MAPEO DE LAS NORMAS DE PRIVACIDAD Y VIGILANCIA **EN COSTA RICA**

accessnow

Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación del apoyo técnico directo, el análisis integral de políticas públicas, la incidencia global, la entrega de subvenciones para grupos locales emergentes, y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

Mapeo de las normas de privacidad y vigilancia en Costa Rica

Autora: Jamila Venturini
Contacto: jamila.venturini@gmail.com

Revisión y edición: Gaspar Pisanu
Coordinación general: Javier Pallero

Este informe fue elaborado por la autora en el marco del programa Policy Fellowship de Google, en el año 2016 y con el apoyo económico de la empresa.

TABLA DE CONTENIDOS

1. Introducción

Este reporte consiste en un primer acercamiento al marco regulatorio costarricense sobre privacidad y vigilancia de comunicaciones. El mismo es producto de un trabajo de investigación y mapeo realizado como parte del programa Google Policy Fellowship en la organización Access Now entre julio y octubre de 2016. El reporte fue actualizado en el mes de Mayo de 2018. Su estructura se inspira en aquella utilizada por la Electronic Frontier Foundation y Fundación Acceso en el reporte ¿Privacidad digital para defensores y defensoras de derechos humanos?. Parte de un primer mapeo de las normas internas sobre privacidad y vigilancia realizado por la Cooperativa Sula Batsú en el capítulo de Costa Rica del estudio "Examinando los derechos y las libertades en Internet en Latinoamérica (EXLILA)", de la Asociación para el Progreso de las Comunicaciones (APC).

Con relación a la metodología, el reporte se centró en el mapeo y análisis de las principales normas existentes referidas a privacidad y vigilancia en Costa Rica. No se analizaron las reglas relativas a la transferencia internacional de datos para fines de investigación criminal ni leyes de inteligencia. Por otra parte, el análisis incluye una breve sección sobre preocupaciones generales relevantes para la protección del derecho a la libertad de expresión y acceso a la información en el ambiente digital del país.

El reporte incluye una breve consideración acerca de la compatibilidad de las normas analizadas con los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. El análisis se hizo tomando en consideración la guía Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance, de Access Now, que contiene orientaciones para la efectiva incorporación de los principios en los marcos regulatorios internos de los países. El análisis del cumplimiento con los principios se hizo solamente en base a los textos legales, ya que este estudio no incluye una revisión sistemática de la jurisprudencia relevante. Un análisis más profundo del cumplimiento de los principios debería tomar en consideración no sólo la jurisprudencia, sino también una revisión del estado del arte del tema en Costa Rica - incluyendo entrevistas con agentes de la sociedad civil, gobierno y sector privado relevantes en el campo - que no pudo realizarse en este primer acercamiento al tema. Sin embargo, se espera que esta primera evaluación pueda orientar y servir de insumo para futuros estudios y acciones de incidencia.

La elección del tema del reporte se dió en conjunto con el equipo de Access Now en América Latina.

2. Tratados internacionales ratificados por Costa Rica

Costa Rica ha ratificado tratados de derechos humanos importantes para la protección de la privacidad como la Declaración Universal de los Derechos Humanos, El Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos, la Declaración Americana de los Derechos y Deberes del Hombre, y el Convenio sobre Ciberdelincuencia (Convenio de Budapest)[1].

[1] Bajo expediente legislativo número 18.484, la Asamblea Legislativa del 19 de mayo de 2017 aprobó la adhesión de Costa Rica al Convenio sobre la Ciberdelincuencia (Convenio de Budapest)

Según el artículo 7[2] de la Constitución del país, los convenios internacionales tienen rango superior a las leyes. Además, la acción de amparo puede utilizarse para la garantía de cualquier derecho humano reconocido en los tratados vigentes en el país (como veremos más adelante).

3. Constitución Política de Costa Rica

La Constitución de Costa Rica[3] fue redactada en 1949. Desde entonces, sufrió distintas reformas, como la del artículo 24 en 1996 que trata de la confidencialidad de las comunicaciones.

3.a VIGILANCIA

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

El título IV de Constitución de Costa Rica se dedica a los derechos y garantías individuales de los habitantes del país e incluye la inviolabilidad del domicilio y recintos privados (art. 23)[4] y la protección de la intimidad, libertad y secreto de las comunicaciones (art. 24)[5]. Además, determina que los documentos privados y comunicaciones de cualquier otro tipo son inviolables (art. 24).

3.a.ii Limitaciones constitucionales al derecho a la privacidad en el contexto de la vigilancia de las comunicaciones

Los mismos artículos constitucionales que tratan de la protección a la privacidad domiciliaria y de la inviolabilidad de las comunicaciones establecen sus límites.

Allanamientos

El artículo 23 determina que los allanamientos a recintos privados pueden ser realizados: (i) mediante autorización de un juez competente, (ii) o bien para impedir la comisión o impunidad de delitos, (iii) o para evitar daños graves a las personas o propiedades. A pesar de ser positiva la necesidad de autorización por parte de un tribunal independiente, el lenguaje adoptado puede dar margen a una interpretación amplia sobre las otras situaciones en que la inviolabilidad del domicilio puede ser limitada sin la revisión de un juez debido a la utilización de la conjunción

[2]Artículo 7: 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. Los tratados públicos y los convenios internacionales referentes a la integridad territorial o la organización política del país, requerirán aprobación de la Asamblea Legislativa, por votación no menor de las tres cuartas partes de la totalidad de sus miembros, y la de los dos tercios de los miembros de una Asamblea Constituyente, convocada al efecto. *(Reformado por el artículo único de la ley N° 4123 de 31 de mayo de 1968)*

[3] Disponible en http://www.pgrweb.go.cr/scij/busqueda/normativa/normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=871&strTipM=TC

[4]Artículo 23: El domicilio y todo recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez 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.

[5]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. Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial. 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 señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión. No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación. *(Reformado por el artículo 1° de la ley N° 7607 de 29 de mayo de 1996)*

disyuntiva “o”. Aún así, la Constitución es explícita en determinar que cualquier intervención en los recintos privados debe respetar lo establecido en la ley.

Inviolabilidad de las comunicaciones

Además de garantizar la inviolabilidad de las comunicaciones de cualquier tipo y de los documentos privados, el artículo 24 de la Constitución de Costa Rica reconoce que mediante una ley se establecerá cómo los Tribunales de Justicia podrán ordenar excepciones a esta regla[6]. Las excepciones según el artículo constitucional son (i) el secuestro, registro o examen de documentos privados y (ii) la intervención en cualquier tipo de comunicación.

El mismo artículo constitucional establece que el registro, secuestro o examen de documentos privados sólo será permitido cuando sea absolutamente indispensable para una investigación penal en curso y que una ley específica determinará los casos en que será permitida. Con relación a las intervenciones en las comunicaciones privadas, nuevamente establece que la ley determinará en qué casos y para cuáles delitos podrán ser autorizadas y por cuánto tiempo. Los funcionarios del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar libros de contabilidad para fines tributarios y de fiscalización del uso de los fondos públicos en situaciones específicas y determinadas en la ley.

A pesar de no adelantar las situaciones o condiciones en las que los Tribunales de Justicia podrán intervenir comunicaciones, la Constitución es clara en explicitar que se trata de un recurso excepcional y que debe ser limitado en el tiempo. Además, agrega que habrá penalidades a los funcionarios que apliquen la excepción ilegalmente. La responsabilidad de aplicar y controlar las órdenes de intervención en las comunicaciones recae en la autoridad judicial.

Finalmente, el mismo artículo determina que no producirán efectos legales las informaciones obtenidas como resultado de intervenciones ilegales de cualquier comunicación o de correspondencia sustraída ilegalmente.

La Sala Constitucional de la Corte Suprema de Justicia determinó en por lo menos dos sentencias de 2007 que la protección prevista por el artículo 24 se refiere a intervenciones telefónicas, pero no al “rastreo de llamadas”, por considerarlo diferente. La sala constitucional entiende por “rastreo de llamadas” a la obtención y análisis de metadatos sobre las comunicaciones (información de origen, destino, duración, etc.). De acuerdo a la Corte, dicho rastreo puede ser ordenado por el Ministerio Público sin necesidad de orden judicial. Según la sentencia 17097-07, “[..] esta Sala ha sostenido reiteradamente que el rastreo de llamadas y la intervención telefónica son figuras diferentes, y en tanto la última está protegida por el artículo 24 de la Constitución Política y sólo puede ser autorizada por juez competente en los casos que taxativamente prevé la ley respectiva, la primera no está sometida a dichas restricciones y no viola el contenido del citado artículo constitucional, por lo que bien puede ser ordenada por el Ministerio Público”.[7] No obstante, otras sentencias señalaron que si bien no se requiere autorización de un juez para realizar rastreo de llamadas, la orden de rastreo debe estar circunscrita a una investigación penal, respetar los derechos humanos y el principio de proporcionalidad - es decir no rastrear a un tercero ajeno a la investigación.[8]

La interpretación de la Sala Constitucional es que la intervención telefónica implica: (i) un procedimiento técnico de colocación de cables que adhieren a la central telefónica y al número telefónico cuya interceptación se pretende y la instalación de un equipo de registro o grabación del contenido de las llamadas y (ii) que el término hace alusión a las implicaciones de dicho procedimiento. Así, se entiende que la intervención telefónica, “implica la grabación y la imposición eventual del contenido de las llamadas registradas” y el rastreo telefónico permite “identificar los números telefónicos de los cuales procede una llamada o a los cuales se dirige la comunicación, sin posibilidad alguna de enterarse del contenido de las llamadas”. En efecto, el análisis de metadatos estaría sujeto a una protección más débil según la interpretación mencionada.

[6] Actualmente la norma que regula el tema es la Ley 7425 de 1994 - Ley sobre el Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones

[7] Sentencia disponible en https://vlex.co.cr/vid/-499268510

[8] “VI. (...) En un sentido similar se puede indicar que, el rastreo telefónico en este caso, sí podría ordenarlo el Ministerio Público, sin necesidad de una orden judicial, si de la investigación de un ilícito penal se trata, PERO únicamente a los sujetos sospechosos y NUNCA a un tercero ajeno a la investigación, so pena de violar el derecho a la intimidad de este último” Sentencia 04035 - 2014. Expediente 14-000848-7-CO. Sala Constitucional.

3.b CIFRADO Y ANONIMATO

3.b.i. Salvaguardas constitucionales para la protección del cifrado y el anonimato

El mismo título IV de la Constitución Política de Costa Rica también protege la libertad de pensamiento (art. 28)[9] y expresión (art. 29)[10], además del derecho de acceso a la información pública (art. 30)[11], con excepción de los secretos de Estado.

No hay en el texto constitucional limitaciones expresas al ejercicio de la libertad de expresión de manera anónima, aunque el artículo 29 explicite que en casos de abusos a la libertad de expresión habrá responsabilización según determine la ley. Con eso, se entiende que el cifrado y anonimato están permitidos en el país.

