuo un ámbito personal, una vida privada que permanezca fuera del alcance del público, a menos que la persona exprese su voluntad contraria, lo que se conoce como autodeterminación informativa como una protección de datos de carácter personal. Así se protege la libertad de las comunicaciones y prohíbe que cualquier entidad, ya sea pública o privada, pueda acceder sin restricciones a dichos contenidos.

Mediante la Ley N.° 8968[14] Ley de Protección de la Persona frente al tratamiento de sus datos personales, y que es complementada por su respectivo reglamento[15], para ejecutarla, se busca garantizar a cualquier persona, con independencia de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales.

Concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes. Dicho ámbito de acción es para los datos personales que figuren en

[13] Sin embargo, a nivel infra legal existe una resolución del Consejo de la Superintendencia de Telecomunicaciones del 2012 que establece en su numeral XVII que "A fin de cumplir con la Ley N.° 8968, Ley de Protección de la Persona Frente al Tratamiento de sus datos personas, todos los datos (números de teléfono, nombres, identificadores, y demás información) deberán ser cifrados con normas equivalentes o superiores a AES, utilizando un nivel de encriptación igual o superior a 256 bits. La ERPN debe garantizar que el cifrado de datos se utilice tanto en el contenido de las comunicaciones como en el almacenamiento de la base de datos.". http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73777&nValor3=90651&strTipM=TC

[14] http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

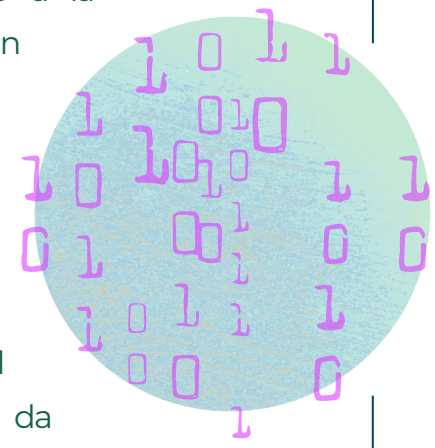
[15] Estas interpretaciones han sido complementadas por los distintos dictámenes administrativos de la Prodhab, los que se encuentran disponibles en el siguiente enlace: https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma_dictamen.aspx?param1=NRI&nValor1=1&nValor2=70975&nValor3=85989&strTipM=P

bases de datos automatizadas o manuales, de organismos públicos o privados.

Si bien la Ley N.° 8968 considera la autodeterminación informativa como un derecho fundamental, la constitución no reconoce este derecho o la protección de datos personales explícitamente como un derecho fundamental, por lo que debe considerarse como un derecho que puede derivarse del derecho fundamental a la intimidad o la privacidad.

En dicha ley también se crea la Agencia de Protección de Datos de los Habitantes (Prodhab), donde la ciudadanía que considere vulnerados sus derechos, en cuanto al uso de sus datos personales, puede denunciar dichas situaciones para que la Agencia, siguiendo el debido proceso, actúe para verificar, o no, un mal uso de los datos personales de las personas.

En cuanto su finalidad, la ley explícitamente señala en su artículo 1 que su objetivo es garantizar *"el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad"*. La mención al derecho a la autodeterminación informativa es en particular relevante, puesto que este término, acuñado por el Tribunal Constitucional Alemán en 1983, da cuenta de que la legislación costarricense considera la protección de los datos personales como parte del ejercicio de un derecho fundamental.



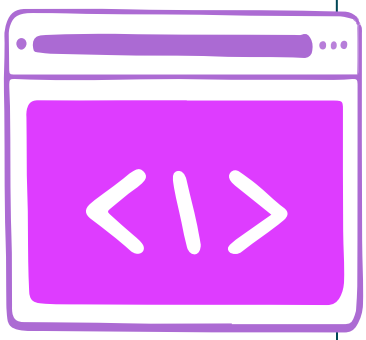
La ley reconoce los derechos de titulares de datos personales en su artículo 7, entre los que se consideran los derechos de acceso a sus datos personales, su rectificación, su cancelación o su supresión y el derecho a consentir la cesión de sus datos.

En cuanto a los principios de la legislación, solo reconoce de forma explícita el principio de consentimiento informado, consentir un trámite luego de ser informado de sus riesgos (artículo 5) y el principio de calidad de la información (artículo 6). Sin embargo, hay varias disposiciones cuyo contenido refleja la aplicación de

principios definidos por la ley con falta de claridad. Así, por ejemplo, el artículo 10 corresponde a una aplicación del principio de seguridad de los datos y el artículo 11 es una aplicación del principio de confidencialidad.

Por otro lado, el principio de finalidad se encuentra reconocido como un subprincipio del principio de calidad de la información, puesto que el artículo 6.4 señala que "los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines". Sin embargo, no existe una definición ni reconocimiento explícito de los principios de licitud, minimización de datos, limitación del plazo de conservación, saber cuánto tiempo o, el principio de responsabilidad activa como una garantía de seguridad del tratamiento de los datos.

Por otro lado, si bien se menciona la posibilidad de que el tratamiento de los datos personales se realice de forma automatizada, no existe un artículo que regule la toma de decisiones automatizadas realizada utilizando el procesamiento de datos personales, incluyendo la creación de perfiles. Esto puede ser particularmente importante para proteger los derechos de titulares respecto a la ejecución de sistemas de inteligencia artificial, que toman decisiones de manera automatizada en función del procesamiento de la información personal de titulares, por ejemplo, en materia de reclutamiento de personal, otorgamiento de beneficios estatales, entre otros.



Respecto a las fuentes de licitud para el tratamiento de datos personales, es decir, las causales bajo las cuales resulta lícito que un tercero procese los datos personales del titular, se encuentran recogidas de forma indirecta en la ley. En efecto, la ley establece que para tratar los datos de un titular se necesita su consentimiento informado (artículo 5) excepto en los siguientes casos (artículo 5.2):

a) Exista orden fundamentada, dictada por autoridad judicial competente o acuerdo adoptado por una comisión especial de investigación de la Asamblea Legislativa en el ejercicio de su cargo.

b) Se trate de datos personales de acceso ilimitado, obtenidos de fuentes de acceso público general.

c) Los datos deben ser entregados por disposición constitucional o legal.

Vale la pena mencionar que el hecho de que un dato se encuentre disponible en fuente de acceso público general, constituye una excepción al requisito del consentimiento del titular, extremadamente amplia, pues toda información disponible en internet podría ser considerada como obtenida de una fuente de acceso público general y, eventualmente, generar una afectación de la privacidad o autodeterminación informativa como consentimiento informado antes de dar datos de las personas titulares.

