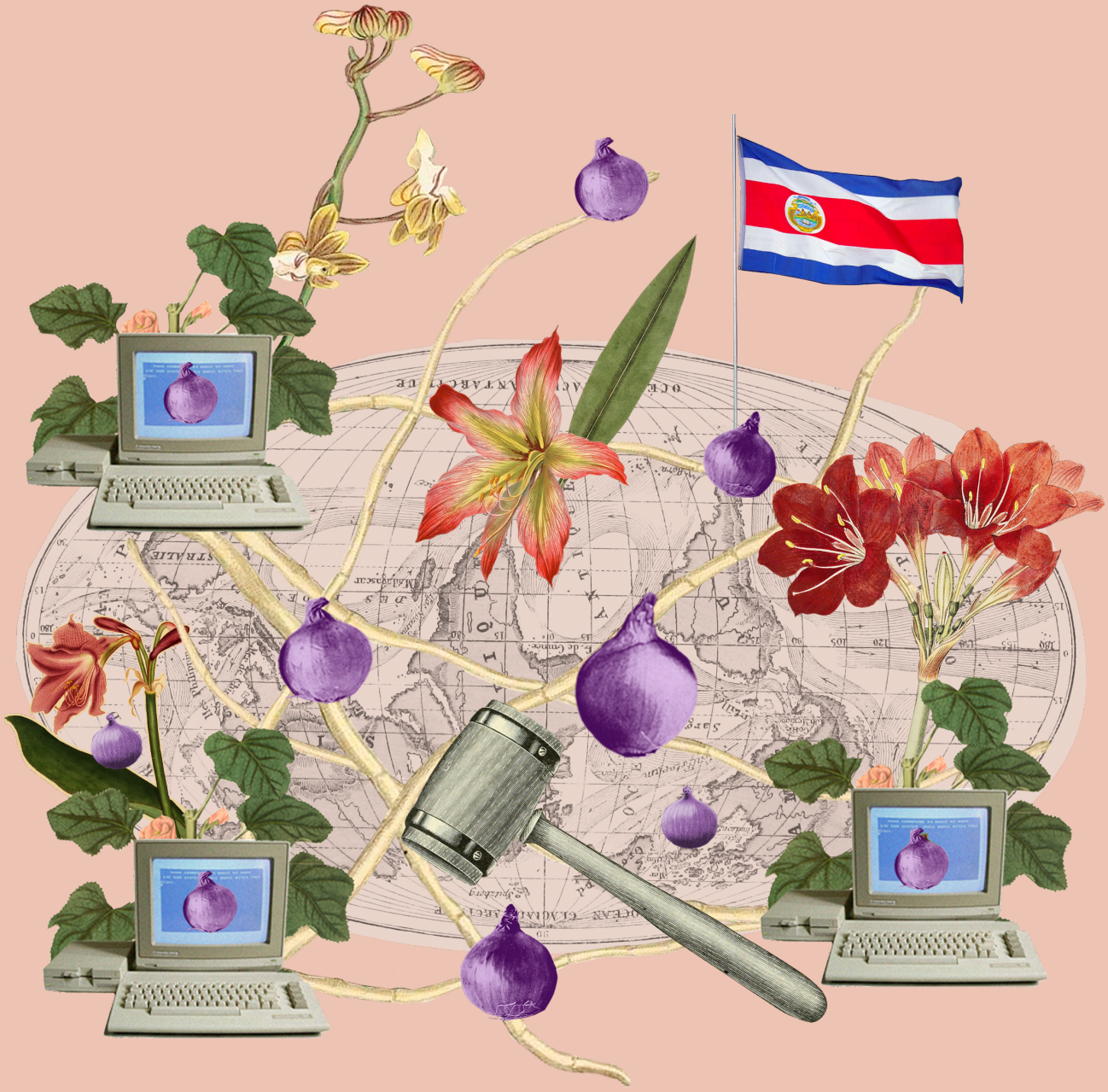
ANÁLISIS DEL MARCO LEGAL RELATIVO A LA OPERACIÓN Y USO DE HERRAMIENTAS DE PRIVACIDAD Y ANONIMATO EN COSTA RICA

ROBERTO LEMAÎTRE PICADO



DERECHOS DIGITALES
América Latina

ANÁLISIS DEL MARCO LEGAL RELATIVO A LA OPERACIÓN Y USO DE HERRAMIENTAS DE PRIVACIDAD Y ANONIMATO EN COSTA RICA

ROBERTO LEMAÎTRE PICADO

DERECHOS DIGITALES
América Latina

Portada y diagramación: Javiera Méndez
Correcciones por Sebastian Alburquerque
Noviembre de 2018.

Esta publicación fue posible gracias al apoyo de Open Technology Fund

Derechos Digitales es una organización independiente y sin fines de lucro, fundada en el año 2005 y cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital, desde el interés público. Entre sus principales ejes de interés está la defensa y promoción de la libertad de expresión, el acceso a la cultura y la privacidad.

Contenido

Introducción

En la actualidad, las nuevas tecnologías se han convertido en una herramienta esencial, y esta situación no ha sido la excepción en Costa Rica. Su uso masivo mediante computadoras, celulares inteligentes, y otros dispositivos, todos conectados a Internet, es una realidad palpable, siendo utilizadas diariamente y en todo momento por la mayoría de la sociedad costarricense.

Esta continua necesidad de estar conectados a la red genera beneficios, pero también importantes problemas. La cantidad masiva de nuestros datos expuestos de manera pública pone en riesgo nuestra seguridad virtual y física. Es por esta razón que los "ciberciudadanos" buscan opciones para proteger su información, y sobre todo su privacidad, concomitantemente su anonimato, es por este motivo que se buscan opciones técnicas que cumplan ese objetivo; entre las opciones más conocidas, y reconocidas, es la herramienta TOR.

TOR es el acrónimo de The Onion Router. Este es un software libre, que sirve como instrumento para evitar la censura de determinados contenidos que de otra forma se encontrarían bloqueados, además de buscar proteger la privacidad, intimidad y anonimato de las personas que lo utilizan en Internet.

Este tipo de herramientas enfrentan el reto de un mercado que busca que todos sean ubicados y ubicables, que nadie sea anónimo, y de marcos legales que no fueron pensados inicialmente para temas tecnológicos, pero que han tenido que adaptarse o interpretarse para seguir protegiendo derechos humanos como lo son la privacidad e intimidad de las personas

Es por esta razón que el presente análisis busca presentar el estado de la privacidad, intimidad, y anonimato en Costa Rica, frente al uso de herramientas técnicas, el estudio legal sobre los aspectos de la legislación que pueden afectar a su uso, y la distinta legislación en la materia que presenta el marco normativo costarricense, y su impacto y uso por parte de organismos judiciales.

Resumen

La evolución de las nuevas tecnologías ha generado una sociedad costarricense constantemente conectada a Internet, que, aunque genera grandes ventajas, también supone enormes riesgos para la privacidad e intimidad de las personas. Por ello, el uso de herramientas que busquen proteger los derechos de privacidad e intimidad constitucionalmente consagrados en Costa Rica es una necesidad real. Una de las herramientas más conocidas para este fin es el proyecto Tor, siendo un instrumento fundamental para la defensa de los derechos de los usuarios, anonimizando tanto a clientes como a servidores. Aunque estos avances también han favorecido al surgimiento de nuevos tipos de cibercriminalidad, el reto a nivel jurídico es seguir protegiendo la privacidad e intimidad de las personas, mientras, al mismo tiempo, equilibrar la balanza para en los casos de delitos poder actuar, siempre dentro del marco del debido proceso, los derechos constitucionales y derechos humanos que han marcado a Costa Rica en su actuar jurídico. Por lo tanto, resulta fundamental analizar el estado de la privacidad e intimidad en el país, el actuar judicial frente a estas herramientas, y la posibilidad del uso de las mismas por parte de la ciudadanía.