3.c. MECANISMOS DE ACCESO A LA JUSTICIA

La Constitución de Costa Rica prevé en su artículo 48[12] el amparo, aplicable no sólo para el goce de derechos previstos en la Constitución, pero también para la garantía de derechos fundamentales establecidos en los tratados internacionales de derechos humanos vigentes en el país. Con la reforma constitucional de la Ley N° 7128 de 1989, los recursos de amparo pasan a ser resueltos por la Sala Constitucional de la Corte Suprema de Justicia.

La Constitución también prevé una serie de reglas de debido proceso que incluyen, entre otros, el derecho a ser juzgado solamente por tribunales establecidos según la Constitución (art. 35)[13], a no ser detenido sin un indicio comprobado de haber cometido delito, y sin mandato escrito de juez o autoridad encargada del orden público (art. 37)[14], a encontrar reparación para las injurias o daños que hayan recibido (art. 41)[15]. Además, determina que un mismo juez no puede juzgar un mismo punto en distintas instancias y que nadie podrá ser juzgado más de una vez por un mismo hecho punible (art. 42)[16].

3.d. OBSERVANCIA DE LOS PRINCIPIOS INTERNACIONALES SOBRE LA APLICACIÓN DE LOS DERECHOS HUMANOS A LA VIGILANCIA DE LAS COMUNICACIONES

La Constitución de Costa Rica cumple con los principios de legalidad, necesidad, autoridad judicial competente, debido proceso y supervisión pública. En primer lugar, por establecer que una ley deberá autorizar la intervención de comunicaciones y detallar las condiciones para la aprobación y eventuales reformas en dicha ley. En segundo lugar, al

[9]Artículo 28: Nadie puede ser inquietado ni perseguido por la manifestación de sus opiniones ni por acto alguno que no infrinja la ley. Las acciones privadas que no dañen la moral o el orden públicos, o que no perjudiquen a tercero, están fuera de la acción de la ley. No se podrá, sin embargo, hacer en forma alguna propaganda política por clérigos o seglares invocando motivos de religión o valiéndose, como medio, de creencias religiosas.

[10]Artículo 29: 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.

[11]Artículo 30: 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.

[12]Artículo 48: Toda persona tiene derecho al recurso de hábeas corpus para garantizar su libertad e integridad personales, y al acción de amparo para mantener o restablecer el goce de los otros derechos consagrados en esta Constitución, así como de los de carácter fundamental establecidos en los instrumentos internacionales sobre derechos humanos, aplicables en la República. Ambos recursos serán de competencia de la Sala indicada en el artículo 10. (Reformado por ley N°.7128 de 18 de agosto de 1989)

[13]Artículo 35: Nadie puede ser juzgado por comisión, tribunal o juez especialmente nombrado para el caso, sino exclusivamente por los tribunales establecidos de acuerdo con esta Constitución.

[14]Artículo 37: Nadie podrá ser detenido sin un indicio comprobado de haber cometido delito, y sin mandato escrito de juez o autoridad encargada del orden público, excepto cuando se tratare de reo prófugo o delincuente infraganti; pero en todo caso deberá ser puesto a disposición de juez competente dentro del término perentorio de veinticuatro horas.

[15]Artículo 41: Ocurriendo a las leyes, todos han de encontrar reparación para las injurias o daños que hayan recibido en su persona, propiedad o intereses morales. Debe hacérseles justicia pronta, cumplida, sin denegación y en estricta conformidad con las leyes.

[16]Artículo 42: Un mismo juez no puede serlo en diversas instancias para la decisión de un mismo punto. Nadie podrá ser juzgado más de una vez por el mismo hecho punible. Se prohíbe reabrir causas penales fenecidas y juicios fallados con autoridad de cosa juzgada, salvo cuando proceda el recurso de revisión.
(La Sala Constitucional mediante resolución N° 353 del 12 de febrero de 1991, interpretó el presente artículo en el sentido de que ".al expresar que "un mismo Juez no puede serlo en diversas instancias para la decisión de un mismo punto", se refiere exclusivamente a que el Juez que dicta una resolución, no puede resolver el recurso de apelación ni el extraordinario que proceda contra ella".)

determinar que cabe a los Tribunales de Justicia autorizar la intervención de comunicaciones y el secuestro de documentos privados. La Constitución también establece que el secuestro de documentos privados será autorizado por los Tribunales de Justicia solamente cuando sea "absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento" (art. 24), lo que es observado por las leyes específicas sobre el tema, como se explica adelante.

Sin embargo, la interpretación jurisprudencial de que las reglas para la intervención telefónica se aplican solamente al contenido de las comunicaciones y no a los llamados "metadatos" fragiliza la protección constitucional a estos datos personales que también pueden revelar informaciones sensibles sobre un individuo. Para estos datos no se cumple con el principio sobre la necesidad de autorización de una autoridad judicial competente. La ausencia de un marco legal claro para establecer las reglas de acceso en estos casos puede perjudicar el cumplimiento con los principios mencionados anteriormente.

4. Salvaguardas y limitaciones del derecho a la privacidad en el contexto de la vigilancia de las comunicaciones en las leyes generales de Costa Rica

4.a Código Penal y Código Procesal Penal

El Código Penal de Costa Rica (Ley N° 4573/1970)[17] posee un título específico dedicado a los delitos contra el ámbito de intimidad. En la sección sobre la violación de secretos se sanciona con prisión de uno a tres años la violación de correspondencia o comunicaciones y la difusión del contenido de comunicaciones o documentos privados que carezcan de interés público (art. 196).[18] La misma pena será impuesta a quienes inciten a terceros a cometer cualquiera de estos delitos.

El mismo artículo determina que, en el caso en el que el crimen sea cometido por personas (i) encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones afectados o (ii) de administrar o dar soporte al sistema informático o que tengan a acceso a dichos sistemas, las penas aplicables serán de dos a cuatro años.

[17] http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=5027

[18] 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)*

Se prohíbe además la violación de datos personales con pena de uno a tres años (art. 196 bis).[19] Esto incluye apoderarse, modificar, interferir, acceder, copiar, transmitir, publicar, difundir, recopilar, inutilizar, interceptar, retener, vender, comprar, desviar para otros fines o dar tratamiento no autorizado a imágenes o datos de personas físicas o jurídicas sin la autorización del titular. La pena aumenta y será de dos a cuatro años (i) si la violación es practicada por personas encargadas de administrar el sistema donde se encuentran almacenados los datos, (ii) si la víctima es un menor de edad o incapaz o (iii) si los datos en cuestión revelen la ideología, religión, creencias, salud, origen racial o preferencia sexual de una persona. No obstante, no entra dentro del tipo penal la publicación, difusión o transmisión de informaciones públicas, de interés público o datos obtenidos en registros públicos o bases de datos de acceso público irrestricto.[20]

En la misma sección también se prohíbe el apoderamiento de cartas o documentos privados[21] y la captación de manifestaciones verbales sin consentimiento[22]. En ambos casos las penas van de uno a tres años de prisión.

Sin embargo, en todos los casos mencionados las penas pueden llegar a seis años - a criterio del juez - si se identifica abuso de función u oficio.[23]

La sección siguiente se dedica a la violación de domicilio e incluye penas de prisión de seis meses a tres años, además de la inhabilitación para el ejercicio de cargos públicos, a los funcionarios que practiquen allanamientos en disconformidad con la ley.[24]

[19]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."
(Así 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)

[20]Los artículos 196 y 196 bis del Código Penal, entre otros (ver abajo), fueron modificados por la Ley 9048, de 2012, que sufrió severas críticas por parte de académicos, periodistas y activistas que veían en la redacción una amenaza a la libertad de expresión. La aprobación de la ley, calificada como "anti-Wikileaks", generó protestas estudiantiles en la capital del país. Para más informaciones ver: http://www.technollama.co.uk/is-this-the-first-anti-wikileaks-law (en inglés), https://es.globalvoices.org/2012/07/23/costa-rica-ley-de-delitos-informaticos-amenaza-la-libertad-en-interne y https://knightcenter.utexas.edu/es/blog/00-12109-en-costa-rica-protesta-estudiantil-por-ley-que-penaliza-la-obtencion-de-informacion-se. Ambos artículos luego fueron modificados por Ley N° 9135 del 24 de abril de 2013.

[21]Artículo 197: Será reprimido, con prisión de uno a tres años, quien se apodere de una carta o de otro documento privado, aunque no esté cerrado, o al que suprima o desvíe de su destino una correspondencia que no le esté dirigida. *(Reformado por el artículo 31 de la "Ley de Registro de Documentos Privados e Intervención de Comunicaciones"; ley Nº 7425 de 9 de agosto de 1994)*

[22]Artículo 198: Será reprimido, con prisión de uno a tres años, quien grabe sin su consentimiento, las palabras de otro u otros, no destinadas al público o que, mediante procedimientos técnicos, escuche manifestaciones privadas que no le estén dirigidas, excepto lo previsto en la Ley sobre registro, secuestro y examen de documentos privados e intervención de las comunicaciones. La misma pena se impondrá a quien instale aparatos, instrumentos, o sus partes, con el fin de interceptar o impedir las comunicaciones orales o escritas, logren o no su propósito. *(Reformado por el artículo 31 de la "Ley de Registro de Documentos Privados e Intervención de Comunicaciones"; ley Nº 7425 de 9 de agosto de 1994)*

[23]Artículo 200: En los casos de los tres artículos anteriores, se impondrá prisión de dos a seis años si la acción se perpetra: a) Por funcionarios públicos, en relación con el ejercicio de sus funciones. b) Por quien ejecute el hecho, prevaliéndose de su vinculación con una empresa o institución pública o privada encargada de las comunicaciones. c) Cuando el autor publique la información obtenida o aún sin hacerlo, tenga carácter privado, todo a juicio del Juez. *(Reformado por el artículo 31 de la "Ley de Registro de Documentos Privados e Intervención de Comunicaciones"; ley Nº 7425 de 9 de agosto de 1994)*

[24]Artículo 205: Se impondrá prisión de seis meses a tres años e inhabilitación para el ejercicio de cargos y oficios públicos, de uno a cuatro años al agente de la autoridad o al funcionario público que allanare un domicilio sin las formalidades prescritas por la ley o fuera de los casos que ella determine. *(Reformado de acuerdo con la anulación parcial ordenada por resolución de la Sala Constitucional N° 4368 del 29 de abril de 2009.)*

El Código Penal de Costa Rica incluye también una sección específica sobre delitos informáticos y conexos, adicionada por la Ley N° 9048/2012.[25] Los crímenes incluyen, entre otros, la suplantación de identidad (art. 230)[26], el espionaje informático (art. 231) destinado a informaciones que generen valor económico para el comercio o la industria, la instalación de programas maliciosos (art. 232) y la suplantación de páginas electrónicas (art. 233).