Del mismo modo, el artículo 8 de la ley establece un catálogo de excepciones a la autodeterminación informativa del titular, señalando que los derechos de la ley podrán ser limitados de manera justa, razonable y acorde al principio de transparencia administrativa en la medida que se persigan los siguientes fines:

a) La seguridad del Estado

b) La seguridad y el ejercicio de la autoridad pública.

c) La prevención, persecución, investigación, detención y represión de las infracciones penales o de las infracciones de la deontología en las profesiones.

d) El funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, cuando no exista riesgo de que las personas sean identificadas.

e) La adecuada prestación de servicios públicos.

f) La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.

En conclusión, Costa Rica cuenta con una ley de protección de datos personales relativamente nueva, pero tiene una serie de deficiencias normativas y dogmáticas que pueden afectar negativamente la protección de los derechos de titulares y personas defensoras de derechos humanos, en particular, el amplio catálogo de excepciones a la autodeterminación informativa, la falta de regulación sobre la toma automatizada de decisiones, el catálogo de derechos del titular, entre otros. Sin embargo, la legislación sí contempla la existencia de una agencia administrativa de control con suficientes facultades para velar por la protección de datos de la población.

Otras leyes relativas a la protección de datos personales y privacidad en Costa Rica:

- Ley N.° 7975 Ley de Información No Divulgada, que regula la utilización y resguardo de información confidencial privada[16]. Esta legislación busca proteger a través de la figura de la propiedad intelectual a aquella información no divulgada relacionada con los secretos comerciales e industriales.

[16] http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=41810&nValor3=74709

- Ley N.° 9048 sobre delitos informáticos[17], regula algunos delitos que afectan el derecho a la protección de datos personales, establece penas de prisión para los infractores y medidas de protección para titulares de los datos. Algunos aspectos relevantes de la ley son:

Regula la violación de datos personales, delito que consiste en apoderarse, modificar, interferir, acceder, copiar transmitir, publicar, difundir, recopilar, inutilizar, interceptar, retener, vender, comprar, desviar o dar un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica, sin el consentimiento y con peligro o daño para su intimidad o privacidad.

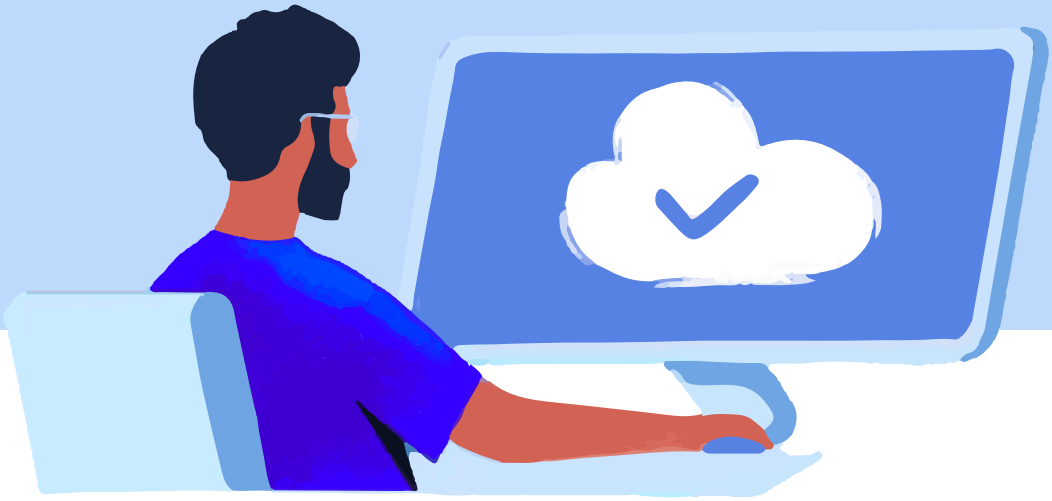
Establece medidas de protección para titulares de datos personales tales como los derechos ARCO; en caso de afectación a su derecho, pueden presentar denuncias o querellas ante las autoridades competentes.

- La Ley General de Telecomunicaciones de Costa Rica, tiene dentro de sus objetivos “proteger los derechos de los usuarios de los servicios de telecomunicaciones, asegurando eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura, mayor y mejor información, más y mejores alternativas en la prestación de los servicios, así como garantizar la privacidad y confidencialidad en las comunicaciones, de acuerdo con nuestra Constitución Política.”. En su segundo capítulo “régimen de protección a la intimidad y derechos del usuario final” desarrolla el régimen de privacidad y de protección de los derechos e intereses de las personas usuarias finales de los servicios de telecomunicaciones.

- Ley de Intervención de las Comunicaciones. Respecto de la inviolabilidad de las comunicaciones, la Sala Constitucional ha señalado que, las garantías establecidas en el artículo 24 de la Constitución de Costa Rica se encontrará

[17] https://www.migliorisiabogados.com/wp-content/uploads/2012/11/ley-9048-Delitos-informaticos-Costa-rica.pdf

satisfecha en la medida que se cumplan las siguientes condiciones: i) intervención necesaria del juez o de la jueza en cualquier autorización para intervenir comunicaciones privadas, ii) Se trate de una autorización debidamente fundamentada donde se autorice la diligencia y se limite el tiempo para su realización, iii) Que exista un estricto control sobre la implementación de la diligencia y iv) Que sea el juez o la jueza quien discrimine el contenido de la información y qué parte de ella pueda trascender a las partes y la policía[18]. El artículo 263 bis del Código Procesal Penal de Costa Rica establece que *"el Juez podrá ordenar, de oficio o a petición de las partes del proceso, la intervención de las comunicaciones orales o escritas del imputado, así como el registro, el secuestro y el examen de documentos privados. Deberá actuar según el procedimiento y en los casos previstos en la ley que rige la materia."*



La ley que actualmente regula los requisitos que debe cumplir la intervención de comunicaciones en Costa Rica es la Ley N.° 7425 sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones. En su artículo 9 establece que *"Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, cuando involucre el esclarecimiento de los*

[18] Resolución de la Sala Constitucional de Costa Rica N.° 3195, dictada el 20 de junio de 1995.

siguientes delitos [...] En los mismos casos, dichos tribunales podrán autorizar la intervención de las comunicaciones entre los presentes, excepto lo dispuesto en el segundo párrafo del artículo 26 de la presente ley, cuando se produzcan dentro de domicilios y recintos privados, la intervención solo podrá autorizarse si existen indicios suficientes de que se lleva a cabo una actividad delictiva".

El artículo 10 de la Ley N.° 7425 establece explícitamente que la realización de la intervención de telecomunicaciones solo resultará lícita en la medida en que exista una autorización judicial previa. Esta orden podrá ser realizada de oficio, sin necesidad de solicitud, o a solicitud del jefe del Ministerio Público, del director del Organismo de Investigación Judicial o de alguna de las partes del proceso. Sin embargo, no basta con que exista una resolución, sino que debe ser de carácter fundada, es decir, implica que el juez o la jueza realice un juicio respecto a los antecedentes del caso y si justifican la autorización de la medida intrusiva.