Cuando hablamos de derecho a la intimidad, lo relacionamos con conceptos como privacidad, secreto, inviolabilidad, anonimato; todos estos son parte del mismo derecho.

Podemos definirlo entonces como *"un derecho humano fundamental por virtud del cual se tiene la facultad de excluir o negar a las demás personas del conocimiento de ciertos aspectos de la vida de cada persona que solo a ésta le incumben"* (De Dienheim Bariguete).

Este derecho va a implicar dos momentos, uno activo y uno pasivo (Rojas Mora), los cuales los podemos definir como:

- La posibilidad que tiene cada persona de excluir ciertos aspectos de su vida del conocimiento e intervención de terceras personas.
- La obligación de terceras personas de respetar la esfera de privacidad y no actuar contra esta.

Asimismo, el Estado se encuentra en la obligación de asegurar a las personas ese derecho a la intimidad, según nuestra Constitución Política, lo que obliga directamente al Estado a velar por la privacidad de los ciudadanos, pero al mismo tiempo debe brindar instrumentos capaces de restituir la privacidad cuando haya sido violada, y los medios legales para sancionar a los que la afecten.

Al respecto, en nuestro marco normativo, la Constitución Política, en el artículo 24, se consagra el derecho a la intimidad, el cual busca garantizarle a todo individuo un sector personal, una esfera privada de su vida que sea inaccesible al público, salvo expresa voluntad de la persona, lo que denominamos autodeterminación informativa. Esta garantía protege la libertad de las comunicaciones y prohíbe que cualquier persona, pública o privada, pueda acceder a estos contenidos, de manera irrestricta. El artículo 24 de la Constitución Política de Costa Rica indica que: (Asamblea Legislativa de la República de Costa Rica, s.f.)

> *ARTÍCULO 24.- Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones.*
>
> *Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.*
>
> *(....).*
>
> *La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos.*
>
> *Una ley especial, aprobada por dos tercios del total de los Diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley se-*

ñale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión.

(...)". (Así reformado por ley N° 7607 de 29 de mayo de 1996).

Al respecto la Sala Constitucional ha sido clara en indicar que se protege el derecho a la intimidad, mediante sentencia número 2008-16336, de las diecisiete horas cincuenta y cinco minutos del treinta de octubre de dos mil ocho (SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA, 2008), señaló que:

"La Sala Constitucional, en múltiples ocasiones, ha desarrollado los alcances y matices del derecho protegido en el artículo 24 de la Constitución Política. Particularmente ilustrativo es lo resuelto por el Tribunal Constitucional en la sentencia N° 2005- 15063 de las 15:59 hrs. del 1° de noviembre de 2005, en que se dijo: "(…) EL SECRETO DE LAS COMUNICACIONES Y LA INVIOLABILIDAD DE LOS DOCUMENTOS PRIVADOS. El artículo 24 de la Constitución Política y el artículo 11 de la Convención Americana sobre Derechos Humanas consagran el derecho a la intimidad que, entre otras cosas, pretende garantizarle a todo individuo un sector personal, una esfera privada de su vida inaccesible a público salvo expresa voluntad del interesado. Como una de sus manifestaciones expresamente contempladas en la Constitución Política se encuentra la inviolabilidad de los documentos privados. Esta garantía protege la libertad de las comunicaciones y prohíbe que cualquier persona - pública o privada - pueda interceptar o imponerse del contenido, de manera antijurídica, de las comunicaciones ajenas.

Además, la Sala Constitucional, también ha señalado, en la sentencia No. 6776-94 de las 14:57 hrs. del 22 de noviembre de 1994, sobre el tema lo siguiente (SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA, 1994):

"El derecho a la intimidad tiene un contenido positivo que se manifiesta de múltiples formas, como por ejemplo: el derecho a la imagen, al domicilio y a la correspondencia. Para la Sala el derecho a la vida privada se puede definir como la esfera en la cual nadie puede inmiscuirse. La libertad de la vida privada es el reconocimiento de una zona de actividad que es propia de cada uno y el derecho a la intimidad limita la intervención de otras personas o de los poderes públicos en la vida privada de la persona; esta limitación puede manifestarse tanto en la observación y captación de la imagen y documentos en general, como en las escuchas o grabaciones de las conversaciones privadas y en la difusión o divulgación posterior de lo captado u obtenido sin el consentimiento de la persona afectada. Asimismo, el texto constitucional en su artículo 24 se refiere a la inviolabilidad de los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República", con lo cual, es evidente, que dicho derecho se refiere a cualquier procedimiento de comunicación privada con independencia de la titularidad del medio a través del cual se realiza la comunicación."

Este último aspecto, nos comienza a delimitar jurídicamente, que las comunicaciones no solo deben ser entendidas como la transmisión de datos por algún medio tecnológico, estas van a incluir la comunicación escrita, o digital, y va a tener la característica de ser considerada de índole privada.

Dicho marco normativo va a exigir, que, en caso de alguna revisión de las comunicaciones

de cualquier tipo, o de la información contenida en dispositivos digitales, deba existir un debido proceso, y mantener las garantías de intimidad de los elementos de índole privada, inclusive aunque sea un trabajador de una empresa o de una institución y le sea brindado los equipos tecnológicos por el patrono. Dicha posición queda reiterada en el voto de la Sala Constitucional en la resolución 2007-16586, donde se le dio la razón al patrono de la revisión que se realizó, fundamentado por lo siguiente (SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA, 2007):

> *"De los anteriores hechos probados no se desprende vulneración alguna de los derechos fundamentales del recurrente; por una parte, no se le ha vulnerado su derecho a la intimidad y a la inviolabilidad de documentos privados, por cuanto el proceso de revisión de archivos se realizó en la computadora que utiliza el amparado, como funcionario, en la Municipalidad de la Unión y no incluyó ni documentos ni su correo electrónico; esa revisión se realizó como consecuencia de una denuncia por presuntas irregularidades en perjuicio de la hacienda pública municipal y no se ha dirigido a verificar ningún extremo relativo a los archivos privados del recurrente; y no se ha dirigido a verificar ningún extremo relativo a los archivos privados del recurrente; la revisión ha sido realizada por la auditoría municipal, la cual se encuentra facultada al efecto por ley formal (art. 33 de la Ley de Control Interno) y la revisión se realizó con el consentimiento y presencia del recurrente. Por tanto: Se declara sin lugar el recurso*" (Resaltado no es del Original).

Ahora bien, nuestro marco normativo en materia de privacidad e intimidad es bastante amplio, incluyendo leyes, reglamentos, tratados y acuerdos internacionales que pasamos a describir:

Declaración Universal de los Derechos Humanos

Costa Rica es parte de la Declaración Universidad de los Derechos Humanos (Organización de Naciones Unidas, 1948), la cual en su artículo 12 establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación y que toda persona tiene derecho a la protección de la ley contra esas injerencias o ataques.

Pacto Internacional de Derechos Civiles y Políticos

De igual forma, Costa Rica forma parte del Pacto Internacional de Derechos Civiles y Políticos (Asamblea Legislativa, 1968), el cual en su artículo 17 establece las mismas disposiciones que el artículo 12 de la Declaración Universal de los Derechos Humanos y en su artículo 19, al referirse a la libertad de expresión, la cual señala que la misma genera deberes y responsabilidades especiales por lo que podrá estar sujeto a ciertas restricciones fijadas por la ley y que sean necesarias para asegurar el respeto a los derechos o a la reputación de los demás, así como para proteger la seguridad nacional, el orden público, la salud o moral públicas.

