CONSEJO PERMANENTE DE LA
ORGANIZACIÓN DE LOS ESTADOS AMERICANOS

COMISIÓN DE ASUNTOS JURÍDICOS Y POLÍTICOS

OEA/Ser.G
CP/CAJP-3026/11
31 octubre 2011
Original: inglés

CUESTIONARIO DE LEGISLACIÓN Y PRÁCTICAS SOBRE PRIVACIDAD Y PROTECCIÓN DE DATOS

[AG/RES. 2661 (XLI-O/11)]

(Documento presentado conforme a lo acordado en la reunión de la Comisión de Asuntos Jurídicos y Políticos del 6 de octubre de 2011)

CUESTIONARIO DE LEGISLACIÓN Y PRÁCTICAS
SOBRE PRIVACIDAD Y PROTECCIÓN DE DATOS[1/]

[AG/RES. 2661 (XLI-O/11)]

(Documento presentado conforme a lo acordado en la reunión de la
Comisión de Asuntos Jurídicos y Políticos del 6 de octubre de 2011)

Conforme a lo acordado en la reunión ordinaria de la CAJP del 6 de octubre de 2011 y en cumplimiento de la resolución AG/RES. 2661 (XLI-O/11), que requiere: (1) que el Departamento de Derecho Internacional elabore un estudio comparativo sobre los distintos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, inclusive las leyes, reglamentos y autorregulación nacionales, con miras a explorar la posibilidad de un marco regional en esta área y (2) que el Comité Jurídico Interamericano presente, antes del cuadragésimo segundo período ordinario de sesiones de la Asamblea General, un documento de principios de privacidad y protección de datos personales en las Américas, sírvase encontrar adjunto al presente una copia del Cuestionario de legislación y prácticas sobre privacidad y protección de datos.

En cumplimiento de la resolución AG/RES. 2661 (XLI-O/11) y a fin de completar sus mandatos, las respuestas[2/] al cuestionario deben enviarse a más tardar el 15 de enero de 2012 a la Secretaría de la CAJP (aaristizabal@oas.org) y al Departamento de Derecho Internacional (jwilson@oas.org). Favor de dirigir la carta con las respuestas al cuestionario al Presidente de la Comisión de Asuntos Jurídicos y Políticos.

CUESTIONARIO

I. LEGISLACIÓN

A. ¿Existen en el ordenamiento jurídico interno de su país leyes o normas (generales o sectoriales) para la protección de la privacidad o de los datos a nivel nacional o federal? En caso afirmativo, describa brevemente estas leyes o normas, especificando si son aplicables en los contextos de los sectores privado y/o público, y adjunte copia de las disposiciones y documentos en que estén previstas.

RESPUESTA: En Costa Rica se emitió la ley No. 8968 de 07 de julio de 2011, denominada precisamente "Protección de la persona frente al tratamiento de sus datos personales". Lógicamente, es un cuerpo normativo aplicable en el ámbito nacional, tanto para los sectores públicos y privados.
Se trata de una ley de treinta y cuatro artículos que procura recoger los principios internacionalmente reconocidos de la autodeterminación informativa. Contiene una serie de objetivos, ámbito de

1. Preparado por el Departamento de Derecho Internacional.

2. Además del envío formal de las respuestas por los Estados miembros, la Secretaría solicita atentamente a las delegaciones que también envíen sus respuestas en formato *Word* o dentro del cuerpo de un correo electrónico, para facilitar las traducciones.

aplicación, definiciones sobre los diferentes elementos e institutos que protegerá y en que se aplicará la norma. Se entiende que su aplicación abarca tanto al sector privado como al público.

Incluye también los principios y derechos básicos en cuanto a protección de datos personales, tales como la explicación del contenido de la autodeterminación informativa, los principios del consentimiento informado, la obligación de informar al ciudadano, la necesidad de contar con el consentimiento del interesado, algunas excepciones a la autodeterminación informativa, desarrolla el principio de la calidad de la información, en que incluye la actualidad, veracidad, exactitud, y la adecuación al fin de la recopilación en bases de datos.

Contiene también otros derechos que asisten a los ciudadanos, tales como el acceso a la información (que incluye las obtenciones periódicas del conocimiento sobre la existencia de datos personales en bases de datos públicas o privadas y el programa de cómputo utilizado para ello) y el derecho de rectificación. Trata también de las distintas categorías de datos, tales como lo que se entenderá por datos sensibles, datos personales de acceso restringido, datos personales de acceso irrestricto y datos referentes al comportamiento crediticio.