El artículo 13 establece cuál debe ser el contenido mínimo de dicha autorización; el artículo 14 establece los medios técnicos para recolectar y almacenar las comunicaciones de escucha ilegal; el artículo 20 señala que las empresas de telecomunicaciones "están obligadas a conceder, a la autoridad judicial, todas las facilidades materiales y técnicas para que las intervenciones sean efectivas, seguras y confidenciales".

- El allanamiento y registro de morada se encuentra regulado en el artículo 193 y siguientes del Código Procesal Penal. Así, el artículo 193 establece que cuando el registro se realice en un lugar habitado este deberá realizarse personalmente por el juez o la jueza entre las seis y las dieciocho horas, solo podrá accederse en un horario distinto a este cuando medie el consentimiento del morador o en casos sumamente graves y urgentes, sobre los que deberán dejarse constancia por parte del juez o de la jueza en

la autorización dictada por él mismo. En caso de lugares no habitados no existirá restricción horaria y el juez o la jueza podrá delegar la diligencia en un funcionario del Ministerio Público.

En ambos casos el juez o la jueza debe dictar una resolución que autorice el allanamiento y que debe cumplir con el contenido mínimo establecido en el artículo 195. A diferencia de la escucha ilegal de comunicaciones, en donde siempre debe existir una autorización judicial previa, la regulación sobre allanamientos y registros sí contempla la situación extraordinaria y excepcional de poner ingresar a una vivienda sin contar con una autorización judicial previa. Así, el artículo 197 del Código Procesal Penal establece que este ingreso estará justificado solo en ciertas circunstancias que se encuentran claramente especificadas.

Vigilancia tecnológica

Costa Rica es considerado un país con altos estándares de protección de los derechos humanos como la privacidad, intimidad y la libertad de prensa. No hay registros de uso o ataques por medio de tecnologías de vigilancia ilegal. Ha sido uno de los primeros países en hacer un llamado para establecer un mayor plazo a la tecnología de vigilancia, se ha considerado que representa una amenaza contra los derechos humanos y la privacidad (Amnesty Internacional, 2023).

Sin embargo, recientemente el país sufrió un grave caso de recolección y utilización ilegal de información de carácter personal. En este caso se acusó al presidente Carlos Alvarado de utilizar políticamente a la Unidad Presidencial de Análisis de Datos (Upad), una unidad cuyo objetivo declarado era procesar información estadística para toma de decisiones, al obtener acceso a información personal y confidencial de las personas de forma inconstitucional y sin ningún tipo de supervisión externa. Lo anterior llevó a la Fiscalía a ordenar el allanamiento de su hogar, así como acusarlo de fraude, prevaricato por incumplir la ley; abuso de autoridad, así como infringir el artículo 14 de la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (Silva, 2022).

Costa Rica no cuenta con una ley dedicada exclusivamente a la regulación de los organismos de inteligencia, sus facultades, su gobernanza y organización institucional. En cambio, estas materias se encuentran reguladas en la Ley

General de Policía de 1994, que establece la "Dirección de Inteligencia y Seguridad" (DIS) en los artículos 13 al 17, junto al Decreto Ejecutivo 23758 MP que establece el "Reglamento de Organización y Servicio de Dirección de Inteligencia y Seguridad Nacional". Dicha organización se ha visto envuelta en el pasado en la realización de intervenciones telefónicas ilegales (Sancho, 2014).

En Costa Rica ha habido un importante crecimiento en la creación de organismos con atribuciones que podrían ser consideradas parte del sistema de inteligencia, entre ellas el Departamento de Inteligencia Policial (Dipol) del Ministerio de Seguridad Pública, la Unidad de Inteligencia del Organismo de Investigación Judicial (OIJ), la Unidad de Inteligencia Financiera (UIF), Instituto Costarricense sobre Drogas (ICD), el Área de Planificación e Inteligencia de la Policía de Control Fiscal y el Área de Seguridad y Protección de Bienes Institucionales del ICE.

Si bien estos organismos no cuentan con atribuciones tan amplias e intrusivas como la DIS, sí resultaría oportuno que Costa Rica avance hacia la creación de una ley que regule un sistema nacional de inteligencia que permita establecer controles claros a su actividad, a fin de que cumpla con estándares internacionales de derechos humanos, que promueva el control político y democrático de las instituciones de inteligencia y que propicie una coordinación entre los distintos organismos a través de un sistema de gobernanza o un proceso eficaz de la inteligencia.

Anexo N°1.

Situación normativa de Centroamérica en materia de protección de datos, privacidad y vigilancia.

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica
La Corte de Constitucionalidad ha interpretado que el derecho a la intimidad y la privacidad se encuentran relacionados con los artículos 23, 24 y 25 de la Constitución. El reconocimiento al derecho a la protección de datos personales y a los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) se da únicamente respecto de aquellos datos personales contenidos en archivos, documentos o registros estatales o públicos (artículo 31 de la Constitución).	El derecho a la privacidad está regulado en el artículo 2 de la Constitución salvadoreña de 1983; se garantiza el derecho al honor a la intimidad personal y familiar ya la propia imagen. El artículo 2 de la Constitución sirve de base sobre el cual se ha interpretado, vía jurisprudencial, el derecho a la autodeterminación informativa, interpretándose que es aplicable tanto en el ámbito público como privado.	El derecho a la privacidad, cualquiera que sea su esfera, se le denomina “derecho a la intimidad”, y está garantizado por la Constitución Política en el artículo 57. Respecto de la inviolabilidad del domicilio, la Constitución establece en el artículo 99 las excepciones para limitar tal derecho.	La Constitución consagra el derecho a la privacidad (art 26), el cual tiene por objeto proteger la privacidad y la inviolabilidad del domicilio, la correspondencia y las comunicaciones. También se consagra el habeas data como herramienta judicial para la protección de los datos personales.	Se encuentra reconocidos por la Constitución diferentes normas relacionadas con la privacidad, tales como la inviolabilidad del domicilio, salvo autorización judicial o para impedir la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad. (art. 23). También consagra el derecho a la privacidad y la inviolabilidad de las comunicaciones (art. 24)

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica

2. Tratados internacionales

Todos los países han ratificado los principales tratados internacionales relacionados con los derechos a la protección de datos personales y la privacidad; estos tratados son:

- Declaración Universal de Derechos Humanos (artículo 1212).
- Pacto Internacional de Derechos Civiles y Políticos (artículo 1712).
- Convención sobre los Derechos del Niño (artículo 162).
- Convención Americana de Derechos Humanos (artículo 112).