Convención Americana sobre Derechos Humanos Pacto de San José

Costa Rica como país sede, y parte firmante, de la Convención Americana sobre Derechos Humanos (Asamblea Legislativa, 1970), se estableció, en el artículo 11, que toda persona

tiene derecho al respeto de su honra y al reconocimiento de su dignidad y que por tanto no deberá ser objeto de injerencias arbitrarias o abusivas en su vida privada, familia, domicilio, correspondencia, ni deberá sufrir ataques ilegales a su honra o reputación. Y establece también el derecho de la persona a ser protegida por la ley contra esas injerencias o ataques.

El artículo 13 establece la libertad de pensamiento y expresión determinando que no deberá existir previa censura, pero que el ejercicio de esos derechos estará sujeto a responsabilidades ulteriores, mismas que deberán estar expresamente fijadas por la ley y que deberán tender a asegurar entre otras cuestiones, el respeto a los derechos o a la reputación de los demás.

Convención sobre los Derechos del Niño

La Convención sobre los Derechos del Niño (Asamblea Legislativa, 1990), en su artículo 16, menciona que ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o a su reputación; y que el niño tiene derecho también a la protección de la ley contra esas injerencias y ataques.

Ley General de Telecomunicaciones

La Ley General de Telecomunicaciones (Asamblea Legislativa, 2008) establece en el Capítulo II denominado *Régimen de protección a la intimidad y derechos del usuario fina*l, el régimen de privacidad y de protección de los derechos e intereses de los usuarios de los servicios de telecomunicaciones en materia de protección de la privacidad e intimidad.

El artículo 41 de la citada normativa, deja claramente establecido que le corresponde a la Superintendencia de Telecomunicaciones (SUTEL) velar por que los operadores y proveedores efectivamente cumplan su deber de proteger los datos de sus clientes. Al respecto señala dicho artículo:

> *Artículo 41.- Régimen jurídico*
>
> *El presente capítulo desarrolla el régimen de privacidad y de protección de los derechos e intereses de los usuarios finales de los servicios de telecomunicaciones. Los acuerdos entre operadores, lo estipulado en las concesiones, autorizaciones y, en general, todos los contratos por servicios de telecomunicaciones que se suscriban de conformidad con esta Ley, tendrán en cuenta la debida protección de la privacidad y los derechos e intereses de los usuarios finales. A la Sutel le corresponde velar por que los operadores y proveedores cumplan lo establecido en este capítulo y lo que reglamentariamente se establezca.*

Dicho artículo deja claro que debe existir un reglamento que desarrolle cómo debe ser este cumplimiento del régimen de protección de la privacidad de los usuarios de telecomunicaciones, al respecto ampliaremos más adelante.

El artículo 42 del mismo marco normativo, establece los deberes que deben cumplir los operadores de redes públicas y proveedores de servicios de telecomunicaciones. Dicho numeral señala que los operadores deberán garantizar el secreto de las comunicaciones, el derecho a la intimidad y la protección de los datos de carácter personal de los abonados

y usuarios finales, mediante la implementación de los sistemas y las medidas técnicas y administrativas necesarias. Estas medidas de protección serán fijadas reglamentariamente por el Poder Ejecutivo.

Es importante manifestar que los datos de carácter personal son en general cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. (Agencia Española de Protección de Datos, 2017).

Resulta interesante resaltar, que el mismo artículo obliga a los operadores y proveedores de telecomunicaciones a informar en caso de un riesgo que se haya generado en la seguridad de sus sistemas o redes y deberá informar a la SUTEL y a los usuarios finales sobre dicho riesgo.

De igual forma, impone el deber de proteger cualquier de las comunicaciones y datos que se generen en sus redes de sus clientes o usuarios con relación a terceros, siempre con la excepción del consentimiento que pueda brindar el usuario para transferir estos datos a terceros o por autorización judicial.

Decreto N. 35205-MINAET del 16 de abril del 2009, publicado en La Gaceta del 18 de mayo del 2009, Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones

Desde su artículo 1, el Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones (Asamblea Legislativa, 2009) deja muy claro que responde a la necesidad de reglamentar el Capítulo II.- Régimen de protección a la intimidad y derechos del usuario final, presente en la Ley General de Telecomunicaciones citado anteriormente

> *Artículo 1.- Objeto del Reglamento.*
>
> *El presente reglamento tiene por objeto establecer las disposiciones reglamentarias, sobre las medidas de protección a la privacidad y confidencialidad de las comunicaciones, derivadas del capítulo II del título II de la Ley General de Telecomunicaciones (Ley N° 8642).*

Este reglamento es de acatamiento obligatorio para todos los operadores o proveedores de servicios de telecomunicaciones que usen y exploten redes públicas de telecomunicaciones, independientemente del tipo de red, de conformidad con el artículo 2 de citado reglamento.

Al respecto, el artículo 4 establece los fines del reglamento, siendo uno de los principales, y para efectos de la investigación, la privacidad e intimidad de los usuarios de los servicios de telecomunicaciones:

> *Artículo 4º-De los fines. El presente Reglamento tiene entre sus fines:*
>
> *a) Garantizar el secreto de las comunicaciones, el derecho a la intimidad y la protección de los datos de carácter personal de los abonados y usuarios.*
>
> *b) Promover que los proveedores y operadores de servicios de telecomunicaciones adopten medidas técnicas y administrativas que preserven la seguridad de sus servicios.*
>
> *c) Garantizar que la información de los abonados que se suministra para las guías de abonados y los recibos telefónicos, sea congruente con los principios de privacidad y confidencialidad de la información, así como que dicha información no sea divulgada ni utilizada con fines comerciales.*

d) Asegurar que los datos de tráfico y de localización relacionados con los usuarios finales, sean tratados y almacenados bajo rigurosos estándares de seguridad, así como que estos sean eliminados o anónimos cuando ya no sean, necesarios a efectos de la transmisión de una comunicación o para la prestación de un servicio.

e) Promover que la utilización de sistemas de llamadas automáticas por voz, fax, correo electrónico o cualquier otro dispositivo con fines de venta directa, se realice conforme a los términos de la legislación vigente.

Es importante indicar que este reglamento responde a temas de índole jurídico y técnico, que puede en algunos aspectos generar dudas, por lo que debe ser visto de manera integral. Uno de los puntos que quisiera resaltar y explicar, es las medidas de seguridad, el artículo 7 del citado reglamento no indica las medidas técnicas explicitas, solamente señala aspectos generales, como, por ejemplo:

Los proveedores y operadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y administrativas adecuadas para preservar la seguridad de sus servicios

Para tales efectos, los operadores o proveedores deberán considerar las técnicas más avanzadas a fin de garantizar un nivel de seguridad adecuado al riesgo existente

En este caso la Superintendencia de Telecomunicaciones tiene el marco normativo, tanto por ley y reglamento, para poder actuar en pro de la protección de la privacidad e intimidad de las personas y de sus datos personales frente las empresas proveedores de servicios de telecomunicaciones que no cumplan la normativa.

Ley No. 8968 Protección de la Persona frente al Tratamiento de sus Datos Personales y su Reglamento

Mediante Ley N° 8968 de 7 de julio del 2011 y publicada en el Diario Oficial La Gaceta No. 170 del 5 de setiembre del 2011, se promulgó la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales (Asamblea Legislativa, 2011), y su Reglamento el cual fue creado mediante Decreto Ejecutivo No. 37554-JP del 30 de octubre del 2012 y publicado en el Alcance No. 45 del Diario Oficial La Gaceta del 5 de marzo del 2013 y reformado en el 2016 mediante el Decreto Ejecutivo No. 40008-JP del 19 de julio del 2016 y publicado en el Alcance No. 287 del Diario Oficial La Gaceta del 6 de diciembre del 2016 (Asamblea Legislativa, 2016).