La ley regula además la seguridad y confidencialidad en el tratamiento de los datos así como protocolos de actuación sobre los procedimientos que deberán seguir en la recolección, el almacenamiento y el manejo de los datos personales; y garantías efectivas a fin de ser protegido contra actos que violen los derechos fundamentales de los ciudadanos. Tiene también una referencia sobre la transferencia de datos personales, cuya regla general es que dicha información sólo podrá transmitirse cuando el titular del derecho haya autorizado expresa y válidamente tal acción y ello se efectúe sin vulnerar los principios y derechos reconocidos en esta ley.

Para una mejor comprensión del contenido de esta importante norma, estamos adjuntando su texto como anexo a estas respuestas.

Otras normas jurídicas sobre protección de datos:

La Ley General de Telecomunicaciones No.8642 del 04 de junio de 2008 contiene también dos numerales que tratan de la privacidad de las comunicaciones y la protección de datos personales que puedan estar en manos de las empresas que presten servicios de telecomunicaciones. Por ello, exige que los operadores y proveedores tengan las medidas técnicas para garantizar la seguridad de las redes y servicios, el derecho a la intimidad y protección de los datos personales de los abonados.

> *ARTÍCULO 42.- Privacidad de las comunicaciones y protección de datos personales*
>
> *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.

ARTÍCULO 43.- Datos de tráfico y localización
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.

Dentro del mismo tema de protección de datos personales que debe aplicarse en materia de telecomunicaciones, se emitió el Reglamento sobre Medidas de Protección de la Privacidad en las Comunicaciones, decreto ejecutivo No.35205 de 16 de abril de 2009, en el cual se señala que estarán sometidos al dicho cuerpo normativo todos los operadores o proveedores de servicios de telecomunicaciones que usen y exploten redes públicas de telecomunicaciones, independientemente del tipo de red. Se ordena que 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.

Igualmente, menciona que las disposiciones que tutelen la privacidad de las comunicaciones establecidas en la Ley General de Telecomunicaciones No.8642 y desarrolladas en ese Reglamento son irrenunciables y de aplicación obligatoria sobre cualesquiera otras leyes, reglamentos, costumbres, prácticas, usos o estipulaciones contractuales en contrario.

En lo que interesa, este reglamento busca 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 así como certificar que la información de los abonados que se suministra para las guías de abonados y los recibos telefónicos, sea congruente con los principios de privacidad y confidencialidad de la información, así como que dicha información no sea divulgada ni utilizada con fines comerciales.

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

Entre otras reglas para la protección de los abonados, se estatuye que 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. Además, 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.

Por la importancia temática de este Reglamento, se adjunta su texto completo con estas respuestas.

Una norma que debe también merece citarse es la Ley Reguladora del Contrato de Seguros No.8956 del 17 de junio de 2011, la cual contempla una disposición sobre la protección que deben darse a los datos recabados, así como la exigencia a las entidades aseguradoras, subsidiarias, proveedores de servicios auxiliares, empresas subcontratadas, y su personal, tanto directivo como de planta de resguardar el deber de confidencialidad de los datos que se recaben el en curso de una contratación de esta naturaleza. La violación del derecho de confidencialidad será causa suficiente para que el propietario de los datos tenga derecho a ser resarcido por los daños y perjuicios que se le hubieran provocado, sin perjuicio de cualquier otra acción legal que corresponda

ARTÍCULO 21.- Protección de datos

La información que en virtud de la suscripción de contratos privados de seguros obtengan las entidades aseguradoras queda tutelada por el derecho a la intimidad y confidencialidad. Las entidades aseguradoras, sus subsidiarias, sus proveedores de servicios auxiliares, empresas subcontratadas, y su personal, tanto directivo como de planta, estarán obligados a guardar el deber de confidencialidad de la información frente a su cliente y solo quedará liberada de este deber mediante convenio escrito, diferente del contrato de seguro, donde se expresen los fines de levantamiento de la confidencialidad y el alcance de diseminación de los datos. En igual sentido, quedan obligados los intermediarios de seguros, así como las personas físicas o jurídicas que realicen actividades destinadas a la promoción, la oferta y, en general, los actos dirigidos a la celebración de un contrato de seguros, su renovación o

modificación y el asesoramiento que se preste en relación con esas contrataciones.
La inobservancia comprobada de este deber constituirá infracción muy grave, sancionable de conformidad con lo establecido por el artículo 37 de la Ley Reguladora del Mercado de Seguros.
Quedan a salvo del deber de confidencialidad los datos que sea necesario exponer ante cualquier autoridad competente. Queda prohibida la divulgación de datos no relacionados directamente con el conflicto.
La violación del derecho de confidencialidad será causa suficiente para que el propietario de los datos tenga derecho a ser resarcido por los daños y perjuicios que se le hubieran provocado, sin perjuicio de cualquier otra acción legal que corresponda.