Excepciones:

- Convención Interamericana sobre Asistencia Mutua en Materia Penal (MLAT, en inglés). Únicamente El Salvador y Honduras se han adherido a la Convención.
- Convenio de Budapest sobre ciberdelincuencia (el cual aborda la intercepción de las comunicaciones como mecanismo para la investigación de delitos informáticos). Únicamente Costa Rica ha ratificado dicho Convenio.

3. Jurisprudencia Un fallo de la Corte Constitucional establece que se debe obtener el consentimiento de la persona interesada para procesar sus datos y utilizar los datos en el ámbito privado.	El derecho a la autodeterminación informativa y Los derechos ARCO han sido reconocidos vía jurisprudencia de la Sala de lo Constitucional de la Corte Suprema de Justicia de El Salvador, específicamente en las sentencias de los amparos 934-2007 y 142-2012 de la Sala de lo Constitucional de la Corte Suprema de Justicia.			

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica
No existe ley especial de protección de datos personales, pero algunos artículos en otras leyes podrían proteger privacidad y los datos personales.	El Salvador no cuenta con una ley de protección de datos personales.	No cuenta con una ley específica de protección de datos personales que proteja la autodeterminación informativa de su ciudadanía y sólo cuenta con un procedimiento parcial de Habeas Data establecido a nivel reglamentario.	La ley N° 787 de protección de datos personales, que tiene por objeto "promover y garantizar el bien común, asumiendo la tarea de promover el desarrollo humano protegiéndolo de todo tipo de explotación, discriminación y exclusión.	Ley N° 8968 ley de protección de la persona frente al tratamiento de sus datos personales, y su respectivo reglamento, que tiene por objeto garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales.

Algunas normativas sectoriales ofrecen protecciones limitadas a la protección de datos personales y a la privacidad.	Algunas normativas sectoriales ofrecen protecciones limitadas a la protección de datos personales y a la privacidad.	Algunas normativas sectoriales ofrecen protecciones limitadas a la protección de datos personales y a la privacidad.	La normativa militar por su parte a el Código Militar de Nicaragua establece en que el ejército de Nicaragua debe cumplir la función de "participar, en coordinación con las instituciones competentes, en la protección a los sistemas de datos, registros informáticos, espectro radioeléctrico y satelital, para evitar alteraciones o afectaciones a los sistemas de comunicación nacional y lo dispuesto para los fines de defensa nacional (art. 2 inciso 15)	La ley N ° 7975 ley de información no divulgada, que regula la utilización y resguardo de información confidencial privada, y cuyo fin es proteger a través de la figura de la propiedad intelectual a aquella información no divulgada relacionada con los secretos comerciales e industriales.

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica
Ley de Acceso a la Información Pública				
Establece parámetros generales para el manejo de los datos personales en registros públicos o estatales y por parte de entidades públicas.	La ley de acceso a la información pública de El Salvador contiene un breve capítulo relativo a la protección de datos personales en bases de datos, archivos físicos o documentos en posesión de entidades públicas sujetas a la ley, dejando sin regulación el manejo de datos personales por sujetos privados.	Consagra la existencia de un procedimiento de Habeas Data; regula el derecho a la protección de los datos personales en el ámbito público, sus principios, obligaciones y sanciones; establece la obligación legal de colaboración entre las empresas proveedores de telecomunicaciones con la Unidad de Intervención de las Comunicaciones la Comisión Nacional de Telecomunicaciones.	Los principales alcances que la ley reforzó son: 1) el habeas data; 2) el principio de transparencia, y 3) el principio de acceso a la información pública.	En los artículos 27 y 30, por una parte, se garantiza la libertad de petición, en forma individual o colectiva, ante cualquier funcionario público o entidad oficial, y el derecho a obtener pronta resolución; y por otra, se garantiza el libre acceso a los departamentos administrativos con propósitos de información sobre asuntos de interés público. Quedan a salvo los secretos de Estado, respectivamente.
Ley de Telecomunicaciones				
La ley de equipos terminales móviles de 2013, en los artículos 3 y 9 establece condiciones que impiden el derecho a comunicarse de forma anónima. La ley de telecomunicaciones regula aspectos relacionados con la confidencialidad de los datos; interceptación,	La ley de telecomunicaciones regula el derecho al secreto de las comunicaciones, la confidencialidad de los datos personales no públicos. Los proveedores de servicios de telecomunicación tienen la obligación legal de llevar un registro de	Se encuentra bajo trámite la llamada “ley SIM” que establece la obligación del registro de clientes de telecomunicaciones, así como el registro y entrega de otras formas de telecomunicación, lo que puede resultar particularmente perjudicial para las personas defensores de derechos humanos y	Según el artículo 68 de la ley de telecomunicaciones se considera como infracción muy grave quien interfiera o intercepte intencionalmente los servicios de telecomunicaciones, afecte su funcionamiento e incumpla las leyes, reglamentos, tratados, convenios o acuerdos internacionales de	La ley tiene objetivo: proteger los derechos de los usuarios de los servicios de telecomunicaciones, así como garantizar la privacidad y confidencialidad en las comunicaciones. Se establece el régimen de protección a la intimidad, y derechos e intereses del usuario final.

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica
grabación o difusión de datos personales transmitidos por medios electrónicos; aplicabilidad de principios y sanciones relacionadas con el tratamiento de datos personales, así como el reconocimiento de los derechos ARCO.	clientes con sus documentos de identificación en relación con su respectivo número telefónico o tarjeta SIM.	para el ejercicio del derecho a comunicarse anónimamente.	telecomunicaciones en los cuales Nicaragua es parte.	
Ley de Protección al Consumidor				
Aunque existe legislación en la materia, la ley no aborda aspectos relacionados con la privacidad o el derecho a la protección de los datos personales.	La ley de protección al consumidor regula la difusión o publicación de datos personales o información confidencial y crediticia; compartir o utilizar los datos personales ante el incumplimiento de obligaciones crediticias.	Aunque existe legislación en la materia, la ley no aborda aspectos relacionados con la privacidad o el derecho a la protección de los datos personales.	Aunque existe legislación en la materia, la ley no aborda aspectos relacionados con la privacidad o el derecho a la protección de los datos personales debido a que existe una ley especial de protección de datos personales.	La ley de promoción de la competencia y defensa efectiva del consumidor de Costa Rica regula establece mecanismos para proteger los derechos de los consumidores, sin embargo, no aborda en específico el derecho a la protección de los datos personales.
Legislación en materia penal				
La divulgación indebida de datos, la usurpación de identidad, el acceso no autorizado a sistemas informáticos y -bajo ciertas circunstancias- el delito de pánico financiero, entre otras acciones contra la privacidad y la protección de los datos personales	El Código Penal de 1997 y el código procesal penal regulan lo relativo al allanamiento, requisa, posesión ilegal de comunicaciones escritas, documentos confidenciales o personales, calumnia, difamación, entre otros delitos que pueden aplicar en el ámbito virtual como	En los delitos de injurias y calumnias, se verá agravada la pena en aquellas declaraciones realizadas "utilizando sitios web de divulgación colectiva o redes sociales a través de internet", lo anterior es desproporcional puesto que establece un	Tipifica y penaliza los delitos contra la vida privada y contra las intromisiones ilegítimas en la privacidad, tales como: la interceptación de telecomunicaciones; allanamiento, denegación de acceso a la información pública; sustracción, desvío o	Se encuentra regulada el allanamiento y registro de morada, la que debe hacerse previa autorización judicial, salvo excepciones, en caso de suma graves y urgentes. Se establece además que éste ingreso estará