Dicha normativa busca garantizar a cualquier persona, independientemente 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 bases de datos automatizadas o manuales, de organismos públicos o privados.

Además, se crea la Agencia de Protección de Datos de los Habitantes, donde los ciudadanos que consideren vulnerados sus derechos en cuanto uso de sus datos personales pueden 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.

Reglamento sobre la limitación a la responsabilidad de los proveedores de servicios por infracciones a derechos de autor y conexos de acuerdo con el artículo 15.11.27 del Tratado de Libre Comercio República Dominicana-Centroamérica- Estados Unidos

Este reglamento (Poder Ejecutivo, 2011), se genera dentro del marco del Tratado de Libre Comercio República Dominicana-Centroamérica- Estados Unidos, y tiene como objetivo dos aspectos:

a. *Las medidas colaborativas de los proveedores de servicios con los titulares de derechos de autor y conexos en disuadir el almacenaje y transmisión no autorizada de materiales protegidos por derechos de autor y derechos conexos;*

b. *La limitación a la responsabilidad de los proveedores de servicios por infracciones a derechos de autor o derechos conexos que no estén en su control, ni que hayan sido iniciadas o dirigidas por ellos, y que ocurran a través de sistemas o redes controladas u operadas por ellos, o en su representación.*

Es importante indicar que este reglamento será aplicable a los proveedores de servicios que voluntariamente se sometan a éstas y establezcan medidas colaborativas, razonables y proporcionales con los titulares de derechos de autor y conexos para atender posibles infracciones por el uso no autorizado de materiales protegidos por tales derechos, de conformidad con las siguientes regulaciones y el Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos.

Para los efectos de privacidad el reglamento establece dos artículos que son importantes tener presentes, tanto en materia de limitación de responsabilidad como de monitoreo de la red:

> *Artículo 4º—De la limitación a la responsabilidad de los Proveedores de Servicios. Los proveedores de servicios no serán sujetos a reparaciones pecuniarias cuando hayan cumplido con las condiciones comprendidas en los artículos 6 al 10 del presente Reglamento frente a casos de infracciones cometidas contra los derechos de autor y conexos que ocurran a través de sistemas o redes controladas u operadas por éstos o en su representación, según corresponda a la naturaleza del servicio prestado. Los proveedores de servicios solamente podrán ser objeto de las medidas correctivas que así determine la autoridad judicial competente, de conformidad con lo establecido en el artículo 15.11.27 del Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos, Ley de Aprobación Nº 8622 del 21 de noviembre del 2007.*
>
> *Artículo 5º—No obligación de monitoreo. Bajo ninguna circunstancia se condicionará la aplicación de la limitación a la responsabilidad a que el proveedor de servicios deba realizar controles de su servicio o que, decididamente, deba buscar hechos que indiquen una posible actividad infractora, excepto en la medida en que éstos sean coherentes con las medidas tecnológicas efectivas aplicadas. Lo anterior se entenderá sin perjuicio de cualquier orden emitida por la autoridad judicial competente, la cual se decrete para investigar, detectar o perseguir delitos o prácticas constitutivas de ejercicios abusivos de los derechos de autor o conexos reconocidos por la legislación nacional.*

En dicho contexto el mismo reglamento establece las condiciones de cómo los proveedores de servicios pueden beneficiarse de las limitaciones de responsabilidad, para lo cual deberán cumplir con las siguientes condiciones generales de conformidad con el artículo 6 del citado Reglamento:

a. *Establecer e implementar políticas mediante las cuales se establezcan las causas por las que se daría término a las cuentas o la resolución del contrato de aquellos usuarios calificados como infractores reincidentes de los derechos protegidos por la Ley de Derechos de Autor y Derechos Conexos.*

b. *Adaptar y no interferir con las medidas tecnológicas efectivas y de gestión de derechos de autor y derechos conexos generalmente utilizadas para proteger tales derechos, siempre que éstas estén disponibles en términos razonables y no discriminatorios, y que no impongan costos sustanciales a los proveedores de servicios ni cargas significativas a sus sistemas o redes.*

La normativa establece que en los casos que exista alguna afectación a los derechos de autor, y de conformidad con las disposiciones establecidas en la Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual y legislación conexa, sin perjuicio de las acciones y procedimientos judiciales que les asisten, los titulares de derechos de autor o derechos conexos o su representante, que consideren que sus derechos han sido infringidos en sistemas controlados u operados por un Proveedor de Servicios, podrán enviar una comunicación a dicho proveedor. Y éste contará con un plazo prudencial y razonable no mayor a quince días naturales para determinar si requiere información adicional del titular del derecho, y luego deberá comunicarla inmediatamente al usuario o proveedor del supuesto material infractor, acompañando dicha comunicación de los antecedentes proporcionados por el titular del derecho o su representante y un lugar o medio para recibir notificaciones, todo dentro de un plazo razonable que no exceda los treinta días naturales contados desde la recepción de la comunicación original.

Bajo este escenario el presunto infractor tendrá dos opciones.

a. *Retirar voluntariamente el material presuntamente infractor, lo cual podrá comunicar al proveedor de servicios o al titular del derecho infringido o su representante, o bien salvo mejor derecho;*

b. *Presentar una contestación que deberá contener, mutatis mutandis, la información de descargo indicada en el artículo anterior.*

En los casos en que el presunto infractor no responda o no se refiera al caso, el proveedor de servicios podrá proceder a la terminación de cuentas específicas o la adopción de medidas efectivas para retirar o inhabilitar el acceso a un determinado contenido supuestamente infractor, de conformidad con las políticas que haya emitido e implementado al efecto.

Es importante señalar, y reiterar, que esta normativa se dirige a los infractores de derechos de autor y busca un equilibrio para quienes provean servicios de Internet y para los usuarios de la propiedad intelectual, ya que se establecen medidas para que se respeten los derechos y hacer reclamos. A la vez, esta normativa no exige a los proveedores de servicios de Internet que realicen un monitoreo de los materiales que suben a la red los usuarios. Además, la normativa exige que el supuesto infractor deba ser notificado, y mediante un debido proceso tiene la oportunidad de corregir o acudir a los tribunales.

Ley N° 9048 y sus reformas Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal

En materia de delitos informáticos la reforma del Código Penal (Asamblea Legislativa, 2014) en el 2012-2013, creó figuras referentes a la protección de la intimidad y privacidad de las comunicaciones y de los datos personales, en este sentido encontramos tres artículos fundamentales; violación de comunicaciones, violación de datos personales y suplantación de identidad:

> *Artículo 196.- Violación de correspondencia o comunicaciones.*
>
> *Será reprimido con pena de prisión de uno a tres años a quien, con peligro o daño para la intimidad o privacidad de otro, y sin su autorización, se apodere, acceda, modifique, altere, suprima, intervenga, intercepte, abra, entregue, venda, remita o desvíe de su destino documentación o comunicaciones dirigidas a otra persona.*
>
> *La misma sanción indicada en el párrafo anterior se impondrá a quien, con peligro o daño para la intimidad de otro, utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público.*
>
> *La misma pena se impondrá a quien promueva, incite, instigue, prometa o pague un beneficio patrimonial a un tercero para que ejecute las conductas descritas en los dos párrafos anteriores.*
>
> *La pena será de dos a cuatro años de prisión si las conductas descritas en el primer párrafo de este artículo son realizadas por:*
>
> *a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.*
>
> *b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.*
>
> *(Reformado por el artículo 1° de la ley N° 9135 del 24 de abril de 2013. Publicado en el Alcance N° 78 a la Gaceta N° 80 del 26 de abril del 2013)*
>
> *Artículo 196 bis.- Violación de datos personales.*
>
> *Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.*
>
> *La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:*
>
> *a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.*
>
> *b) La información vulnerada corresponda a un menor de edad o incapaz.*

c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley.

Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley."

(Adicionado por Ley N° 8148 de 24 de octubre del 2001 y posteriormente reformado en la forma indicada por el artículo 1° de la ley N° 9135 del 24 de abril de 2013. Publicada en el Alcance N° 78 a la Gaceta N° 80 del 26 de abril del 2013)

Artículo 230.- Suplantación de identidad.

Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información.

(Adicionado por el artículo 3° de la Ley N° 9048 del 10 de julio de 2012, "Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal")

(Reformado por el artículo 1° de la ley N° 9135 del 24 de abril de 2013. Publicado en el Alcance N° 78 a la Gaceta N° 80 del 26 de abril del 2013)

Es importante señalar, que el marco de privacidad e intimidad que tiene el país tiene una relación directa con el anonimato, y por tanto guardar o proteger la identidad, se enmarca dentro del derecho a la privacidad e intimidad que tiene todo ciudadano costarricense.

La excepción a este derecho se genera cuando la persona aproveche su derecho al anonimato, o a utilizar un seudónimo, con un fin delictual. Un ejemplo muy claro lo tenemos en nuestro código penal en el delito de Seducción o encuentros con menores por medios electrónicos, el cual señala que:

Artículo 167 bis.- Seducción o encuentros con menores por medios electrónicos.

Será reprimido con prisión de uno a tres años a quien, por cualquier medio, establezca comunicaciones de contenido sexual o erótico, ya sea que incluyan o no imágenes, videos, textos o audios, con una persona menor de quince años o incapaz.

La misma pena se impondrá a quien suplantando la identidad de un tercero o mediante el uso de una identidad falsa, por cualquier medio, procure establecer comunicaciones de contenido sexual o erótico, ya sea que se incluyan o no imágenes, videos, textos o audios, con una persona menor de edad o incapaz.

La pena será de dos a cuatro años, en las conductas descritas en los dos párrafos anteriores, cuando el actor procure un encuentro personal en algún lugar físico con una persona menor de edad incapaz.

(Adicionado por el artículo 2° de la ley N° 9135 del 24 de abril de 2013. Publicado en el Alcance N° 78 a la Gaceta N° 80 del 26 de abril del 2013)

En este caso el uso de la identidad falsa o el anonimato, al ser utilizado para este fin delictivo, deja de tener una protección del Estado y más bien genera que el aparato judicial persiga a esta persona.

Ley de Procedimientos de Observancia de Derechos de Propiedad Intelectual N. 8039 del 12 de octubre del 2000. La Gaceta del 27 de octubre del 2000.

Para los fines del estudio, es importante indicar que ante la violación de cualquier derecho sobre la propiedad intelectual, se dará lugar al ejercicio de las acciones administrativas ejercidas ante el Registro de la Propiedad Industrial o el Registro Nacional de Derechos de Autor y Derechos Conexos y de las acciones judiciales por medio de la Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual (Asamblea Legislativa, 2018). Cuando se den acciones tecnológicas que afecten los derechos de propiedad intelectual, los artículos 62 y 62 bis indican lo siguiente:

> *Artículo 62.- Alteración, evasión, supresión, modificación o deterioro de las medidas tecnológicas efectivas contra la reproducción, el acceso o la puesta a disposición del público de obras, interpretaciones o ejecuciones, o fonogramas.**
>
> *Será sancionado con prisión de uno a cinco años o multa de cinco a quinientos salarios base, quien, de cualquier forma, altere, evada, suprima, modifique o deteriore medidas tecnológicas efectivas de cualquier naturaleza que controlen el acceso a obras, interpretaciones o fonogramas u otra materia objeto de protección.*
>
> *No se impondrán sanciones penales en las conductas indicadas, cuando estas sean realizadas por funcionarios de bibliotecas, archivos, instituciones educativas u organismos públicos de radiodifusión no comerciales sin fines de lucro, en el ejercicio de sus funciones.*
>
> *Cualquier acto descrito en el primer párrafo anterior constituirá una acción civil o un delito separado, independiente de cualquier violación que pudiera ocurrir según la Ley de derechos de autor y derechos conexos.*
>
> *Unicamente las siguientes actividades no serán punibles, siempre y cuando no afecten la adecuación de la protección legal o la efectividad de los recursos legales contra la evasión de medidas tecnológicas efectivas:*
>
> *a) Actividades no infractoras de ingeniería inversa respecto de la copia obtenida legalmente de un programa de computación, con respeto a los elementos particulares de dicho programa de computación que no han estado a disposición de la persona involucrada en esas actividades, con el único propósito de lograr la interoperabilidad de un programa de computación creado independientemente con otros programas.*
>
> *b) Actividades de buena fe no infractoras realizadas por un investigador debidamente calificado que haya obtenido legalmente una copia, ejecución o muestra de obra, interpretación o ejecución no fijada, o un fonograma y que haya hecho un esfuerzo por obtener autorización para realizar dichas actividades, en la medida necesaria y con el único propósito de identificar y analizar fallas y vulnerabilidades de las tecnologías para codificar y descodificar la información.*
>
> *c) La inclusión de un componente o parte, con el fin único de prevenir el acceso de meno-*

res a contenido inapropiado, en línea, de una tecnología, producto, servicio o dispositivo que por sí mismo no está prohibido.

d) Actividades de buena fe no infractoras, autorizadas por el propietario de una computadora, sistema o red de cómputo, realizadas con el único propósito de probar, investigar o corregir la seguridad de esa computadora, sistema o red de cómputo.

e) El acceso por parte de funcionarios de una biblioteca, un archivo o una institución educativa, sin fines de lucro, a una obra, interpretación o ejecución, o fonograma al cual no tendrían acceso de otro modo, con el único propósito de tomar decisiones sobre adquisiciones.

f) Actividades no infractoras, con el único fin de identificar y deshabilitar la capacidad de compilar o diseminar información de datos de identificación personal no divulgada que reflejen las actividades en línea de una persona natural, de manera que no afecte, de ningún otro modo, la capacidad de cualquier persona de obtener acceso a cualquier obra.

g) Actividades legalmente autorizadas, ejecutadas por empleados, agentes o contratistas gubernamentales para implementar la ley, cumplir funciones de inteligencia, defensa nacional, seguridad esencial o propósitos gubernamentales similares.

**Reformado por el artículo 1° aparte e) de la Ley 8656 de 18 de julio de 2008.*

Artículo 62 bis.-

*Fabricación, importación, distribución, ofrecimiento o tráfico de dispositivos, productos, componentes o servicios para la evasión de medidas tecnológicas efectivas contra la comunicación, la reproducción, el acceso, la puesta a disposición del público o la publicación de obras, interpretaciones o ejecuciones o fonogramas.**

Será sancionado con prisión de uno a cinco años o multa de cinco a quinientos salarios base, quien fabrique, importe, distribuya, ofrezca al público, proporcione o de otra manera trafique dispositivos, productos o componentes, u ofrezca al público o proporcione servicios, los cuales:

i) Sean promocionados, publicitados o comercializados con el fin de evadir una medida tecnológica efectiva.

ii) Sean diseñados, producidos o ejecutados principalmente con el fin de permitir o facilitar la evasión de una medida tecnológica efectiva.