El Código Procesal Penal de Costa Rica (Ley N° 7594/1996)[27] determina que los elementos de prueba que hayan sido obtenidos por medios ilícitos - lo que incluye información obtenida a través de la intromisión indebida en la intimidad del domicilio, correspondencia, comunicaciones y papeles y archivos privados a menos que favorezca al imputado (art. 181).[28] Finalmente, establece los procedimientos para la efectivización de un allanamiento (art. 196)[29] y las condiciones en las cuales será permitida la realización de un allanamiento sin orden judicial (art. 197)[30].

4.b Ley sobre Registro, Secuestro, y Examen de Documentos Privados e Intervención de las Comunicaciones

Como establece la Constitución, las excepciones al secreto de las comunicaciones y documentos privados son reglados por una ley específica, la Ley sobre Registro, Secuestro, y Examen de Documentos Privados e Intervención de las Comunicaciones (N° 7425/1994).[31] La ley trata en en su primera parte del registro, secuestro o examen de documentos privados y determina que ello sólo podrá ser autorizado por los Tribunales de Justicia cuando sea absolutamente necesario en investigaciones de naturaleza penal (art. 1). Además, establece que las órdenes de secuestro deben especificar, entre otras cosas, los documentos que serán objeto del registro, secuestro o examen (art. 3) y que la no observación de este procedimiento puede llevar a su anulación.[32]

Con relación a las medidas de intervención en las comunicaciones de cualquier tipo, la ley refuerza su carácter excepcional al limitar su aplicación solamente a la investigación de un número limitado de delitos (art. 9).[33] Los cuales son: secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía,

[25] http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=101586&strTipM=TC

[26] El artículo fue luego modificado por la Ley N° 9135 del 24 de abril de 2013.

[27] http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=41297

[28] 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.

[29] Artículo 196: Formalidades para el allanamiento Una copia de la resolución que autoriza el allanamiento será entregada a quien habite o posea el lugar donde se efectúe o, cuando esté ausente, a su encargado, y, a falta de éste, a cualquier persona mayor de edad que se halle en el lugar. Se preferirá a los familiares. Cuando no se encuentre a nadie, ello se hará constar en el acta. Practicado el registro, en el acta se consignará el resultado, con expresión de las circunstancias útiles para la investigación. La diligencia se practicará procurando afectar lo menos posible la intimidad de las personas. El acta será firmada por los concurrentes; no obstante, si alguien no la firma, así se hará constar.

[30] Artículo 197: Allanamiento sin orden Podrá procederse al allanamiento sin previa orden judicial cuando: a) Por incendio, inundación u otra causa semejante, se encuentre amenazada la vida de los habitantes o la propiedad. b) Se denuncia que personas extrañas han sido vistas mientras se introducen en un local, con indicios manifiestos de que pretenden cometer un delito. c) Se introduzca en un local algún imputado de delito grave a quien se persiga para su aprehensión. d) Voces provenientes de un lugar habitado, sus dependencias o casa de negocio, anuncien que allí se está cometiendo un delito o pidan socorro.

[31] http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=16466&nValor3=17615&param2=1&strTipM=TC&lResultado=3&strSim=simp

[32] Artículo 3: 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.

[33] Artículo 9: 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 siguientes delitos: secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía, tráfico de personas y tráfico de personas para comercializar sus órganos; homicidio calificado; genocidio, terrorismo y los delitos previstos en la Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas, N° 8204, del 26 de diciembre del 2001. 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. *(Reformado por Ley N° 8238 de 26 de marzo del 2002)*

tráfico de personas y tráfico de personas para comercializar sus órganos; homicidio calificado; genocidio, terrorismo y los delitos previstos en la ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas (N° 8204/2001[34]).

Nuevamente, solo un juez podrá autorizar las intervenciones en las comunicaciones cuando ello pueda servir como prueba indispensable de la comisión de alguno de estos delitos (art. 10).[35] La solicitud de intervención puede ser presentada por escrito por el Jefe del Ministerio Público, el Director del Organismo de Investigación Judicial o alguna de las partes del proceso y debe presentar una justificación sobre sus motivos (art. 10).

Según la ley, las intervenciones tienen un límite máximo de 3 meses de duración, prorrogables un máximo de dos veces por igual período en los casos de extrema gravedad o difícil investigación (art. 12).[36]

Con relación a la ejecución de los procedimientos de intervención de comunicaciones, es de responsabilidad del Poder Judicial nombrar al personal técnico capacitado a realizarlos. Además, son creados mecanismos de supervisión interna (Jefe del Ministerio Público y Director del Organismo de Investigación Judicial) y externa (una comisión especial formada por tres magistrados nombrados por el Poder Judicial) para observar la ejecución de las intervenciones (art. 15).[37] Asimismo, el juez es el responsable de todas las actuaciones realizadas para la aplicación de las medidas de intervención y de la supervisión del personal técnico encargado de su ejecución (art. 16).[38] También cabe a él garantizar que ellas afecten lo mínimo posible a terceros que no son parte de la investigación (art. 16). Por otra parte, las empresas que ofrezcan servicios de comunicación en Costa Rica están obligadas no sólo a facilitar que las intervenciones sean efectivas (art. 23)[39], pero que además sean seguras y confidenciales (art. 20).[40]

[34] Esta ley reformó integralmente la Ley N° 7786/1998 Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso No Autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo. Posteriormente la Ley N° 8204/2001 ha sufrido varias modificaciones siendo la última la del 2017 mediante la Ley N° 9449/2017.

[35]Artículo 10: El Juez, mediante resolución fundada, de oficio, a solicitud del Jefe del Ministerio Público, del Director del Organismo de Investigación Judicial o de alguna de las partes del proceso, si hubiere, podrá ordenar intervenir las comunicaciones orales o escritas, cuando pueda servir como prueba indispensable de la comisión de alguna de las conductas delictivas, a las que se refiere el artículo anterior. El Juez realizará personalmente la diligencia, salvo en casos de excepción en los cuales, según su criterio, podrá delegarla en miembros del Organismo de Investigación Judicial o del Ministerio Público, quienes deberán informarle, por escrito, del resultado. De ello deberá levantarse el acta correspondiente. *(La Sala Constitucional mediante resolución N° 3195 del 20 de junio de 1995, estableció que del párrafo anterior no es inconstitucional la frase que dice "podrá delegarla en miembros del Organismo de Investigación Judicial o del Ministerio Público", toda vez que lo que puede delegar el juez es únicamente la realización de los actos materiales de ejecución de la intervención y no la responsabilidad sobre la misma ni la escucha de las comunicaciones intervenidas.) (Adicionado posteriormente por resolución interlocutoria N° 329-I-95 del 27 de junio de 1995)* La solicitud de intervención deberá estar por escrito, expresar y justificar sus motivos y cometidos, con el propósito de que puedan ser valorados por el Tribunal. En caso de que sea solicitada por el Organismo de Investigación Judicial deberá contener, además, los nombres de los oficiales a cargo de la investigación. En los demás casos, el Juez solicitará a ese Organismo la designación respectiva.

[36]Artículo 12: La intervención ordenada se autorizará por un lapso máximo hasta de tres meses, salvo en los casos de extrema gravedad o de difícil investigación, en los que el Juez, mediante resolución fundada, disponga una prórroga. Excepcionalmente, se podrán ordenar, por igual plazo, hasta dos prórrogas como máximo.

[37]Artículo 15: El Poder Judicial, por medio de los órganos correspondientes, nombrará al personal técnico especializado para cumplir con las tareas que se ordenan en esta Ley. Este personal deberá ser de comprobada integridad y ser capacitado en sus labores específicas y en los derechos civiles, que puedan ser perturbados por la intervención. El nombramiento de ese personal deberá ser ratificado por la Corte Plena, la cual establecerá y desarrollará sus sistemas y formas de operación. La Corte Plena establecerá, asimismo, los mecanismos de supervisión interna y externa. La supervisión interna estará a cargo del Jefe del Ministerio Público y del Director del Organismo de Investigación Judicial; la externa será responsabilidad de una comisión especial, integrada por tres magistrados, nombrada por la Corte Plena.

[38]Artículo 16: El Juez que ordene la intervención será el responsable directo de todas las actuaciones realizadas en la aplicación de las medidas, sin que pueda haber delegación alguna en este sentido. El personal técnico encargado de ejecutar la medida quedará subordinado a la autoridad judicial correspondiente, mientras dure su aplicación. El Juez ordenará y velará porque la intervención se realice de la manera menos gravosa para terceras personas no investigadas.

[39]Artículo 23: Serán obligaciones de los funcionarios responsables de las empresas o instituciones públicas y privadas a cargo de las comunicaciones: 1.- Dar todas las facilidades para que las medidas ordenadas por el Juez competente se hagan efectivas. 2.- Acatar la orden judicial, de tal manera que no se retarde, se obstaculice o se impida la ejecución de la medida ordenada.

[40]Artículo 20: 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.

Finalmente, la ley establece sanciones a los funcionarios que divulguen o utilicen informaciones obtenidas mediante el secuestro de documentos privados o la intervención de comunicaciones para fines distintos a los establecidos por la orden judicial o que no observen los requisitos establecidos en la ley al ordenar el secuestro o intervención (arts. 24[41] y 25[42]).

4.c Código Civil

Los derechos de personalidad están protegidos bajo el Título II, Capítulo I, del Código Civil Costarricense (Ley N° 63/1887).[43] Según su artículo 47, el consentimiento del sujeto es la condición fundamental para la publicación, reproducción, exposición o venta de sus imágenes - con excepción de personas que sean públicas, que tengan alguna función pública, que haya necesidad de justicia o policía, o que las imágenes hayan sido tomadas en lugares públicos. [44] En caso de que no haya consentimiento, las personas afectadas pueden solicitar como medida cautelar la suspensión de la publicación, exhibición o venta de las fotografías (art. 48).[45] Finalmente, se garantiza el derecho de obtener indemnización por daño moral en los casos de lesión a los derechos de personalidad (art. 59).[46]

[41]Artículo 24: Se reprimirá, con prisión de uno a tres años, al juez y al funcionario policial o del Ministerio Público, que divulgue o utilice la información recabada mediante el secuestro de documentos o la intervención de comunicaciones, con un propósito diferente del establecido en la orden. Con igual pena, se reprimirá al funcionario que no observe las formalidades ni los requisitos prescritos en esta Ley, al ordenar o practicar un secuestro, un examen, un registro de documentos o una intervención de comunicaciones.

[42]Artículo 25: Se reprimirá, con prisión de seis meses a dos años, al juez o al funcionario policial o del Ministerio Público que, por culpa, divulgue o permita que se divulgue información obtenida mediante el secuestro de documentos o la intervención de las comunicaciones.