Normas internacionales que mencionan el tema de la privacidad:

Costa Rica ha suscrito una serie de tratados internacionales sobre muy diferentes temas, dentro de los cuales es común encontrar referencias a la necesidad de resguardar la intimidad de las personas participantes a las que dicha normativa se dirige.

Un ejemplo de ello es el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y utilización de niños en la pornografía, aprobado mediante ley No.8172 de 7 de diciembre de 2001, el cual señala la obligación de los Estados en la protección de la intimidad e identidad de los menores víctimas en todas las fases del proceso penal:

Artículo 8º—
1.-
Los Estados Partes adoptaran medidas adecuadas para proteger en todas las fases del proceso penal los derechos e intereses de los niños víctimas de las prácticas prohibidas por el presente Protocolo y, en particular, deberán:

a) *...*
b) *...*
c) *...*
d) *...*
e) *Proteger debidamente la intimidad e identidad de los niños víctimas y adoptar medidas de conformidad con la legislación nacional para evitar la divulgación de información que pueda conducir a la identificación de esas víctimas;*
f) *[...]*

Costa Rica ha aprobado también, mediante ley No.7993 de 7 de marzo de 2000, el Acuerdo con el Gobierno con Francia sobre Readmisión Personas en Situación Irregular. Si bien no trata propiamente del tema de la protección de datos personales, su artículo 8 sí regula el tema, la indicar lo siguiente:

"PROTECCIÓN DE DATOS
Artículo 8

Los datos personales necesarios para la ejecución del presente Acuerdo y comunicados por las Partes contratantes, deben ser tratados y protegidos según las legislaciones relativas a la protección de datos en vigencia en cada Estado.

En este marco:

1°- La Parte contratante requerida utiliza los datos comunicados exclusivamente para los fines previstos por el presente Acuerdo.

2°- Cada una de las Partes contratantes informa a la otra Parte contratante, por solicitud de esta, sobre la utilización de los datos comunicados.

3°- Los datos comunicados solo pueden ser tratados por las autoridades competentes de la ejecución del presente Acuerdo. Los datos solo pueden ser transmitidos a otras personas si se cuenta con la previa autorización escrita de la Parte contratante que las había comunicado."

Otro acuerdo internacional que contiene una referencia a la intimidad es la Convención Internacional para la Protección de todas las personas contra las Desapariciones Forzadas, aprobada mediante ley No.9005 de 31 de octubre de 2011. En el artículo 20 se estatuye que cuando una persona esté bajo custodia judicial, podrá limitarse la información sobre ella si ello perjudicase de alguna manera la intimidad del

Artículo 20

1 Únicamente en el caso en que una persona esté bajo protección de la ley y la privación de libertad se halle bajo control judicial, el derecho a las informaciones previstas en el artículo 18 podrá limitarse, sólo a título excepcional, cuando sea estrictamente necesario en virtud de restricciones previstas por la ley, y <u>si la transmisión de información perjudicase la intimidad</u> o la seguridad de la persona o el curso de una investigación criminal, o por otros motivos equivalentes previstos por la ley, y de conformidad con el derecho internacional aplicable y con los objetivos de la presente Convención. En ningún caso se admitirán limitaciones al derecho a las informaciones previstas en el artículo 18 que puedan constituir conductas definidas en el artículo 2 o violaciones del párrafo 1 del artículo 17. [El subrayado no es del original]

2. (...).

Finalmente, es menester mencionar las denominadas Reglas de Brasilia sobre Acceso a la Justicia de las personas en Condición de Vulnerabilidad de 6 de marzo de 2008, las cuales si bien no han sido aprobadas formalmente por la Asamblea Legislativa, bien podrían invocarse como quebrantadas pues nuestra jurisprudencia constitucional ha establecido que cualquier norma internacional que tenga carácter protector de derechos humanos puede ser invocada en caso de quebranto, aunque la ratificación positiva no se haya dado.