La pena también se aplicará a quien fabrique, importe, distribuya, ofrezca al público, proporcione o de otra manera trafique dispositivos, productos, componentes u ofrezca al público o proporcione servicios que tengan, únicamente, un limitado propósito o uso de importancia comercial diferente del de evadir una medida tecnológica efectiva.

No se impondrá sanción penal en las conductas indicadas, cuando sean realizadas por funcionarios de bibliotecas, archivos e instituciones educativas sin fines de lucro u organismos públicos de radiodifusión no comerciales sin fines de lucro, en el ejercicio de sus funciones.

Con respecto a productos, servicios o dispositivos que evadan medidas tecnológicas efectivas que protejan cualquiera de los derechos de autor o conexos exclusivos en una obra,

interpretación o ejecución, o fonograma, únicamente las siguientes actividades no serán punibles, siempre y cuando no afecten la adecuación de la protección legal o la efectividad de los recursos legales contra la evasión de medidas tecnológicas efectivas:

a) Las actividades no infractoras de ingeniería inversa, respecto a la copia obtenida legalmente de un programa de computación, realizado de buena fe con respeto a los elementos particulares de dicho programa de computación que no han estado a disposición de la persona involucrada en esas actividades, con el único propósito de lograr la interoperabilidad de un programa de computación creado independientemente con otros programas.

b) Las actividades legalmente autorizadas, ejecutadas por funcionarios, agentes o contratistas de la Administración Pública o del Sector Público para implementar la ley, cumplir funciones de inteligencia, seguridad esencial o propósitos gubernamentales similares.

Con respecto a productos, servicios o dispositivos que evadan medidas tecnológicas efectivas que controlen el acceso a una obra, interpretación o ejecución, o fonograma protegidos, únicamente las siguientes actividades no serán punibles, siempre y cuando no afecten la adecuación de la protección legal o la efectividad de los recursos legales contra la evasión de medidas tecnológicas efectivas:

i) Las actividades no infractoras de ingeniería inversa, respecto a la copia obtenida legalmente de un programa de computación, realizado de buena fe con respeto a los elementos particulares de dicho programa de computación que no han estado a disposición de la persona involucrada en esas actividades, con el único propósito de lograr la interoperabilidad de un programa de computación creado independientemente con otros programas.

ii) Las actividades legalmente autorizadas, ejecutadas por funcionarios, agentes o contratistas de la Administración Pública o del Sector Público para implementar la ley, cumplir funciones de inteligencia, seguridad esencial o propósitos gubernamentales similares.

iii) Las actividades de buena fe no infractoras, realizadas por un investigador debidamente calificado que haya obtenido legalmente una copia, ejecución o muestra de obra, interpretación o ejecución no fijada, o fonograma, y que haya hecho un esfuerzo de buena fe por obtener autorización para realizar dichas actividades, en la medida necesaria, y con el único propósito de identificar y analizar fallas y vulnerabilidades de las tecnologías para codificar y decodificar la información.

iv) La inclusión de un componente o parte, con el fin único de prevenir el acceso de menores a contenido inapropiado en línea en una tecnología, producto, servicio o dispositivo que, por sí mismo, no esté prohibido en este artículo.

v) Las actividades de buena fe no infractoras autorizadas por el propietario de una computadora, sistema o red de cómputo, realizadas con el único propósito de probar, investigar o corregir la seguridad de esa computadora, sistema o red de cómputo.

**Adicionado por el artículo 2° aparte d) de la Ley 8656 de 18 de julio de 2008.*

También es sustancial acotar, que Costa Rica no cuenta con una regulación específica que regule la operación y uso de herramientas para proteger la privacidad y el anonimato en el país. Las personas pueden usar las herramientas que consideren que protejan su privacidad e intimidad, y más bien, como hemos visto en nuestro marco normativo, es un derecho

constitucional el poder ejercer el derecho a la privacidad e intimidad, tanto en el mundo físico como en el virtual.

Pero, en los casos en que se deba actuar judicialmente, siempre respetando el debido proceso y los derechos humanos que atraviesa todo nuestro marco normativo, en nuestro país existe la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones, la cual viene a regular la posibilidad de intervenir en el ámbito de intimidad de las personas que otorga al Estado el artículo 24 de la Constitución Política, bajo dos escenarios:

a. el registro, secuestro y examen de documentos privados y

b. la intervención de las comunicaciones privadas.

El artículo 9 de la referida ley sobre intervención de las comunicaciones dice:

> *Artículo 9.- Autorización de las intervenciones. Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de las comunicaciones orales, escritas, o de otro tipo…*

Esto quiere decir que la autoridad judicial correspondiente puede ordenar la intervención de las comunicaciones, siendo que estos dos escenarios varían en el momento en que se realizan y el conocimiento de los interesados. En los casos de secuestro de los documentos, el receptor de los mismos ya los tiene en su poder y es conocedor de que la autoridad judicial requiere de los mismos, mientras que la intervención se da antes de que el receptor reciba el documento y no conoce el hecho de que está siendo intervenido. Esta intervención incluye la posibilidad de intervenir las comunicaciones de carácter digital.

La acción penal en materia de intervención de las comunicaciones

Es importante indicar que el derecho penal tiene el carácter de *ultima ratio* y solamente se busca aplicar bajo el escenario de situaciones que afecten de tal forma a los ciudadanos que socialmente se considera que se requiere de la intervención del régimen represivo máximo.

En este escenario, Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones (Asamblea Legislativa, 2002) establece los parámetros para poder actuar

El artículo 1 de la citada normativa señala que:

> *ARTICULO 1.- Competencia.*
>
> *Los Tribunales de Justicia podrán autorizar el registro, el secuestro o el examen de cualquier documento privado, cuando sea absolutamente indispensable para esclarecer asuntos penales sometidos a su conocimiento. Para los efectos de esta Ley, se consideran documentos privados: la correspondencia epistolar, por fax, télex, telemática o cualquier otro medio; los videos, los casetes, las cintas magnetofónicas, los discos, los disquetes, los escritos, los libros, los memoriales, los registros, los planos, los dibujos, los cuadros, las radiografías, las fotografías y cualquier otra forma de registrar información de carácter privado, utilizados con carácter representativo o declarativo, para ilustrar o comprobar algo.*

Este artículo genera la posibilidad de que la autoridad jurisdiccional pueda ordenar el registro, secuestro o examen de un documento privado cuando lo crea necesario y, además crea una lista no taxativa de qué se considerará como documento privado.

De igual forma, el artículo 2 de ley de marras les brinda a los jueces de Costa Rica potestad de ordenar el registro o secuestro de los documentos privados, siempre limitada a los principios de racionalidad y proporcionalidad; lo cual limita al juez a que deban existir elementos suficientes de que ocurrió un delito y que el imputado pueda estar involucrado. En dado caso que deba registrar o secuestrar documentos privados solamente deban revisarse o secuestrarse aquellos documentos que tengan relación con la causa investigada.