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica
están incluidas en la normativa penal. La Ley de Control y Prevención del Lavado de Dinero autoriza el uso de cualquier medio tecnológico disponible para la investigación de cualquier delito para facilitar el esclarecimiento de éste.	presencial. Al igual que Honduras, El Salvador se ha adherido a la Convención Interamericana sobre Asistencia Mutua en Materia Penal. Recientemente se aprobaron una serie de reformas legales en materia penal y procesal penal que, de acuerdo con la Relatoría Especial para la Libertad de Expresión, pueden representar riesgos de criminalización al ejercicio legítimo de la libertad de expresión, de prensa y acceso a la información.	agravante sólo por el medio utilizado para expresarla; establece penas de cárcel para quien intercepte telecomunicaciones sin consentimiento de la persona titular; sanciona con multas a las empresas proveedoras de servicios de telecomunicaciones por la falta u omisión de registro o identificación de clientes. El país se adhirió a la Convención Interamericana sobre Asistencia Mutua en Materia Penal.	destrucción de comunicaciones; captación indebida de comunicaciones ajenas; acceso y uso no autorizado de información, entre otras.	justificado sólo en ciertas circunstancias que se encuentran claramente especificadas.
Caso INFORNET				
En 2018, el congresista Ronald Arango presentó un recurso de amparo (habeas data) contra la empresa Infornet por la comercialización datos personales de las y los guatemaltecos sin consentimiento previo, alegando que dicha práctica va en contra de la prohibición de la Corte Constitucional.	Dos casos emblemáticos respecto al derecho a la autodeterminación informativa fueron los procesos de amparo interpuestos por el presidente y representante legal de la Asociación Salvadoreña para la Protección de Datos e Internet (INDATA) en contra de las empresas Dicom Centroamérica General Automotriz, e Infornet. Ambos amparos fueron favorables para INDATA, lo que confirmó la interpretación de la Constitución de que el derecho a la autodeterminación informativaes uno de los reflejos del derecho a la seguridad.		A raíz del caso Infornet, en cual se obtenían datos personales y crediticios, sin el consentimiento de las personas y con la finalidad de comercializarlos, se creó la Ley de Protección de Datos Personales de Nicaragua.	No existe.

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica
Leyes de Delitos Informáticos				
El decreto 39-2022, ley de prevención y protección contra la ciberdelincuencia, tiene como objetivo sancionar y regular la prevención de la ciberdelincuencia, la tipificación de conductas delictivas, mejorar la protección de los datos personales; también establece normas para la incorporación de medios de pruebas digitales.	La ley especial contra los delitos informáticos y Conexos tiene como objetivo proteger los derechos e intereses que puedan verse afectados por acciones o conductas delictivas cometidas por medio de las tecnologías de la información y la comunicación (TIC's). Algunos ejemplos de delitos informáticos relacionados con el derecho a la protección de los datos personales y la privacidad son: la utilización de datos personales sin autorización y a través de las TIC'; la revelación indebida de datos o de información confidencial.	El código penal incluye la tipificación de una serie de delitos informáticos muy similar a la forma de redacción de estos delitos en el Convenio de Budapest, tales como: delito de acceso no autorizado, daños a datos y sistemas informáticos.	Existe la ley de delitos informáticos que tiene por objeto prevenir, investigar, perseguir y sancionar aquellos delitos cometidos a través de las TIC, en perjuicio de las personas naturales o jurídicas. prevención, investigación, y así como también la protección integral de los sistemas que utilicen dichas tecnologías, su contenido y cualquiera de sus componentes, en los términos previstos en esta Ley.	La ley 9048 sobre delitos informáticos regula algunos delitos que afectan el derecho a la protección de datos personales, establece penas de prisión para los infractores y medidas de protección para titulares de los datos. Regula de violación de datos personales y medidas de protección como la regulación de los derechos ARCO.
Relacionada con la Vigilancia Tecnológica				
Derecho a la inviolabilidad del domicilio, la correspondencia y las comunicaciones; sin embargo, no existe otra específicamente legislación especial en la materia.	El derecho a la inviolabilidad del domicilio, la correspondencia y las comunicaciones; sin embargo, no existe otra específicamente legislación especial en la materia.	De las Comunicaciones que no cuenta los controles y contrapesos habituales de un Estado de Derecho.	Derecho a la inviolabilidad del domicilio, la correspondencia y las comunicaciones; sin embargo, no existe otra específicamente legislación especial en la materia.	Derechos humanos como la privacidad, intimidad y la libertad de prensa; no hay registros de uso o ataques por medio de tecnologías de vigilancia ilegal, y tampoco existe normativa específica relativa a ello..

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica
Leyes de Intervenciones de Telecomunicaciones o Escuchas				
La intervención de las comunicaciones es posible ejecutarla aplicando la Ley contra la Delincuencia Organizada con el objetivo de prevenir y sancionar los delitos cometidos por grupos del crimen organizado.	La ley especial para la intervención de las telecomunicaciones de El Salvador tiene como objetivo fortalecer los procedimientos, y mecanismos para la persecución y combate de la criminalidad, obtención, ofrecimiento y producción de prueba en un proceso judicial; debe estar autorizada por un juez o jueza competente, solicitada previamente y de manera fundada y motivada por parte de la fiscalía general.	La ley de intervención de las comunicaciones establece un marco legal de regulación procedimental de la intervención de las comunicaciones; el órgano a cargo es la Unidad de Intervención de las Comunicaciones.	El código penal regula la interceptación de comunicaciones, requiriendo que sea a solicitud expresa y fundamentada por Fiscal General de la República o del Director General de la Policía Nacional. Ambos deben evaluar los antecedentes y justificar la intervención, especificando la duración y las personas con acceso.	La Ley N°7425 sobre registro, secuestro y examen de documentos privados e intervención de las comunicaciones, que establece explícitamente que la realización de la intervención de telecomunicaciones establece que sólo resultará lícita en la medida en que exista una autorización judicial previa.
Normativas sobre transparencia en adquisiciones de tecnologías de vigilancia				
No existen mecanismos especiales de transparencia o supervisión pública para transparentar la adquisición de tecnologías de vigilancia. La normativa aplicable a la transparencia en la adquisición de tecnología de vigilancia en los países centroamericanos suele ser las leyes que regulan las compras públicas junto con las leyes de acceso a la información pública (mediante la cual se obliga a los entes y funcionarios públicos a rendir cuentas); sin embargo, la compra de este tipo de tecnología, por lo general, se suele justificar con base en razones de seguridad pública, y además se clasifica como información reservada o confidencial (excepciones a la publicidad de la información pública conferidas por las leyes de acceso a la información pública).				