[43] Disponible en http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=15437

[44]Artículo 47: La fotografía o la imagen de una persona no puede ser publicada, reproducida, expuesta ni vendida en forma alguna si no es con su consentimiento, a menos que la reproducción esté justificada por la notoriedad de aquélla, la función pública que desempeñe, las necesidades de justicia o de policía, o cuando tal reproducción se relacione con hechos, acontecimientos o ceremonias de interés público o que tengan lugar en público. Las imágenes y fotografías con roles estereotipados que refuercen actitudes discriminantes hacia sectores sociales no pueden ser publicadas, reproducidas, expuestas ni vendidas en forma alguna.
(Reformado por el artículo 79 de la Ley de Igualdad de Oportunidades para Personas con Discapacidad No.7600 de 2 de mayo de 1996)

[45]Artículo 48: Si la imagen o fotografía de una persona se publica sin su consentimiento y no se encuentra dentro de alguno de los casos de excepción previstos en el artículo anterior, aquella puede solicitarle al Juez como medida cautelar sin recursos, suspender la publicación, exposición o venta de las fotografías o de las imágenes, sin perjuicio de lo que resuelva en definitiva. Igual medida podrá solicitar la persona directamente afectada, sus representantes o grupos de interés acreditados, en el caso de imagen o fotografías que estereotipen actitudes discriminantes. *(Reformado por el artículo 79 de la Ley de Igualdad de Oportunidades para Personas con Discapacidad No.7600 mayo 1996)*

[46]Artículo 59: Se establece el derecho a obtener indemnización por daño moral, en los casos de lesión a los derechos de la personalidad.
(Reformado por Ley No. 5476 de 21 de diciembre de 1973, artículo 2º. Por Ley Nº 7020 de 6 de enero de 1986, artículo 2º, su número fue corrido del 41 al actual).

4.d Ley General de Telecomunicaciones

La Ley General de Telecomunicaciones de Costa Rica (N° 8642/2008)[47]establece a la privacidad de la información entre sus principios rectores. Esto es, la obligación de los operadores de telecomunicaciones de garantizar el derecho a la intimidad, libertad y secreto de las comunicaciones, además de la confidencialidad de la información que obtengan de los usuarios u otros operadores (art. 3, j).[48] La violación de la confidencialidad de las comunicaciones es considerada una infracción muy grave (art. 67, a, 16) e implica una multa de entre 0,5 a 1% de los ingresos brutos del operador en el período fiscal anterior (art. 68, a)[49]. Adicionalmente, el Estado - a través de la autoridad de telecomunicaciones - está autorizado a, entre otras medidas, imponer el cierre definitivo de un establecimiento caso lo juzgue necesario para garantizar la integridad y calidad de la red y de los servicios de telecomunicaciones (art. 69).[50]

La ley contiene un capítulo completo dedicado a la privacidad de las comunicaciones y la protección de datos personales. En él se establece que los proveedores y operadores de servicios de telecomunicación deberán implantar las medidas técnicas y administrativas necesarias para garantizar la seguridad de sus redes y servicios (art. 42).[51]

Los datos de tráfico y localización de los usuarios deben ser eliminados o anonimizados cuando no sean necesarios para la prestación del servicios. Los datos de tráfico necesarios para efectos de la facturación sólo serán tratados hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago. Asimismo, previo consentimiento o proceso de anonimización se podrán tratar los datos de localización. (art. 43).[52]

[47]http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=63431&nValor3=91176&strTipM=TC

[48]Artículo 3: La presente Ley se sustenta en los siguientes principios rectores: [...] j) Privacidad de la información: obligación de los operadores y proveedores, de conformidad con el artículo 24 de la Constitución Política, a garantizar el derecho a la intimidad, la libertad y el secreto de las comunicaciones, así como proteger la confidencialidad de la información que obtengan de sus clientes, o de otros operadores, con ocasión de la suscripción de los servicios, salvo que estos autoricen, de manera expresa, la cesión de la información a otros entes, públicos o privados.

[49]Artículo 68: Las infracciones serán sancionadas de la siguiente manera: a) Las infracciones muy graves serán sancionadas mediante una multa de entre cero coma cinco por ciento (0,5%) y hasta un uno por ciento (1%) de los ingresos brutos del operador o proveedor obtenidos durante el período fiscal anterior. b) Las infracciones graves serán sancionadas mediante una multa de entre cero coma cero veinticinco por ciento (0,025%) y hasta un cero coma cinco por ciento (0,5%) de los ingresos brutos del operador o proveedor obtenidos durante el período fiscal anterior. Cuando un operador o proveedor no haya obtenido ingresos brutos o se encuentre imposibilitado para reportarlos, la Sutel utilizará como parámetro para la imposición de sanciones el valor de sus activos. En el caso de las infracciones referidas en el inciso a) del artículo anterior que, a juicio de la Sutel, revistan gravedad particular, esta Superintendencia puede imponer como sanción una multa de un uno por ciento (1%) y hasta un diez por ciento (10%) de las ventas anuales obtenidas por el infractor durante el ejercicio fiscal anterior, o entre un uno por ciento (1%) y hasta por un diez por ciento (10%) del valor de los activos del infractor. En el caso de que no se pueda aplicar la sanción sobre las ventas o los activos, la Sutel utilizará como parámetro para la imposición de sanciones los ingresos presuntos del período, tomando en cuenta los ingresos brutos promedio de períodos anteriores y los ingresos promedio del período anterior de otros operadores o proveedores que desarrollen actividades económicas y comerciales similares. Para efectos de imponer la sanción, la Sutel deberá valorar si el infractor forma parte de un grupo económico, de conformidad con lo definido en el artículo 6 de esta Ley. En este caso, la sanción será impuesta con base en el ingreso bruto o las ventas anuales, según sea el caso, de las empresas que conforman el grupo.

[50]Artículo 69: Con el objetivo de garantizar la integridad y calidad de la red y los servicios de telecomunicaciones, así como la seguridad de los usuarios, la Sutel podrá imponer como sanción, en el caso de las infracciones muy graves, el cierre definitivo de un establecimiento y la clausura de sus instalaciones, la remoción de cualquier equipo o instrumento que permita la operación de redes o la prestación de servicios de telecomunicaciones en forma ilegítima, o ponga en riesgo la integridad de las instalaciones, redes, equipos y aparatos. Para ejecutar estas medidas se dispondrá del auxilio de la Fuerza Pública.

[51]Artículo 42: Los operadores de redes públicas y proveedores de servicios de telecomunicaciones disponibles al público, 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. Los operadores y proveedores deberán adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios. En caso de que el operador conozca un riesgo identificable en la seguridad de la red, deberá informar a la Sutel y a los usuarios finales sobre dicho riesgo. Los operadores y proveedores deberán garantizar que las comunicaciones y los datos de tráfico asociados a ellas, no serán escuchadas, gravadas, almacenadas, intervenidas ni vigiladas por terceros sin su consentimiento, salvo cuando se cuente con la autorización judicial correspondiente, de conformidad con la ley.

[52]Artículo 43: Los datos de tráfico y de localización relacionados con los usuarios finales que sean tratados y almacenados bajo la responsabilidad de un operador o proveedor, deberán eliminarse o hacerse anónimos cuando no sean necesarios para efectos de la transmisión de una comunicación o para la prestación de un servicio. Los datos de tráfico necesarios para efectos de la facturación de abonados y los pagos de las interconexiones, podrán ser tratados hasta la expiración del plazo durante el cual pueda impugnarse, legalmente, la factura o exigirse el pago. Los datos de localización podrán tratarse solamente si se hacen anónimos o previo consentimiento de los abonados o usuarios, en la medida y por el tiempo necesario para la prestación de un servicio.

Entre los derechos de los usuarios de servicios de telecomunicaciones también se incluye el de solicitar la exclusión gratuita de las guías de abonados disponibles al público y de decidir qué datos pueden ser incluídos (art. 45, 16).[53]

Finalmente, la ley determina que un reglamento específico tratará de las medidas de protección de la privacidad de las comunicaciones (art. 77, 1, e)[54]). El Decreto Ejecutivo N° 35205-MINAE/2009[55] se aplica a todos los operadores y prestadores de servicios de telecomunicaciones que utilicen o exploten redes públicas (art. 2). Sus reglas de protección de la privacidad - así como las de la Ley General de Telecomunicaciones - se sobreponena cualquier medida o norma en contrario, incluso dispositivos contractuales (art. 2).[56]

Además de reiterar las reglas establecidas en la Ley General de Telecomunicaciones - como la obligación de garantizar el secreto de las comunicaciones, la intimidad y protección de datos personales de los usuarios[57] y de implementar medidas técnicas de seguridad[58] -, el decreto detalla procedimientos de seguridad que deben ser observados por los operadores y proveedores de los servicios de telecomunicación. Asimismo, la autoridad de telecomunicaciones tiene competencia para velar por el cumplimiento de las obligaciones establecidas por ambas normas (art. 9), y debe ser informada por las prestadoras de servicios de cualquier riesgo a la seguridad de la red. Las empresas de telecomunicaciones deben establecer medidas de seguridad técnicas y administrativas con relación al acceso a información protegida por parte de su personal y detallar en los contratos laborales las políticas y sanciones previstas en casos de infracción (art. 9).[59]

[53]Artículo 45: Los usuarios finales de los servicios de telecomunicaciones disponibles al público tendrán los siguientes derechos: 16) Solicitar la exclusión, sin costo alguno, de las guías de abonados disponibles al público, ya sean impresas o electrónicas. Los abonados podrán decidir cuáles datos personales se incluyen, así como comprobarlos, corregirlos o suprimirlos.

[54] Artículo 77.-Reglamentación de la Ley 1) En un plazo no mayor a nueve meses, contado desde la entrada en vigencia de la presente Ley, el Poder Ejecutivo dictará los siguientes reglamentos:[…] e) Reglamento sobre medidas de protección de la privacidad de las comunicaciones.

[55]http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=65468

[56]Artículo 2: Están sometidos al presente reglamento todos los operadores o proveedores de servicios de telecomunicaciones que usen y exploten redes públicas de telecomunicaciones, independientemente del tipo de red. 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 seguridad de las transacciones electrónicas que desarrollen los usuarios finales de los servicios de telecomunicaciones. Las disposiciones que tutelen la privacidad de las comunicaciones establecidas en la Ley General de Telecomunicaciones y desarrolladas en este Reglamento son irrenunciables y de aplicación obligatoria sobre cualesquiera otras leyes, reglamentos, costumbres, prácticas, usos o estipulaciones contractuales en contrario.

[57]Artículo 6: Los operadores de redes públicas y proveedores de servicios de telecomunicaciones disponibles al público, 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 instalación y operación de los sistemas y las medidas técnicas y administrativas para cumplir ese propósito. Los operadores y proveedores deberán adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios. En caso de que el operador o proveedor conozca de un riesgo identificable en la seguridad de la red, deberá informar a la Superintendenciade Telecomunicaciones y a los usuarios finales sobre dicho riesgo. Los operadores y proveedores deberán garantizar que las comunicaciones y los datos de tráfico asociados a ellas, no serán escuchadas, grabadas, registradas, almacenadas, intervenidas o vigiladas por terceros sin su consentimiento, salvo cuando se cuente con la autorización judicial correspondiente de conformidad con la ley.