> *Artículo 2.- Atribuciones del juez.*
>
> *Cuando resulte indispensable para averiguar la verdad, el Juez podrá ordenar, de oficio, a petición de la autoridad policial a cargo de la investigación, del Ministerio Público o de alguna de las partes del proceso, el registro, el secuestro y el examen de cualquier documento privado, siempre que pueda servir como prueba indispensable de la comisión de alguna conducta delictiva. El Juez realizará personalmente la diligencia, salvo en casos de excepción, en los que, según su criterio, pueda ser delegada en miembros del Organismo de Investigación Judicial o del Ministerio Público, quienes deberán informarle sobre el resultado de la diligencia.*

Al respecto, la Sala Constitucional en su voto Nº 6273-96 (SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA, 1996), ha señalado que:

> "No obstante que los derechos fundamentales pueden estar sujetos a determinadas restricciones, éstas resultan legítimas únicamente cuando son necesarias para hacer posible la vigencia de los valores democráticos y constitucionales, por lo que además de "necesaria", "útil", "razonable" u "oportuna", la restricción debe implicar la existencia de una necesidad social imperiosa que la sustente…"

El artículo 3 de la ley de rito señala:

> *Artículo 3.- Requisitos de la orden de secuestro, registro o examen.*
>
> *La orden de secuestro, registro o examen deberá efectuarse, so pena de nulidad, mediante auto fundado en el que se individualicen, de ser posible, los documentos sobre los que se ejecutará la medida de registro, secuestro o examen, el nombre de la persona que los tenga en su poder y el lugar donde se encuentran.*
>
> *De ser secuestrados otros documentos que no se incluyan en la orden, deberán restituirse inmediatamente a quien se le secuestraron, salvo que el Juez los estime trascendentales para esa u otra investigación; si así fuera, el Juez deberá ampliar la orden para incluirlos y justificar el motivo por el cual se incluyeron.*

Este artículo refleja la protección jurídica del debido proceso para estas acciones, iniciando que debe existir un auto debidamente fundamentado que autorice el secuestro, registro o examen de la información. Esto en razón que una acción como esta pone en peligro una serie de derechos humanos: intimidad, autodeterminación informativa, etc., por lo que debe ser realizada cumpliendo con un procedimiento antes y después de su recolección para así poder garantizar el respeto a estos derechos. Por eso en todo el proceso vamos a tener un

juez que vele por dicho cumplimiento, siendo necesario que exista la firme convicción de que la información que se pueda obtener ayudará a los fines de la investigación, así como prueba, por lo menos a nivel de indicios razonables que den pie a la creencia de que la persona a quien se le va a invadir su privacidad tiene algo que ver con el caso a resolver

Es importante recordar que todos estos derechos no tienen un carácter absoluto y pueden ser limitados de acuerdo a la existencia de una necesidad social imperativa, como es el caso de las acciones judiciales, en pro de la búsqueda de la culpabilidad o no de un imputado, pero esto implica que dicho proceso sea legalmente establecido, brindando las herramientas de defensa al imputado, y respetando los límites ya mencionados de proporcionalidad y razonabilidad.

Al respecto ha dicho la Sala Constitucional mediante la Sentencia N° 4845-96 de las 15:06 horas del 17 de setiembre de 1996 (Sala Constitucional, 1996), que:

> *"Cuando se realice un acto procesal de naturaleza probatoria, que implica la incidencia en los derechos fundamentales de los ciudadanos, la principal exigencia a nivel constitucional es que ésta se dé mediante resolución debidamente fundamentada de juez competente; que dicha decisión tenga como presupuesto la existencia de indicios comprobados de estar en presencia de un delito, aún cuando se ignore su supuesto responsable, en casos en que aún no se haya individualizado al imputado, no obstante que los elementos con que se cuenta permiten anticipar un resultado de interés para la averiguación de la verdad, que hace procedente la realización de la diligencia. La intervención del juez es una garantía de respeto al principio de no injerencia injustificada en los derechos fundamentales de los ciudadanos, siendo garantía de la interdicción de la arbitrariedad, así como de respeto al principio de proporcionalidad, pues ante la existencia de indicios comprobados de estarse en presencia de un delito, la intervención del juez pondera si éstos son suficientes –por la entidad del bien jurídico involucrado- para permitir una restricción a un derecho fundamental"*

Es importante en este punto mencionar lo que el artículo 181 del Código Procesal Penal (Asamblea Legislativa, 2016), el señala:

> *Artículo 181.- Legalidad de la prueba*
>
> *Los elementos de prueba sólo tendrán valor si han sido obtenidos por un medio lícito e incorporados al procedimiento conforme a las disposiciones de este Código.*
>
> *A menos que favorezca al imputado, no podrá utilizarse información obtenida mediante tortura, maltrato, coacción, amenaza, engaño, indebida intromisión en la intimidad del domicilio, la correspondencia, las comunicaciones, los papeles y los archivos privados, ni información obtenida por otro medio que menoscabe la voluntad o viole los derechos fundamentales de las personas.*

Si se tomara información de manera ilícita y sin respeto al debido proceso, la evidencia recabada adquiere el carácter de prueba ilícita.

Para los efectos es importante indicar que la normativa establece los derechos de la persona a la que se le interviene las comunicaciones, el artículo 4 de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones:

Artículo 4.- Derechos del intervenido.

Al ejecutar el registro, el secuestro o el examen, el Juez o el funcionario designado notificará y entregará copia de la orden judicial que lo autoriza, a quien le sean registrados, secuestrados o examinados los documentos. De esto se levantará un acta de la cual también se le entregará una copia, al finalizar la diligencia.

El interesado, dentro de los tres días posteriores a la ejecución de la medida, podrá solicitar su reconsideración y que se le restituyan los documentos secuestrados. La resolución de la anterior solicitud se sustanciará dando audiencia, por tres días a las partes. Contra lo resuelto por el Juez cabrá recurso de apelación.

De igual forma, dicha ley establece la obligatoriedad de las empresas e instituciones de facilitar la intervención de la autoridad judicial para que dicha acción sea efectiva, el artículo 20 señala al respecto:

Artículo 20.- Obligatoriedad de empresas e instituciones para facilitar la intervención.

Las empresas y las instituciones que brindan los servicios de comunicación están obligadas a conceder, a la autoridad judicial, todas las facilidades materiales y técnicas para que las intervenciones sean efectivas, seguras y confidenciales.

Para informarles sobre la disposición judicial, será necesario un oficio del Tribunal, en el que se consigne la información necesaria; no será requisito notificarles el contenido de la resolución que dispuso la medida.

Es claro que existe el deber de colaborar con las autoridades judiciales para la efectiva realización del procedimiento; el problema está en los alcances jurisdiccionales cuando las empresas no están radicadas en Costa Rica, por lo que deberá recurrirse a los acuerdos internacionales de colaboración en materia penal con los que contemos para facilitar la investigación.

Para efectos de acciones judiciales en que se vea involucrado temas TOR, no se conocen casos en que se haya incautado, hasta la fecha, TOR relays o servidores de un nodo TOR, pero como hemos visto podrían, respetando el debido proceso y los principios de razonabilidad y proporcionalidad, en los casos que existan indicios suficientes para sospechar de la comisión de un delito, siempre por orden judicial. De igual forma, no se conoce acciones que directamente el Organismo de Investigación Judicial haya utilizado específicamente TOR para acciones de investigación, pero si lo hicieran también deberán respectar el debido proceso y los principios de razonabilidad y proporcionalidad antes desarrollados.

Conclusiones

Costa Rica tiene un amplio marco normativo de protección de la privacidad e intimidad y respeto a derechos humanos; tanto nacional e internacional. Solamente en los escenarios en que exista la posibilidad real de un delito es que se puede afectar dichos derechos y generar un proceso judicial, siempre enmarcado en el debido proceso y dentro del marco de la proporcionalidad y razonabilidad.

Las herramientas en defensa de la privacidad, sea TOR o cualesquiera otras herramientas digitales que se utilice, no está regulada en concreto en nuestra normativa, y los ciudadanos pueden utilizarlas en pro de defender y proteger su derecho constitucional a la privacidad e intimidad sin restricción.