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica
Estados de excepción y suspensiones de derechos constitucionales				
Regulado, pero actualmente no se encuentra aplicado.	Existe una suspensión de los derechos constitucionales y garantías procesales que inició en marzo de 2022 y que se ha prolongado por más de dos años consecutivos, bajo el argumento de velar por la seguridad pública y para el combate de las maras (pandillas).	Regulado, pero actualmente no se encuentra aplicado.	Regulado, pero actualmente no se encuentra aplicado.	Regulado, pero actualmente no se encuentra aplicado.

5. Situación Actual

Mecanismos legales de protección				
El amparo, el recurso de inconstitucionalidad y el hábeas data constituyen garantías constitucionales para defender el derecho a la privacidad y a la protección de datos; particularmente, mediante el habeas data se puede conocer, acceder y controlar la información y los datos personales en registros públicos y en manos de entidades del sector público (artículos 30 al 35 de la Constitución Política).	Con base a la Constitución, los derechos de privacidad y protección de datos personales pueden defender a través del proceso de amparo, recurso de inconstitucionalidad. No existe propiamente la figura del hábeas data.	Con base a la Constitución, los derechos de privacidad y protección de datos personales pueden defender a través del amparo constitucional, recurso de inconstitucionalidad y el hábeas data; el ultimo tiene como finalidad que la información se pueda actualizar, rectificar y/o suprimir.	Nicaragua cuenta con una ley de protección de datos personales, Asimismo se reforzó esto con la garantía del habeas data. El ordenamiento jurídico nicaragüense no aborda la promoción o limitación del cifrado y el anonimato, excepto en el ámbito del comercio electrónico. En materia de vigilancia tecnológica destaca la ausencia del principio de transparencia en la realización de interceptación de comunicaciones, así como el peligroso proyecto que el presidente Ortega busca	El amparo, el recurso de inconstitucionalidad y el hábeas data constituyen garantías constitucionales para defender el derecho a la privacidad y a la protección de datos; particularmente, mediante el habeas data se puede conocer, acceder y controlar la información y los datos personales en registros públicos y en manos de entidades del sector público (artículos 30 al 35 de la Constitución Política).

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica
			aprobar para obligar a las empresas telefónicas a suministrar información de sus usuarios al ente regulador de telecomunicaciones.	

Agencias independientes que velen por cumplimiento (Ombudsman, Defensorías, etc.)

No cuenta con una Agencia independiente para la defensa de los derechos a la protección de los datos personales, privacidad y contra la vigilancia tecnológica. Este tipo de casos pueden presentarse ante entidades de la administración de justicia, el Instituto de Acceso a la Información Pública (IAIP), o la Procuraduría de Derechos Humanos.	No cuenta con una Agencia independiente específica para la defensa de los derechos a la protección de los datos personales, privacidad y contra la vigilancia tecnológica. Este tipo de casos pueden presentarse ante entidades de la administración de justicia, el Instituto de Acceso a la Información Pública (IAIP), o la Procuraduría para la Defensa de los Derechos Humanos.	No cuenta con una Agencia independiente específica para la defensa de los derechos a la protección de los datos personales, privacidad y contra la vigilancia tecnológica. Sin embargo, el instituto de acceso a la información pública IAIP y la administración de justicia tienen responsabilidad y competencias en la materia.	La Dirección de Protección de Datos Personales.	La agencia de protección de datos de los habitantes.

Desafíos principales y controversias, con ejemplos

Caso Tigo: se trata de una investigación sobre vigilancia ilícita llevada a cabo por la Comisión Internacional Contra la Impunidad en Guatemala (CICIG), en la que se determinó que existían indicios relevantes y significativos que permiten inferir la práctica de seguimientos, escuchas e	En enero de 2022 se dio a conocer mediante un informe de CitizenLab con la colaboración de varias organizaciones de derechos digitales y seguridad informática acerca de la adquisición y uso del software de vigilancia “Pegasus” en contra de periodistas, activistas y	La vigilancia en internet y en las telecomunicaciones en Honduras forma parte de una política en materia de seguridad pública mediante la cual fueron fusionados temas relativos a seguridad, defensa e inteligencia. Un ejemplo de compra de tecnología de vigilancia altamente intrusiva es el sistema de	Creación de normativa relativa a la promoción y limitación de cifrado y anonimato, la que actualmente solo se encuentra regulado en el ámbito del comercio electrónico. Caso “Fake Antenna Detection Project” y el Proyecto que el presidente Ortega busca aprobar para obligar a las	El caso más reciente es aquel que hubo recolección y utilización ilegal de información de carácter personal. En este caso se acusó al presidente Carlos Alvarado de utilizar políticamente a la Unidad Presidencial de Análisis de Datos (UPAD), una unidad cuyo objetivo declarado era procesar información

Guatemala	El Salvador	Honduras	Nicaragua	Costa Rica
intervenciones de teléfonos celulares sin la debida orden judicial por parte del Ministro de Economía de la época y exgerente de la empresa Tigo. La vigilancia y monitoreo de las comunicaciones de manera ilegal a través de tecnología para el espionaje y practicas autoritarias es uno de los desafíos actuales para las y los defensores de derechos humanos.	miembros de la sociedad civil en El Salvador. La prolongación de un régimen de suspensión de garantías constitucionales, y la falta de regulación respecto a temas de privacidad y protección de datos toman especial relevancia en contexto actual de El Salvador.	espionaje "Galileo" tiene la capacidad de descifrar archivos, correos cifrados, grabar llamadas, entre otras comunicaciones.	empresas telefónicas a suministrar información de sus usuarios al ente regulador de telecomunicaciones.	estadística para toma de decisiones, al obtener acceso a información personal y confidencial de los y las costarricense de forma inconstitucional y sin ningún tipo de supervisión externa. Lo anterior, llevó incluso al allanamiento de la casa del Presidente.

Conclusión

A partir del análisis comparativo de los cinco países objeto de este estudio es posible concluir que existe un nivel disímil de cumplimiento de estándares internacionales de derechos humanos en lo que respecta a materias de regulación tecnológica y derechos digitales.