[58]Artículo 7: Los proveedores y operadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas y administrativas adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con otros operadores o proveedores de telecomunicaciones en materia de la seguridad de la red. 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 caso de que exista un riesgo particular de violación de la seguridad de la red, el proveedor del servicio de telecomunicaciones deberá informar a sus abonados sobre dicho riesgo. Asimismo corresponderá al proveedor u operador del servicio informar cuando el riesgo quede fuera del ámbito de las medidas que éste deberá tomar, así también sobre las posibles soluciones, los costos y las vulnerabilidades que aún quedan al descubierto.

[59]Artículo 9: La SUTEL mediante el presente reglamento velará, por el cumplimiento del mandato establecido en el artículo 42 de la Ley Nº 8642 en donde se le ordena a los operadores y proveedores de servicios de Telecomunicaciones garantizar la confidencialidad de las comunicaciones realizadas a través de sus redes y de los servicios de telecomunicación que brindan. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los mismos, salvo cuando exista autorización judicial para hacerlo de conformidad con la ley vigente o a fin de fiscalizar la calidad del servicio, siempre y cuando, el usuario final sea informado previamente.Los proveedores deberán garantizar que el personal autorizado para acceder a los datos objeto de este reglamento, adopten las medidas técnicas y administrativas que impidan su manipulación o uso para fines distintos de los comprendidos en este reglamento, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, quedarán sujetos a las sanciones administrativas y penales correspondientes. Los operadores o proveedores deberán advertir, en los contratos de trabajo de su personal, directrices, políticas institucionales, o cualquier otro medio que considere oportuno, especialmente aquellos funcionarios o trabajadores que tengan acceso a datos sensibles y personalísimos de los usuarios, sobre las sanciones administrativas o laborales, civiles y penales a las que se verán expuestos en caso de infringir y lesionar los derechos de los usuarios.

El decreto también establece reglas detalladas sobre la inclusión de los datos de los usuarios en las guías de abonados - que debe darse solamente bajo consentimiento expreso. En el caso de las guías telefónicas electrónicas, los proveedores deberán informar las posibilidades de uso que puede implicar la inclusión de datos en este formato (art. 10).[60]

El consentimiento es considerado válido cuando el usuario - al suscribir el contrato de prestación de servicios telefónicos - informe por escrito que acepta entregar sus datos para la inclusión en la guía de abonados. La inclusión de datos adicionales dependerá de un nuevo consentimiento expreso (art. 12).[61] Aún así, los usuarios tendrán derecho a que sus datos no sean utilizados para otros fines (como publicidad u otros) sin su autorización y a omitir parcialmente, acceder, corregir, rectificar, suprimir o eliminar sus datos personales de manera gratuita (art. 13).[62]

A pesar de establecer procedimientos para la eliminación o anonimización de datos de carácter personal utilizados para se establecer una comunicación o para fines de facturación, el decreto obliga la conservación de diversos datos relacionados a los registros de comunicación (art. 28). Dichos datos deben ser mantenidos de forma confidencial (art. 29)[63] y podrán ser puestos a disposición bajo consentimiento del titular u orden judicial. Cabe resaltar que el decreto no establece un plazo máximo para la retención de datos de manera general; no obstante, en caso que sean datos de carácter personal sobre el tráfico, deberán ser eliminados o anonimizados cuando ya no sean necesarios a efectos de su transmisión; y sólo se podrán conservar aquellos datos para la facturación y los pagos de las interconexiones durante el plazo en el que pueda impugnarse la factura o exigirse el pago, luego de ello igual se solicita que sean eliminados o anonimizados (art. 25 y 26).

[60]Artículo 10: Todos los abonados al servicio telefónico disponible al público, tendrán derecho a figurar en la guía de abonados. Los proveedores deberán informar gratuitamente a sus abonados antes de incluir o facilitar sus datos a otra persona física o jurídica que tenga como destino incluirlos en cualquier tipo de guía de abonados, sea impresa o electrónica, disponible al público o accesible a través de servicios de información o de consulta sobre ella. Deberán informar además al abonado acerca de cualquier otra posibilidad de uso basada en funciones de búsqueda incorporadas en sus versiones electrónicas. Dicha información a los abonados deberá producirse al menos dos meses de antelación a que los datos sean incluidos o facilitados a otra entidad para su inclusión, y se les deberá solicitar su consentimiento, en los términos establecidos en los apartados siguientes.

[61]Artículo 12: Para que los datos correspondientes a un abonado sean incluidos en algún tipo de guía o facilitados a otra entidad para su inclusión en ella o para la prestación de servicios de información o de consulta sobre ella, será preciso el consentimiento expreso del abonado. A estos efectos, se entenderá que existe consentimiento del abonado, cuando al suscribir el contrato de prestación del servicio telefónico, exprese por escrito su consentimiento para que sus datos se entreguen a fin de ser incluidos en la guía telefónica o para la prestación de servicios de información o de consulta sobre ella. Para las sucesivas inclusiones de dichos datos en la guía o su entrega a otra entidad para su inclusión en ella o para la prestación de servicios de información o de consulta sobre ella, bastará que en el plazo de un mes, después del anuncio en el que se informa el inicio de la elaboración de la guía, que el abonado no se oponga expresamente a su inclusión. La inclusión en una guía, impresa o electrónica, de cualquier dato distinto de los previstos en este reglamento, exigirá el consentimiento expreso del abonado para ello. Aparecerán también, los datos de los abonados del servicio telefónico móvil que hayan solicitado a su proveedor del servicio su deseo de aparecer en ellas, y los datos de los abonados que tengan números no geográficos asignados, conforme al Plan Nacional de Numeración. Cuando se trate del servicio telefónico fijo y el titular sea una persona física, podrá solicitar que asociado a un mismo número figure el nombre de otra persona mayor de edad. La solicitud de dicha inscripción se realizará de manera conjunta.

[62]Artículo 13: Los abonados tendrán derecho a que los datos que aparecen en la guía no sean utilizados sin su consentimiento con fines de publicidad u otro fin comercial. Del mismo modo tendrán derecho a que se omita parcialmente su dirección o algún otro dato. Asimismo, podrán ejercer los derechos de acceso, corrección, rectificación, supresión o eliminación de sus datos personales, sin cobro alguno.

[63]Artículo 29: Los operadores adoptarán las medidas necesarias para garantizar que los datos se conserven de conformidad con lo dispuesto en este reglamento, en la medida en que sean generados o tratados por aquellos en el marco de la prestación de los servicios de telecomunicación de que se trate. Todos estos datos serán confidenciales y no podrán hacerse públicos ni ser entregados a persona física o jurídica alguna, si no es con la autorización expresa del abonado o su representante; o por orden judicial conforme a la legislación vigente. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los proveedores. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en este reglamento.

En caso que el proveedor quiera dar un uso distinto a datos de tráfico u otros datos de localización (por ejemplo para promoción comercial u oferta de servicios de valor agregado), es necesario el consentimiento de los usuarios el cual puede ser retirado en cualquier momento (art. 25 y 26).[64] [65] Los datos de localización, distintos de los datos de tráfico, pueden ser tratados si se hacen anónimos aunque no haya consentimiento del titular (art. 30).[66] Adicionalmente, es menester señalar que aquellos datos que revelen contenido de la comunicación no podrán conservarse (art.28).

[64]De conformidad con lo establecido en los artículos 42 y 43 de la Ley Nº 8642, los operadores y proveedores de servicios de telecomunicaciones deberán eliminar o hacer anónimos los datos de carácter personal sobre el tráfico referidos a una comunicación y relacionados con los abonados y usuarios finales que hayan sido tratados y almacenados para establecer una comunicación, en cuanto ya no sean necesarios a los efectos de su transmisión. Los datos de tráfico que fueran necesarios para realizar la facturación y los pagos de las interconexiones, podrán ser tratados únicamente durante el plazo en que pueda impugnarse la factura o exigirse el pago, de conformidad con la legislación aplicable. Transcurrido dicho plazo, los operadores deberán eliminar o hacer anónimos los datos de carácter personal, en los términos del inciso anterior. Los operadores y los proveedores, deberán solicitar el consentimiento del abonado o usuario final, al menos, con un mes de antelación al inicio de la prestación del servicio, con el fin de informar sobre el tratamiento que se le dará a sus datos; informándole sobre los tipos de datos que serán tratados y el plazo durante el cual serán utilizados. Esta comunicación, deberá efectuarse a través de cualquier medio que garantice su recepción efectiva por parte del abonado o usuario final; pudiendo llevarse a cabo de forma conjunta con la facturación del servicio prestado. Deberá facilitarse al abonado o usuario final un medio sencillo (número telefónico gratuito, sitio de Internet), que no le implique gasto alguno; para manifestar su negativa o aceptación del tratamiento de los datos citados. Si en el plazo de un (1) mes a partir de recibida la solicitud de consentimiento por parte del abonado o usuario, éste no se hubiese pronunciado al respecto, se entenderá que consiente el tratamiento de sus datos de tráfico y localización para esta finalidad; siempre que así se hubiera hecho constar en la información dirigida al abonado o usuario. En todo caso, los abonados o usuarios dispondrán de la posibilidad de retirar en cualquier momento su consentimiento. El tratamiento de los datos de tráfico y localización, realizado de conformidad con los incisos anteriores, sólo podrá ser efectuado por el personal a cargo del operador o proveedor cuyo abonado o usuario está asociado a estos datos. Cuando se haya obtenido el consentimiento de un abonado o usuario para el tratamiento de datos de localización distintos de los datos de tráfico, el abonado o usuario deberá seguir contando con la posibilidad, por un procedimiento sencillo y gratuito, de rechazar temporalmente el tratamiento de tales datos para cada conexión a la red o para cada transmisión de una comunicación.