El Poder Judicial, mediante orden judicial fundamentada, y ante la posibilidad de la existencia de un delito, podría tomar acciones contra los nodos de TOR y los TOR Relays, pero deberá ser ante este escenario y por orden judicial, de igual forma respetando el debido proceso.

Los proveedores de servicio de internet no tendrían responsabilidad por el contenido que se transmita en sus redes, pero deberán colaborar con las autoridades judiciales, dentro de los marcos normativos nacionales, y brindar la información que esté en capacidad de brindar, cuando sucedan situaciones que violenten propiedad intelectual, derechos de autor o estemos frente a un posible delito. La colaboración debe incluir el acceso a la información, a los equipos, a las redes y a cualquier elemento que considere la investigación judicial que debe accederse para lograr recabar pruebas para comprobar el posible delito. Esto en razón que nuestra normativa no establece qué hechos pueden ser acreditados por pruebas legales (es "numerus apertus"), por lo que cualquier hecho, material y jurídicamente posible, que tenga alguna significación para un posterior proceso de juicio, puede ser probados por dichos medios, siempre enmarcado en los principios de razonabilidad y proporcionalidad y respeto a los derechos humanos, y que solamente las pruebas relacionadas con lo investigado se podrán utilizar. Es importante indicar que de acuerdo al nuestro código procesal penal, en sus artículos 181, 183 y 184 (Asamblea Legislativa, 2016) , se señala que los elementos de prueba sólo tendrán valor si han sido obtenidos por un medio lícito e incorporados al procedimiento conforme a las disposiciones de ley y a menos que favorezca al imputado, no podrá utilizarse información obtenida mediante tortura, maltrato, coacción, amenaza, engaño, indebida intromisión en la intimidad del domicilio, la correspondencia, las comunicaciones, los papeles y los archivos privados, ni información obtenida por otro medio que menoscabe la voluntad o viole los derechos fundamentales de las personas.

De igual forma, la prueba para ser admisible deberá referirse, directa o indirectamente, al objeto de la averiguación y deberá ser útil para descubrir la verdad.

No existen referencias del uso de la herramienta TOR para investigaciones judiciales ni que se hayan realizado acciones contra nodos TOR o TOR Relays en Costa Rica.

Bibliografía

Asamblea Legislativa. (11 de diciembre de 1968). *Sistema Costarricense de Información Jurídica*. Obtenido de Pacto Internacional de Derechos Civiles y Políticos: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=20579&nValor3=0&strTipM=FN

Asamblea Legislativa. (23 de febrero de 1970). Obtenido de Convención Americana sobre Derechos Humanos (Pacto de San José): http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=36150&nValor3=38111&strTipM=FN

Asamblea Legislativa. (09 de agosto de 1990). *Sistema Costarricense de Información Jurídica*. Obtenido de Convención sobre los Derechos del Niño: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=6606&nValor3=7032&strTipM=TC

Asamblea Legislativa. (26 de marzo de 2002). *Sistema Costarricense de Información Jurídica*. Obtenido de Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&strTipM=TC

Asamblea Legislativa. (30 de 06 de 2008). *Sistema Costarrricense de Información Jurídica*. Obtenido de Ley General de Telecomunicaciones: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=63431&nValor3=91176&strTipM=TC

Asamblea Legislativa. (18 de mayo de 2009). *Sistema Costarricense de Información Jurídica*. Obtenido de Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=65468&nValor3=107303&strTipM=TC

Asamblea Legislativa. (05 de setiembre de 2011). *Sistema Costarricense de Información Jurídica*. Obtenido de Protección de la Persona frente al tratamiento de sus datos personales: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

Asamblea Legislativa. (30 de setiembre de 2014). *Sistema Costarricense de Información Jurídica*. Obtenido de Código Penal: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=5027&nValor3=98548&strTipM=TC

Asamblea Legislativa. (19 de julio de 2016). *Sistema Costarricense de Información Jurídica*. Obtenido de Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=74352&nValor3=106487&strTipM=TC

Asamblea Legislativa. (02 de noviembre de 2016). *Sistema Costarricense de Información Jurídica*. Obtenido de Código Procesal Penal: http://www.pgrweb.go.cr/scij/Busqueda/Normati-

va/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=41297&nValor3=0&strTipM=TC

Asamblea Legislativa. (07 de marzo de 2018). *Sistema Costarricense de Información Jurídica*. Obtenido de Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=44448&nValor3=0&strTipM=TC

Asamblea Legislativa. (s.f.). *Asamblea Legislativa*. Recuperado el 20 de Mayo de 2012, de http://www.elfinancierocr.com/accesolibre/2011/julio/03/Proyecto-16679.pdf

Asamblea Legislativa de la República de Costa Rica. (s.f.). *Sistema Costarricense de Información Jurídica*. Obtenido de Costitución Política de la República de Costa Rica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_norma.aspx?param1=NRM&nValor1=1&nValor2=871&nValor3=0&strTipM=FN

De Dienheim Bariguete, C. (s.f.). *EL DERECHO A LA INTIMIDAD, AL HONOR Y A LA PROPIA IMAGEN.* Recuperado el 18 de junio de 2018, de http://www.unla.mx/iusunla3/reflexion/derecho%20a%20la%20intimidad.htm

Organización de Naciones Unidas. (10 de diciembre de 1948). *Sistema Costarricense de Información Jurídica*. Obtenido de Declaración Universal de Derechos Humanos: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=49015&nValor3=52323&strTipM=TC

Poder Ejecutivo. (18 de octubre de 2011). *Sistema Costarricense de Información Jurídica*. Obtenido de Reglamento sobre la limitación a la responsabilidad de los proveedores de servicios por infracciones a Derechos de Autor y Conexos de Acuerdo con el Artículo 15.11.27 del Tratado de Libre Comercio República Dominicana-Centroamérica- Estados Unidos: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=71640&nValor3=87035&strTipM=TC

Procuraduría General de la República. (s.f.). *Procuraduría General de la República*. Recuperado el 20 de Mayo de 2012, de http://www.pgr.go.cr/scij/Busqueda/Normativa/Pronunciamiento/pro_detalle.asp?param6=1&nDictamen=16464

Rojas Mora, G. E. (08 de mayo de 2008). *Instituto de Investigaciones Jurídicas de la Universidad de Costa Rica.* Obtenido de http://iij.ucr.ac.cr/wp-content/uploads/bsk-pdf-manager/2017/07/Secreto-en-las-comunicaciones-electronicas.pdf

Sala Constitucional. (17 de setiembre de 1996). *Sistema Costarricense de Información Jurídica*. Obtenido de Sentencia 4845-96: http://jurisprudencia.poder-judicial.go.cr/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=83117&strTipM=T&strDirSel=directo

SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA. (22 de noviembre de 1994). Obtenido de http://jurisprudencia.poder-judicial.go.cr/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=83723&strTipM=T&strDirSel=directo

SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA. (19 de noviembre de 1996). *Sistema Costarricense de Información Jurídica*. Obtenido de Sentencia: 06273: http://ju-

risprudencia.poder-judicial.go.cr/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=82174&strTipM=T&strDirSel=directo

SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA. (16 de noviembre de 2007). Obtenido de http://jurisprudencia.poder-judicial.go.cr/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=407562&strTipM=T&strDirSel=directo

SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA. (30 de octubre de 2008). *Sistema Costarricense de Información Jurídica*. Obtenido de http://jurisprudencia.poder-judicial.go.cr/SCIJ_PJ/busqueda/jurisprudencia/jur_Documento.aspx?param1=Ficha_Sentencia&nValor1=1&nValor2=436025&strTipM=T&strDirSel=directo


DERECHOSDIGITALES
Derechos Humanos y Tecnología en América Latina