Adicionalmente, se pudo constatar importantes deficiencias normativas en la regulación de distintos países, como se señala en el Anexo N.º1, los cinco países cuentan con un cumplimiento favorable de aplicación de derechos constitucionales y de ratificación de tratados internacionales; sin embargo, al momento de revisar la aplicación legal de dichos derechos es posible encontrar importantes fallas. Solo Nicaragua y Costa Rica cuentan con una ley de protección de datos personales.

Del mismo modo, ni Guatemala ni Costa Rica cuentan con una normativa que regule, específicamente, la privacidad digital. De forma más grave, solo Costa Rica tiene, parcialmente, regulado el uso de tecnologías de vigilancia gubernamental y privada.

Todo lo anterior da cuenta de que, si bien en la constitución y en los tratados internacionales se consagran los derechos fundamentales que se cruzan con el uso de las tecnologías, existen importantes deficiencias y lagunas regulatorias al momento de concretar y ejecutar legalmente los derechos. Esto es en particular grave por dejar a la ciudadanía y a las personas defensores de derechos humanos con un “derecho de papel”, que si bien existe en la constitución, no necesariamente se aplica en la práctica, ya sea por la falta de una ley que lo haga efectivo o por la inexistencia de entes institucionales que se dediquen a aplicar dichas disposiciones o por fallas en la forma en que opera el estado de derecho en un país particular.

Referencias

- Access Now. (10 de marzo de 2023). Guatemala, Honduras y El Salvador se abstienen de entregar información sobre el tratamiento de datos biométricos de personas migrantes. Access Now. https://www.accessnow.org/press-release/-guatemala-honduras-el-salvador-no-dan-informacion-acuerdos-biometricos-migrantes/

- Amnesty International. (june 5 de 2023). Costa Rica: All states must immediately ban highly invasive spyware. AI. https://www.amnesty.org/en/latest/-news/2023/06/costa-rica-all-states-must-immediately-ban-highly-invasive-spyware/

- Argueta, Otto. (2020). El reto de crear un nuevo Consejo Nacional de Defensa y Seguridad es político. Contracorriente. https://contracorriente.red/2022/09/14/el-reto-de-crear-un-nuevo-consejo-nacional-de-defensa-y-seguridad-es-politico/

- Asamblea Nacional. Ley de Protección de Datos Personales, Ley N°. 787. (2012, 21 de marzo). La Gaceta (61). http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d#:~:text=

- Asociación Salvadoreña Derecho y Desarrollo (Adesa). (2011). El caso Infornet, un paso hacia la regulación del habeas data. Adesa. https://adesaelsalvador.blogspot.com/2011/06/el-caso-infornet-un-paso-hacia-la.html

- Bermúdez, Margarita. (21 de junio de 2018). Error 402 ¿Terrorismo Cibernético en Guatemala? Derechos Digitales. https://www.derechosdigitales.org/12205/error-402-terrorismo-cibernetico-en-guatemala/

- Bernal, David. (2 de marzo de 2022). Investigación sobre espionaje con Pegasus: Fiscalía cita a directivos de la APES. La Prensa Gráfica. https://www.laprensagrafica.com/elsalvador/Investigacion-sobre-espionaje-con-Pegasus-Fiscalia-cita-a-directivos-de-la-APES-20220302-0038.html

- Comisión Interamericana de Derechos Humanos (CIDH). (2015). Situación de derechos humanos en Honduras. OEA/Ser.L/V/II. Doc. 42/15 31 diciembre 2015. https://www.oas.org/es/cidh/informes/pdfs/Honduras-es-2015.pdf

- Comisión Internacional contra la Impunidad en Guatemala (CIGIC). (2019). Denuncia No. 2 Espionaje y escuchas telefónicas ilegales en la compañía Tigo. CICIG. https://www.cicig.org/wp-content/uploads/2019/08/DENUNCIA_02_Espionaje.pdf

- Congreso de la República. (9 de junio de 2021). Iniciativa de ley garantiza la protección de datos personales. https://www.congreso.gob.gt/noticias_congreso/6513/2021/1#gsc.tab=0; https://www.congreso.gob.gt/detalle_pdf/iniciativas/5971#gsc.tab=0

- Contraloría General de Cuentas. (2002). Ley de Bancos y Grupos Financieros. Decreto 19-2002. https://www.contraloria.gob.gt/imagenes/i_docs/i_leg_ley/LEY%20DE%20BANCOS%20Y%20GRUPOS%20FINANCIEROS.pdf

- Cristosal. (octubre de 2023). La excepción se volvió la norma. Una mirada a las reformas penales y su impacto en las garantías ciudadanas. Cristosal. https://cristosal.org/ES/la-excepcion-se-volvio-la-norma-una-mirada-a-las-reformas-penales-y-su-impacto-en-las-garantias-ciudadanas/

- De Mata, Diana. (2020). La privacidad de datos en Guatemala y los derechos fundamentales que se derivan de la misma según la jurisprudencia de la Corte de Constitucionalidad. Consortium Legal. https://s3.amazonaws.com/documents.lexology.com/7c431e7d-89ef-4aff-a5ee-15b6c836bbd5.pdf.

- Derechos Digitales. (4 de marzo de 2022). Costa Rica: elecciones entre denuncias, violación de datos personales y reformas de ley insuficientes. https://www.derechosdigitales.org/18043/costa-rica-elecciones-entre-denuncias-violacion-de-datos-personales-y-reformas-de-ley-insuficientes/

- Derechos Digitales (2023). Informe: Derechos humanos en entornos digitales en Nicaragua. https://www.derechosdigitales.org/nicaragua-2023-esp/#Abusos_y_vulneraciones_registradas/

- Deutsche Welle (DW). (18 de octubre de 2022). Nicaragua: detectan 39 falsas antenas que espían celulares. DW. https://www.dw.com/es/nicaragua-detectan-39-falsas-antenas-que-esp%C3%ADan-celulares/a-63468522

- Díaz, Marianne. (16 de agosto de 2018). Herramientas para seguir a la oposición en Guatemala. Derechos digitales. https://www.derechosdigitales.org/12385/herramientas-para-perseguir-a-la-oposicion-en-guatemala/

- Durón Chow, J. Ñancahuazú. (2005). Los ataques de la informática y la protección de datos personales en Nicaragua. Encuentro, (71), 30-53. https://doi.org/10.5377/encuentro.v0i71.4224

- Electronic Frontier Foundation. (2 de febrero de 2021). ¿Qué garantías legales existen en España y América latina si las fuerzas del orden quieren tus comunicaciones privadas? Electronic Frontier Foundation. https://www.eff.org/es/deeplinks/2021/02/when-law-enforcement-wants-your-private-communications-what-legal-safeguards-are

- Fundación Acceso (2020). Vigilancia en Centroamérica. Fundación Acceso. https://www.acceso.or.cr/wp-content/uploads/2021/08/2020-VigilanciaCA-28S.pdf