[65]Artículo 26: Los operadores y proveedores deberán eliminar o hacer anónimos los datos de carácter personal sobre el tráfico referidos a una comunicación y relacionados con los usuarios y los abonados que hayan sido tratados y almacenados para establecer una comunicación, en cuanto ya no sean necesarios a los efectos de su transmisión, sin perjuicio de lo dispuesto en los apartados siguientes. Los datos de tráfico que fueran necesarios para realizar la facturación y los pagos de las interconexiones, podrán ser almacenados únicamente durante el plazo en que pueda impugnarse la factura o exigirse el pago, de conformidad con la legislación aplicable. Transcurrido dicho plazo, los operadores o proveedores deberán eliminar o hacer anónimos los datos de carácter personal. Asimismo, podrán emplear los datos de tráfico con fines de promoción comercial de servicios de telecomunicaciones o para la prestación de servicios con valor agregado, en la medida y durante el tiempo necesarios para la prestación de tales servicios o su promoción comercial, siempre y cuando el abonado haya dado su consentimiento. A estos efectos, los sujetos obligados deberán dirigirse a los abonados, al menos, con un mes de antelación al inicio de la promoción o de la prestación del servicio con valor añadido, informarles del tipo de servicios para los que se efectuará el tratamiento, los tipos de datos que serán objeto de tratamiento y la duración que tendrá y solicitarles su consentimiento para el tratamiento de los datos. Esta comunicación, que deberá efectuarse a través de un medio que garantice su recepción por parte del abonado, podrá llevarse a cabo de manera conjunta a la facturación del servicio prestado por los sujetos obligados al abonado. Deberá facilitarse al interesado un medio sencillo y que no implique ingreso alguno para el sujeto obligado, para manifestar su negativa al tratamiento de los datos. Si en el plazo de un mes desde que el abonado reciba la solicitud éste no se hubiese pronunciado al respecto, se entenderá que consiente el tratamiento de los datos de tráfico para esta finalidad, siempre que así se hubiera hecho constar en la información dirigida al abonado. En todo caso, los abonados dispondrán de la posibilidad de retirar en cualquier momento su consentimiento para el tratamiento de sus datos de tráfico al que se refiere este apartado. El operador deberá informar al abonado o al usuario de los tipos de datos de tráfico que son tratados y de la duración de este tratamiento y antes de obtener el consentimiento. El tratamiento de los datos de tráfico, de conformidad con los apartados anteriores, sólo podrá realizarse por las personas que actúen bajo la autoridad del proveedor que se ocupen de la facturación o de la gestión del tráfico, de las solicitudes de información de los abonados, de la detección de fraudes, de la promoción comercial de los servicios de telecomunicaciones, de la prestación de un servicio con valor agregado o de suministrar la información requerida por la administración judicial. En todo caso, dicho tratamiento deberá limitarse a lo necesario para realizar tales actividades.

[66]Artículo 30: Cuando se trate de datos de localización, distintos a los datos de tráfico, relativos a los usuarios o abonados de redes y servicios de telecomunicaciones disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento expreso de los usuarios o abonados, en la medida y por el tiempo necesarios para la prestación de un servicio con valor agregado. A estos efectos, los proveedores deberán dirigirse a los usuarios o abonados, al menos con un mes de antelación al inicio de la prestación del servicio con valor agregado, e informarles del tipo de datos de localización distintos de los datos de tráfico que serán tratados, la finalidad y duración del tratamiento y si los datos se transmitirán a un tercero a los efectos de la prestación del servicio con valor agregado. Para estos efectos se deberá contar con el consentimiento del usuario o abonado para el tratamiento de los datos. Esta comunicación, que deberá efectuarse por un medio que garantice su recepción por el usuario o abonado, podrá llevarse a cabo de manera conjunta a la facturación del servicio prestado por los sujetos obligados al abonado. Se entenderá que existe consentimiento expreso cuando el usuario o el abonado se dirijan al sujeto obligado y le soliciten la prestación de los servicios con valor agregado que exijan el tratamiento de sus datos de localización. En todo caso, los usuarios o abonados deberán tener la posibilidad de retirar en cualquier momento, su consentimiento para el tratamiento de sus datos de localización distintos de los de tráfico al que se refiere este apartado, así como de rechazar temporalmente el tratamiento de tales datos, mediante un procedimiento sencillo y gratuito, para cada conexión a la red o para cada transmisión de una comunicación. Sólo podrán encargarse del tratamiento de datos de localización distintos de los datos de tráfico las personas que actúen bajo la autoridad del proveedor o del tercero que preste el servicio con valor agregado, y dicho tratamiento deberá limitarse a lo necesario a efectos de la prestación del servicio con valor agregado. No obstante lo dispuesto en este artículo, los proveedores facilitarán los datos de localización distintos a los datos de tráfico a la Comisión Coordinadora del Sistema de Emergencias 9-1-1 y a las instituciones que ésta indique.

Finalmente, está el Reglamento sobre el Régimen de Protección al Usuario Final de los Servicios de Telecomunicaciones, publicado por la Autoridad Reguladora de los Servicios Públicos de Costa Rica.[67] El reglamento detalla los procedimientos de reclamación por violaciones a la intimidad por parte de los usuarios de los servicios de telecomunicaciones (arts. 9, 10, 11 y 12), además de las sanciones por violación (art. 75), y reitera las reglas de protección de privacidad e intimidad garantizados en las normas de telecomunicaciones mencionadas anteriormente (arts. 4 y 6).

4.e Ley de Protección de datos personales

Costa Rica es uno de los países de la región que posee una ley general sobre la protección de datos personales, la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (Ley N° 8968/2011)[68]. Esta busca garantizar el derecho a la autodeterminación informativa con respecto al tratamiento automatizado o manual de datos personales (art. 1)[69] y se aplica a los entes públicos y privados.

La definición de datos personales es amplia, englobando datos relativos a personas identificadas o identificables. La ley además define datos sensibles como aquellos relacionados, por ejemplo, al origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, orientación sexual, etc. Por otra parte, existe una categoría de datos personales de acceso irrestricto, que son aquellos que por ley están disponibles en bases de datos de acceso general. Entre ellos no se incluyen la dirección exacta, citación o notificación administrativa o judicial, número de teléfono privado, entre otros. (art. 9, 3)

Entre los principios de protección de datos personales, la ley reconoce el consentimiento informado (art. 5)[70] y la calidad de la información, o sea, actualidad, veracidad, exactitud y adecuación al fin (art. 6)[71].

[67] http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=67664&nValor3=80265&strTipM=TC
[68] http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC
[69] Artículo 1: Esta ley es de orden público y tiene como objetivo 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.
[70] Artículo 5: 1.- Obligación de informar Cuando se soliciten datos de carácter personal será necesario informar de previo a las personas titulares o a sus representantes, de modo expreso, preciso e inequívoco: a) De la existencia de una base de datos de carácter personal. b) De los fines que se persiguen con la recolección de estos datos. c) De los destinatarios de la información, así como de quiénes podrán consultarla. d) Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se le formulen durante la recolección de los datos. e) Del tratamiento que se dará a los datos solicitados. f) De las consecuencias de la negativa a suministrar los datos. g) De la posibilidad de ejercer los derechos que le asisten. h) De la identidad y dirección del responsable de la base de datos. Cuando se utilicen cuestionarios u otros medios para la recolección de datos personales figurarán estas advertencias en forma claramente legible. 2.- Otorgamiento del consentimiento Quien recopile datos personales deberá obtener el consentimiento expreso de la persona titular de los datos o de su representante. Este consentimiento deberá constar por escrito, ya sea en un documento físico o electrónico, el cual podrá ser revocado de la misma forma, sin efecto retroactivo. No será necesario el consentimiento expreso cuando: 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 irrestricto, obtenidos de fuentes de acceso público general. c) Los datos deban ser entregados por disposición constitucional o legal. Se prohíbe el acopio de datos sin el consentimiento informado de la persona, o bien, adquiridos por medios fraudulentos, desleales o ilícitos.
[71] Artículo 6: Sólo podrán ser recolectados, almacenados o empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean actuales, veraces, exactos y adecuados al fin para el que fueron recolectados. 1.- Actualidad Los datos de carácter personal deberán ser actuales. El responsable de la base de datos eliminará los datos que hayan dejado de ser pertinentes o necesarios, en razón de la finalidad para la cual fueron recibidos y registrados. En ningún caso, serán conservados los datos personales que puedan afectar, de cualquier modo, a su titular, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que disponga otra cosa. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados de su titular. 2. Veracidad Los datos de carácter personal deberán ser veraces. La persona responsable de la base de datos está obligado a modificar o suprimir los datos que falten a la verdad. De la misma manera, velará por que los datos sean tratados de manera leal y lícita. 3.- Exactitud Los datos de carácter personal deberán ser exactos. La persona responsable de la base de datos tomará las medidas necesarias para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados. Si los datos de carácter personal registrados resultan ser inexactos en todo o en parte, o incompletos, serán eliminados o sustituidos de oficio por la persona responsable de la base de datos, por los correspondientes datos rectificados, actualizados o complementados. Igualmente, serán eliminados si no media el consentimiento informado o está prohibida su recolección. 4.- Adecuación al fin Los datos de carácter personal serán recopilados con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. No se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando se establezcan las garantías oportunas para salvaguardar los derechos contemplados en esta ley. Las bases de datos no pueden tener finalidades contrarias a las leyes ni a la moral pública.

A pesar de eso, la ley establece una serie de excepciones a la autodeterminación informativa y los principios garantizados anteriormente - algunos de los cuales podrían dar margen a abusos por traer un lenguaje genérico, como por ejemplo: la seguridad del Estado y de la autoridad pública; la prevención, persecución, investigación y represión de infracciones penales o de la deontología en las profesiones y el funcionamiento de la administración pública (art. 8).[72] Las limitaciones deben ser justas, razonables y transparentes (art. 8).

La ley además crea una Agencia de Protección de Datos de los Habitantes en el ámbito del Ministerio de Justicia y Paz (art. 15)[73] con competencias para fiscalizar el cumplimiento de la ley por parte de entes públicos o privados, resolver reclamos relacionados a la infracción de normas de protección de datos, imponer sanciones en caso de infracción, dictar directrices sobre el manejo de informaciones privadas por parte de órganos públicos, entre otras (art. 16).[74] Asimismo, ante esta agencia los responsables del tratamiento de datos personales deberán inscribir los Protocolos de Actuación y registrar las bases de datos que tengan a su titularidad (ar. 12 y 21). Finalmente, la ley establece las sanciones administrativas en el caso de violaciones leves, graves o gravísimas y (arts. 28 al 31).

El Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales fue publicado a través del Decreto Ejecutivo N° 37554/2012[75], que reafirma las garantías previstas en la ley y detalla algunos procedimientos. Por ejemplo, determina que el consentimiento para el tratamiento de datos personales debe ser expreso, libre, inequívoco, informado, individualizado y específico (art. 2 y 4) y establece el proceso gratuito que debe ser observado para su revocación (art. 7 y 8).

El decreto determina que la conservación de datos personales que pueden afectar al titular no debe exceder 10 años desde la fecha de terminación del objeto de tratamiento del dato, salvo disposiciones en contrario, a menos que por acuerdo entre las partes se haya establecido un plazo distinto, que exista una relación continuada entre las partes, o que medie interés público para conservar el dato (art. 11).[76]

[72] Artículo 8: Los principios, los derechos y las garantías aquí establecidos podrán ser limitados de manera justa, razonable y acorde con el principio de transparencia administrativa, cuando 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.

[73]Artículo 15: Créase un órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz denominado Agencia de Protección de Datos de los habitantes (Prodhab). Tendrá personalidad jurídica instrumental propia en el desempeño de las funciones que le asigna esta ley, además de la administración de sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones. La Agencia gozará de independencia de criterio.