- Gavarrete, Julia. (17 de marzo de 2022). CIDH exige a El Salvador investigar espionaje contra periodistas y activistas. Elfaro. https://elfaro.net/es/202203/el_salvador/26074/CIDH-exige-a-El-Salvador-investigar-espionaje-contra-periodistas-y-activistas.htm

- Gordillo, Ivonne. (3 de agosto de 2020). Juzgado multa a Infornet y por comercialización de datos y pide al MP investigar posibles delitos. Publinews. https://www.publinews.gt/gt/noticias/2020/08/03/juzgado-multa-a-infornet.htmlhttps://www.publinews.gt/gt/noticias/2020/08/03/juzgado-multa-a-infornet.html

- Human Rights Watch. (2 de mayo de 2022). El Salvador: Evidencias de graves abusos durante el régimen de excepción. Human Rights Watch. https://www.hrw.org/es/news/2022/05/02/el-salvador-evidencias-de-graves-abusos-durante-el-regimen-de-excepcion

- Infobae. (13 de marzo de 2024). Daniel Ortega quiere imponer una ley que obliga a las telefónicas a suministrar información de sus usuarios en Nicaragua. Infobae. https://www.infobae.com/america/america-latina/2024/03/13/daniel-ortega-quiere-imponer-una-ley-que-obliga-a-las-telefonicas-a-suministrar-informacion-de-sus-usuarios-en-nicaragua/

- Infodemia. (4 de febrero de 2024). Es falso que no existan denuncias por vulneraciones a la prensa en El Salvador. Infodemia. https://twitter.com/andresguzm/status/1754139376563401212

- Marquis-Boire, Morgan, et al. (9 de julio de 2013). Some Devices Wander by Mistake: Planet Blue Coat Redux. Citizen Lab. https://citizenlab.ca/2013/07/planet-blue-coat-redux/

- Organización de Estados Americanos (OEA). (13 de abril de 2022). La Relatoría Especial alerta sobre riesgos de criminalización a ejercicios legítimos de la libertad de expresión en El Salvador a partir de reformas legislativas. [Comunicado de prensaR80/22]. https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1232&lID=2

- Oliva, David. (2021). ¿Qué sabemos sobre la intervención de llamadas telefónicas en el caso Tigo? Fundación Acceso. https://www.acceso.or.cr/2021/05/03/-que-sabemos-sobre-la-intervencion-de-llamadas-telefonicas-en-el-caso-tigo/

- Ortez, Kelly. (2023). Ley "SIM" violaría privacidad de ciudadanos y representaría futura misiva contra opositores. CriterioHN. https://criterio.hn/ley-sim-violaria-privacidad-de-ciudadanos-y-representaria-futura-misiva-contra-opositores/

- Pisanu, Gaspar. (2022). Más allá de Pegasus: Las amenazas de las nuevas políticas en el El Salvador. Access Now. https://www.accessnow.org/amenazas-politicas-el-salvador/

- Proceso digital. (16 de noviembre de 2015). ¿Solo el Estado escucha en Honduras? Proceso digital. https://proceso.hn/solo-el-estado-escucha-en-honduras/

- Rodríguez, Katitza, et al. (octubre 16 de 2018). Protecting Security Researchers' Rights in the Americas. Electronic Frontier Foundation. https://www.eff.org/coders-rights-americas

- Rodríguez, Milton. (5 de mayo de 2021). Bukele veta Ley de Protección de Datos Personales y otros decretos. El Salvador.com. https://historico.elsalvador.-com/historico/839543/nayib-bukele-veto-ley-proteccion-datos-personales.html

- Sancho, Manuel. (10 de mayo de 2014). Gobierno busca cambios en la DIS, una institución que pocos saben cómo funciona. CRHoy. https://archivo.crhoy.com/-gobierno-busca-cambios-en-la-dis-una-institucion-que-pocos-saben-como-funciona-w9l7m0x/nacionales/

- Sandoval, Williams. (1 de febrero de 2024). Agresiones contra periodistas se duplicaron durante 2023, según informe de la APES. La Prensa Gráfica. https://www.laprensagrafica.com/elsalvador/Agresiones-contra-periodistas-se-duplicaron-durante-2023-segun-informe-de-la-APES-20240201-0025.html

- Sas, Ángel y Orantes, Coralia. (2018). Espionaje ilegal del Gobierno: Aquí está la investigación de Nuestro Diario (Parte I) Nómada. https://nomada.gt/pais/la-corrupcion-no-es-normal/espionaje-ilegal-del-gobierno-aqui-esta-la-investigacion-de-nuestro-diario-parte-i/

- Scott-Railton, John, et al. (enero 12 de 2022). Project Torogoz Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware. Citizen Lab Report. https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/

- Silva, Ileana. (4 de marzo de 2022). Costa Rica: elecciones entre denuncias, violación de datos personales y reformas de ley insuficientes. Derechos Digitales. https://www.derechosdigitales.org/18043/costa-rica-elecciones-entre-denuncias-violacion-de-datos-personales-y-reformas-de-ley-insuficientes/

- Swissinfo. (17 de octubre de 2022). Organismo detecta 39 falsas antenas que espían celulares en Nicaragua. Swissinfo. https://www.swissinfo.ch/spa/organismo-detecta-39-falsas-antenas-que-esp%C3%ADan-celulares-en-nicaragua/47986222

- Hernández, Lía. (2020). Panorama de la Protección de Datos en Centroamérica. Adefinitivas. https://web.archive.org/web/20210116203020/https://adefinitivas.com/adefinitivas-internacional/proteccion-de-datos-en-centroamerica/

- Guatemala (2017). Guatecompras - Detalle de un concurso. http://www.guatecompras.gob.gt/concursos/consultaDetalleCon.aspx?o=5&nog=6557937

Sentencias:

- Sentencia de la Corte de Constitucionalidad dictada dentro del expediente número 1356-2006 el 11 de octubre de 2006 (Guatemala)

- Sentencias N.° 142-2012 y N.° 934-2007 de la Sala de lo Constitucional de la Corte Suprema de Justicia (El Salvador).

- Resolución de la Sala Constitucional de Costa Rica N.°3195, dictada el 20 de junio de 1995. (Costa Rica).

- Resolución N.° 032-2022 de 2018, de la Dirección Nacional de la Agencia de Protección de Datos de los Habitantes (Prodhab) de Costa Rica.

FUNDACIÓN Acceso

Fundacción Acceso

Informe sobre los marcos legales vigentes de Centroamérica en materia de vigilancia tecnológica, privacidad y datos personales

Teléfono: (506) 2253-9860
Correo electrónico: info@acceso.or.cr
San José, Costa Rica.

www.acceso.or.cr