[74]Artículo 16: Son atribuciones de la Prodhab, además de las otras que le impongan esta u otras normas, las siguientes: a) Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas o jurídicas privadas, como por entes y órganos públicos. b) Llevar un registro de las bases de datos reguladas por esta ley. c) Requerir, de quienes administren bases de datos, las informaciones necesarias para el ejercicio de su cargo, entre ellas, los protocolos utilizados. d) Acceder a las bases de datos reguladas por esta ley, a efectos de hacer cumplir efectivamente las normas sobre protección de datos personales. Esta atribución se aplicará para los casos concretos presentados ante la Agencia y, excepcionalmente, cuando se tenga evidencia de un mal manejo generalizado de la base de datos o sistema de información. e) Resolver sobre los reclamos por infracción a las normas sobre protección de los datos personales. f) Ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de las informaciones contenidas en los archivos y las bases de datos, cuando éstas contravengan las normas sobre protección de los datos personales. g) Imponer las sanciones establecidas, en el artículo 28 de esta ley, a las personas físicas o jurídicas, públicas o privadas, que infrinjan las normas sobre protección de los datos personales, y dar traslado al Ministerio Público de las que puedan configurar delito. h) Promover y contribuir en la redacción de normativa tendiente a implementar las normas sobre protección de los datos personales. i) Dictar las directrices necesarias, las cuales deberán ser publicadas en el diario oficial La Gaceta, a efectos de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales, respetando los diversos grados de autonomía administrativa e independencia funcional. j) Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, el almacenamiento, la transferencia y el uso de sus datos personales. En el ejercicio de sus atribuciones, la Prodhab deberá emplear procedimientos automatizados, de acuerdo con las mejores herramientas tecnológicas a su alcance.

[75]Disponible en http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=74352

[76] Artículo 11. Derecho al olvido. La conservación de los datos personales que puedan afectar a su titular, no deberá exceder el plazo de diez años, desde la fecha de terminación del objeto de tratamiento del dato, salvo disposición normativa especial que establezca otro plazo, que por el acuerdo de partes se haya establecido un plazo distinto, que exista una relación continuada entre las partes o que medie interés público para conservar el dato. *(Así adicionado el párrafo anterior por el artículo 9 del decreto ejecutivo N° 40008 del 19 de julio de 2016)*

Los derechos al acceso, rectificación, modificación, revocación o eliminación de los datos personales son ratificados por el decreto (arts. 12)[77], que además delimita situaciones en que podrán ser legítimamente restringidos (art. 14).[78] Según el reglamento, los responsables por las bases de datos deben poner a disposición de los titulares un medio simplificado de comunicación para que puedan ejercer sus derechos y los mecanismos de notificación y respuesta. Los titulares tienen también el derecho de obtener información acerca de lo relativo a las condiciones, finalidad y generalidades de su tratamiento y a consultar cada seis meses las bases de datos que contengan sus informaciones (art. 21).[79]

La transferencia de datos personales está sujeta al consentimiento del titular de datos personales. Empero, no se considerará transferencia al traslado de datos personales del responsable de la base de datos a un encargado, proveedor de servicios o intermediario tecnológico o las empresas del mismo grupo de interés tecnológico (art. 40).[80] El receptor de los datos debe asumir como mínimo las mismas obligaciones que tenía el responsable por la transferencia mediante contrato firmado por ambas partes (art. 43), pero no hay requisitos legales mínimos para la transferencias internacionales de datos.

Las personas físicas o jurídicas propietarias de bases de datos personales deben registrarlas en la Agencia de Protección de Datos de los Habitantes (art. 44), informando - entre otras cosas - los responsables y encargados de las bases, sus finalidades y usos previstos, los tipos de datos sometidos a tratamiento, el procedimiento de obtención de los datos personales, las medidas de seguridad implementadas, entre otros datos.[81] El registro incluye el pago de un

[77]Artículo 12: Es el derecho fundamental de toda persona física, a conocer lo que conste sobre ella, sus bienes o derechos en cualquier base de datos, de toda naturaleza, pública o privada, el fin para el cual está siendo utilizada o recabada su información personal, así como exigir que sea rectificada, actualizada, complementada o suprimida, cuando la misma sea incorrecta o inexacta, o esté siendo empleada para un fin distinto del autorizado o del que legítimamente puede cumplir.

[78]Artículo 14: El ejercicio de los derechos mencionados en el artículo anterior, podrá restringirse por razones de seguridad nacional, disposiciones de orden público y salud pública o para proteger los derechos de terceras personas, en los casos y con los alcances previstos en las leyes aplicables en la materia, mediante resolución de la autoridad competente debidamente fundamentada y motivada.

[79]Artículo 21: El titular tiene derecho a obtener del responsable, la información relacionada con sus datos personales, entre ellos lo relativo a las condiciones, finalidad y generalidades de su tratamiento. Podrá realizar las consultas de información a la base de datos, con un intervalo mínimo de seis meses, salvo que de manera fundamentada el titular exprese al responsable de la base de datos sus motivos y pruebas, por los cuales considera existe una vulneración de sus derechos protegidos en la Ley y el presente Reglamento. En caso de que el responsable de la base de datos considere que los motivos no son de recibo y existiera la posibilidad de un uso abusivo de ese derecho, dentro de los cinco días hábiles siguientes a la solicitud, elevará el asunto ante la PRODHAB, quien resolverá en definitiva, dentro del plazo de diez días hábiles, a partir de la recepción de dicha gestión. El responsable, deberá evacuar la consulta de información dentro del plazo de cinco días hábiles a partir de la recepción de la solicitud.

[80] Artículo 40. Condiciones para la transferencia. La transferencia requerirá siempre el consentimiento inequívoco del titular. La transferencia implica la cesión de datos personales por parte, única y exclusivamente, del responsable que transfiere al responsable receptor de los datos personales. Dicha transferencia de datos personales requerirá siempre del consentimiento informado del titular, salvo disposición legal en contrario, asimismo que los datos a transferir hayan sido recabados o recolectados de forma lícita y según los criterios que la Ley y el presente Reglamento dispone. No se considera transferencia el traslado de datos personales del responsable de una base de datos a un encargado, proveedor de servicios o intermediario tecnológico o las empresas del mismo grupo de interés económico.
Toda venta de datos del fichero o de la base de datos, parcial o total, deberá reunir los requerimientos establecidos en el párrafo anterior. *(Así adicionado el párrafo anterior por el artículo 9 del decreto ejecutivo N° 40008 del 19 de julio de 2016)*

[81]Artículo 44. **Inscripción del registro de base de datos**. Las personas físicas o jurídicas propietarias de bases de datos personales, de conformidad con la Ley y este Reglamento, deberán inscribir ante la Agencia un registro de dichas bases de datos, proporcionando la siguiente información: **a)** Solicitud del propietario físico o jurídico, debidamente autenticado notarialmente o confrontada la firma. En el caso de persona jurídica deberá presentarse personería jurídica vigente con máximo un mes de haber sido expedida; **b)** Designación del responsable de la base de datos personales ante la Agencia y ante terceros, con indicación del medio y lugar de contacto. Así como carta de aceptación del cargo y las responsabilidades inherentes al mismo. **c)** Identificación de los encargados, incluyendo sus datos de contacto, así como carta de aceptación del cargo y las responsabilidades inherentes al mismo. *(Reformado el inciso anterior por el artículo 9° del decreto ejecutivo N° 40008 del 19 de julio de 2016)* **d)** Nombres de las bases de datos y su ubicación física; **e)** Especificación de las finalidades y los usos previstos de la base de datos. *(Reformado el inciso anterior por el artículo 9° del decreto ejecutivo N° 40008 del 19 de julio de 2016)* **f)** Tipos de datos personales sometidos a tratamiento en dichas bases de datos;**g)** Procedimientos de obtención, según el consentimiento informado, de los datos personales. *(Reformado el inciso anterior por el artículo 9° del decreto ejecutivo N° 40008 del 19 de julio de 2016)* **h)** Descripción técnica de las medidas de seguridad que se utilizan en el tratamiento de los datos personales, según lo dispuesto en el presente Reglamento; **i)** Los destinatarios de transferencias de los datos personales; **j)** Copia de los protocolos mínimos de actuación; *(Reformado el inciso anterior por el artículo 9 del decreto ejecutivo N° 40008 del 19 de julio de 2016)* **k)** Listado de los contratos globales y ventas de ficheros vigentes, así como indicación de la estimación pecuniaria de cada uno de esos contratos. **l)** *(Derogado por el artículo 11° del decreto ejecutivo N° 40008 del 19 de julio de 2016)* **m)** Señalamiento de fax o correo electrónico para recibir notificaciones de la Agencia. Asimismo, el responsable deberá mantener el registro de la base de datos, en todo momento, actualizados ante la Agencia, según lo establecido en el presente Reglamento. No serán sujetas de inscripción ante la Agencia, las

canon anual de 200 USD[82] por base de datos (arts. 50 y 78) y la revisión por parte de la Agencia, que puede declarar improcedente el registro (art. 53). Además, la Agencia podrá en cualquier momento revisar las bases de datos cuando haya denuncia o evidencia de mal manejo (art. 47). [83] Mediante Decreto Ejecutivo N° 40008 - JP del 19 de julio de 2016[84], se derogó la figura de "superusuario" que hacía las veces de un "usuario de consulta" que se lel responsable de la base de datos electrónica entregaba a la Agencia, para que ésta pueda consultar la base de datos en cualquier momento y sin restricción alguna.

Las reglas de protección de datos personales de Costa Rica no incluyen a bases de datos mantenidas por personas jurídicas o físicas, públicas o privadas, con fines exclusivamente internos, domésticos o personales - que no sean comercializadas (art. 3). Sin embargo, no se prevén excepciones específicas para la actividad periodística o de otros tipos de organizaciones sin fines de lucro, comunitarias, etc.

4.f Observación a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones

La Ley sobre Registro, Secuestro, y Examen de Documentos Privados e Intervención de las Comunicaciones (N° 7425/1994) puede ser considerada como un ejemplo de buena práctica legal con relación al principio de necesidad. Esta dispone que las solicitudes de intervención de comunicaciones sean justificadas por escrito para permitir la debida valoración por el Tribunal de Justicia (art. 10). Además, en el caso del secuestro de documentos, la ley determina que se especifique los documentos solicitados de manera individualizada (art. 3) y que "los resultados de la intervención de las comunicaciones orales o escritas no podrán ser utilizados para ningún propósito distinto del que motivó la medida" (arts. 22 y 28), lo que también responde al principio de necesidad.

Con relación al principio de debido proceso, la ley costarricense lo cumple parcialmente. Por ejemplo, la guía de implementación de Access Now recomienda que las solicitudes de intervención de comunicaciones se hagan por escrito con la identificación de los solicitantes y que los extremos que la motivan sean explicitados. Sin embargo, la ley N° 7425/1994 determina que las solicitudes sean presentadas en forma escrita con la identificación de los responsables por la investigación (art. 10), pero no detalla si habrán procedimientos para su fundamentación.

No fue encontrada ninguna garantía en cuanto a la notificación de ciudadanos afectados por la intervención en sus comunicaciones privadas en las normas analizadas. Sin embargo, tampoco fueron encontradas prohibiciones a que los proveedores ofrezcan ese tipo de notificación a sus usuarios. De manera similar, no fueron encontradas prohibiciones a que las empresas publiquen reportes de transparencia o informaciones estadísticas sobre las solicitudes de datos y de intervención en las comunicaciones. De todo modo, se entiende que los proveedores deben observar las reglas de la ley de protección de datos personales al hacer cualquier tipo de publicación del estilo.

Costa Rica prevé medidas administrativas y civiles, como así, penas criminales en el caso de acceso, difusión y uso indebido de informaciones personales y del contenido de las comunicaciones privadas obtenido a través de la intervención en las comunicaciones en el Código Penal, la Ley sobre Registro, Secuestro, y Examen de Documentos Privados e Intervención de las Comunicaciones y la Ley de Protección de Datos Personales. De esta forma, cumple con el principio que trata de las garantías contra el acceso ilegítimo y derecho a recurso específico.

A pesar de las garantías presentes en las normas costarricenses, se han registrados violaciones a la privacidad en los últimos años. El caso más grave se refiere al espionaje de un periodista del Diario Extra por parte del Organismo de

bases de datos personales, internas o domésticas. *Así adicionado el párrafo anterior por el artículo 9 del decreto ejecutivo N° 40008 del 19 de julio de 2016)*

[82]Artículo 78: De conformidad con la Ley, todas las bases de datos, públicas o privadas, con fines de distribución, difusión o comercialización, deben inscribirse ante la Agencia, y por ende cancelar ante ésta, la suma de doscientos dólares moneda de curso legal de los Estados Unidos de América (USD $200,00), al tipo de cambio mayor de referencia de venta del Banco Central de Costa Rica del día en que se realice el pago. Dicho monto corresponde al canon anual de regulación y administración de las bases de datos.

[83]Artículo 47: La Agencia podrá en cualquier momento y de oficio acceder a las bases de datos manuales sin restricción alguna, cuando exista denuncia presentada ante la Agencia o se tenga evidencia de un mal manejo de la base de datos o sistema de información. Para tales efectos, la Agencia deberá establecer lineamientos que garanticen el debido cumplimiento del secreto profesional o funcional, y para todos los casos llevar una bitácora en donde al menos se consignen el motivo, los accesos y consultas realizadas, así como el funcionario asignado que los realice.

[84]http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=83048&nValor3=106478&strTipM=TC

Investigación Judicial (OIJ)[85] y trajo preocupación a organizaciones internacionales como Reporteros sin Fronteras.[86] La acción fue declarada ilegal por la Sala Constitucional por violar los principios de proporcionalidad y necesidad. A pesar de la condena, no hubo hasta el momento punición de los agentes involucrados en el caso, según informa el propio Diario Extra. Los medios además registran uso de espionaje en contra empleados en el interior de organismos estatales para instaurar procesos administrativos.[87]

Por otro lado, la decisión de la Sala Constitucional en favor del jugador del Real Madrid, Keylor Navas, en contra del OIJ y la Fiscalía por revisar su información privada sin orden judicial[88] parece evidenciar que la corte más alta del país está preparada para identificar abusos y aplicar los principios de derechos humanos previstos en la legislación nacional - lo que refuerza también el cumplimiento con el principio de debido proceso. Aún así es preocupante que las víctimas de intervenciones ilegales tengan que recurrir a las cortes para hacer valer sus derechos, principalmente considerando la ausencia de garantías de notificación en las normas analizadas.

5. Anexo: preocupaciones por la libertad de expresión

El Estado de Costa Rica ha sido condenado en 2004 por la Corte Interamericana de Derechos Humanos por violar el derecho a la libertad de expresión previsto en el artículo 13 de la Convención Americana sobre Derechos Humanos. El caso Herrera Ulloa v. Costa Rica[89] discutió la condena criminal del periodista Mauricio Herrera Ulloa por difamación. El caso se refería a la publicación de una serie de artículos en el periódico La Nación sobre un diplomático costarricense acusado de cometer actividades ilegales en Bélgica. Además de la condena criminal y civil en contra del periodista y del periódico, la sentencia de 1999 del Tribunal Penal del Primer Circuito Judicial de San José estableció una espécie de "derecho al olvido" al ordenar la retirada del "enlace" existente en La Nación Digital entre el apellido del diplomático y los artículos presuntamente difamatorios. La orden fue comparada a censura previa por parte de la Comisión (párrafo 101.5).[90]

En su decisión, la Corte resaltó la condición particular de la protección del honor de los funcionarios públicos y personas que ejercen funciones de naturaleza pública (para. 128)[91], que están sujetas a un escrutinio público más

[85]El caso, ocurrido entre 2013 y 2014, estableció el vínculo de diferentes agentes judiciales quienes procedieron a escuchar las llamadas del comunicador Manuel Estrada, con el fin de conocer sus fuentes de información. Ver la denuncia del Diario Extra en: http://www.diarioextra.com/Dnew/noticiaDetalle/223266.

[86]La organización clasificó Costa Rica en el 6o lugar en su ranking mundial de libertad de prensa en 2016, pero llamó atención a la gravedad del caso de espionaje del periodista Manuel Estrada del Diario Extra. Ver: https://rsf.org/es/noticias/diario-extra-es-victima-de-espionaje-un-escandalo-que-recuerda-al-de-ap. La posición del país en el ranking fue cuestionada en algunos medios que apuntan a un escenario de violaciones a la libertad de expresión e información. Ver la nota del Diario Extra sobre el tema: http://www.diarioextra.com/Noticia/detalle/290046/reporteros-sin-fronteras--desconoce-realidad-de-pais.

[87]En 2016, la Sala Constitucional condenó el Instituto Costarricense de Acueductos y Alcantarillados (AyA) por "haber espiado a una empleada, usar comunicaciones privadas y grabarlas para luego usarlas en su contra en un proceso administrativo para despedirla", según reportó el Diario Extra. Ver: http://www.diarioextra.com/Noticia/detalle/308158/sala-iv-condena-al-aya-por-espionaje.

[88]El caso fue decidido en 2016, pero remite a hechos de 2014. Ver: http://www.nacion.com/sucesos/poder-judicial/IV-OIJ-Fiscalia-Keylor-Navas_0_1553044771.html.

[89]http://www.corteidh.or.cr/docs/casos/articulos/seriec_107_esp.pdf

[90]101.5) Respecto de la orden de retirar el enlace existente en "La Nación" Digital entre el apellido Przedborski y los artículos querellados escritos por Mauricio Herrera Ulloa y de establecer un vínculo entre dichos artículos y la parte dispositiva de la sentencia condenatoria, la Comisión alegó que: a) la orden de retirar dicho enlace constituye una intromisión y una censura previa de la información por parte del Estado que viola el artículo 13 de la Convención. A su vez, la orden de establecer otro enlace con la parte dispositiva de la sentencia condenatoria constituye una restricción a la libertad de expresión, por cuanto impone el contenido de la información, lo cual está fuera del marco de las limitaciones permitidas por el artículo 13 de la Convención; b) tales órdenes dispuestas en la sentencia condenatoria tienen como efecto directo la censura previa, la cual supone el control y veto de la información antes de que ésta última sea difundida, impidiendo tanto al individuo, cuya expresión ha sido censurada, como a la totalidad de la sociedad, ejercer su derecho a la libertad de expresión e información. Asimismo, afectan al periodista en su derecho a difundir información sobre temas de legítimo interés público que se encuentran disponibles en la prensa extranjera; y c) la prohibición de censura previa para proteger el honor de un funcionario público es absoluta y no encuentra justificación alguna en las excepciones dispuestas en el artículo 13 de la Convención.

[91]128. En este contexto es lógico y apropiado que las expresiones concernientes a funcionarios públicos o a otras personas que ejercen funciones de una naturaleza pública deben gozar, en los términos del artículo 13.2 de la Convención, de un margen de apertura a un debate amplio respecto de asuntos de interés público, el cual es esencial para el funcionamiento de un sistema verdaderamente democrático. Esto no significa, de modo alguno, que el honor de los funcionarios públicos o de las personas públicas no deba ser jurídicamente protegido, sino que éste debe serlo de manera acorde con los principios del pluralismo democrático.

exigente (para. 129).[92] Además, ordenó al Estado de Costa Rica que dejara sin efecto la sentencia emitida, incluso la relativa a la eliminación de los enlaces que relacionaban los artículos al diplomático.

6. Bibliografía

Access Now, Article 19, et. al. (2013). Necessary and Proportionate: International Principles On The Application Of Human Rights To Communications Surveillance. Disponible en https://necessaryandproportionate.org/es/necesarios-proporcionados

Access Now (2015). Universal Implementation Guide for the International Principles on the Application of Human Rights to Communication Surveillance. Disponible en: https://www.accessnow.org/cms/assets/uploads/archive/docs/Implementation_guide_-_July_10_print.pdf

Constitución Política de Costa Rica. Disponible en: https://www.cne.go.cr/cedo_dvd5/files/flash_content/pdf/spa/doc362/doc362-contenido.pdf

Cooperativa Sulá Batsú. (2016) “Informe Nacional Costa Rica”. En: Asociación para el Progreso de las Comunicaciones (APC), Examinando los derechos y las libertades en Internet en Latinoamérica (EXLILA). Disponible en: https://www.apc.org/es/system/files/EXLILA_informe%20nacional%20Costa%20Rica.pdf

Fundación Acceso. (2015). Privacidad digital para defensores y defensoras de derechos: un estudio sobre cómo los marcos legales de El Salvador, Guatemala, Honduras y Nicaragua pueden ser utilizados para la protección,criminalización y/o vigilancia digital de defensoras y defensores de derechos humanos / Peri, Luciana (coord.). Disponible en: https://acceso.or.cr/assets/files/investigacion-resumen-ejecutivo.pdf

Romero, Roberto Cruz. (2016). “Marco Institucional, Políticas Públicas y Regulación TIC”. En: Universidad de Costa Rica. Programa Sociedad de la Información y el Conocimiento. Hacia la Sociedad de la Información y el Conocimiento en Costa Rica: Informe 2016. Disponible en: http://www.prosic.ucr.ac.cr/sites/default/files/recursos/informe_2016.pdf

[92] 129. Es así que el acento de este umbral diferente de protección no se asienta en la calidad del sujeto, sino en el carácter de interés público que conllevan las actividades o actuaciones de una persona determinada. Aquellas personas que influyen en cuestiones de interés público se han expuesto voluntariamente a un escrutinio público más exigente y, consecuentemente, se ven expuestos a un mayor riesgo de sufrir críticas, ya que sus actividades salen del dominio de la esfera privada para insertarse en la esfera del debate público.