En lo que interesa, la sección 4ta. de las Reglas de Brasilia tratan de la protección de la intimidad, especialmente el párrafo 3) que habla de la protección de datos personales en casos de vulnerabilidad, sobre todo si tal información se encuentra en soportes digitales.

Sección 4ª.- Protección de la intimidad

> ***1.- Reserva de las actuaciones judiciales***
> *(80) Cuando el respeto de los derechos de la persona en condición de vulnerabilidad lo aconseje, podrá plantearse la posibilidad de que las actuaciones jurisdiccionales orales y escritas no sean públicas, de tal manera que solamente puedan acceder a su contenido las personas involucradas.*
>
> ***2.- Imagen***
> *(81) Puede resultar conveniente la prohibición de la toma y difusión de imágenes, ya sea en fotografía o en vídeo, en aquellos supuestos en los que pueda afectar de forma grave a la dignidad, a la situación emocional o a la seguridad de la persona en condición de vulnerabilidad.*
> *(82) En todo caso, no debe estar permitida la toma y difusión de imágenes en relación con los niños, niñas y adolescentes, por cuanto afecta de forma decisiva a su desarrollo como persona.*
>
> ***3.- Protección de datos personales***
> *(83) En las situaciones de especial vulnerabilidad, se velará para evitar toda publicidad no deseada de los datos de carácter personal de los sujetos en condición de vulnerabilidad.*
> *(84) Se prestará una especial atención en aquellos supuestos en los cuales los datos se encuentran en soporte digital o en otros soportes que permitan su tratamiento automatizado.*

Otras normas de rango internacional que tienen relación con la protección de datos pueden ser vistas *infra*, en la respuesta IV-C y IV-D.

B. ¿Existen en el ordenamiento jurídico interno de su país leyes o normas (generales o sectoriales) para la protección de la privacidad o de los datos a nivel estatal, municipal o local? En caso afirmativo, describa brevemente estas leyes o normas y adjunte copia de las disposiciones y documentos en que estén previstas.

RESPUESTA: Véase las respuesta I-A). Por ser Costa Rica una República y no un Estado Federal o similar, las leyes son de aplicación nacional, lo que implica que, igualmente, son de acatamiento obligatorio para las municipalidades o gobiernos locales. Véase, a manera de ejemplo, el artículo 7 del Reglamento para el otorgamiento, fiscalización y recaudación de actividades lucrativas de la Municipalidad de Osa, el cual establece que la información suministrada por los patentados o contribuyentes a la Municipalidad de Osa mantendrá el carácter confidencial y será de uso exclusivo de la municipalidad, según lo indica el Código de Normas y Procedimientos Tributarios y la ley de Protección de datos personales, y solo será facilitada por la municipalidad cuando sea solicitada por un despacho judicial.

Todo ello significa que cualquier ente local o municipal igualmente deberá ajustar sus actuaciones a las disposiciones de la ley nacional.

Las Reglas Mínimas para la Difusión de Información Judicial en Internet

Se trata de las llamadas **Reglas de Heredia**, las cuales son una serie de diez recomendaciones y cinco alcances más una serie de definiciones, todo lo cual es plenamente coincidente con los principios de la autodeterminación informativa y la protección a los datos personales de las personas sentenciadas.

Fueron aprobadas durante el Seminario Internet y Sistema Judicial realizado en la ciudad de Heredia (Costa Rica), los días 8 y 9 de julio de 2003 con la participación de poderes judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay. Se aclara que no es una norma de derecho positivo sino reglas a las que se espera se ajusten los respectivos poderes judiciales de los países suscriptores cuando pongan a disposición de terceros la información y el contenido de las sentencias para ser consultadas por Internet.

Allí se explica, entre otras cosas, que la finalidad de la difusión en Internet de la información procesal es garantizar el inmediato acceso de las partes o quienes tengan un interés legítimo en el proceso, a sus movimientos, citaciones o notificaciones. Se reconoce al interesado el derecho a oponerse, previa petición y sin gastos, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de difusión, salvo cuando la legislación nacional disponga otra cosa. En caso de determinarse, de oficio o a petición de parte, que datos de personas físicas o jurídicas están siendo difundidos ilegítimamente, deberá efectuarse la exclusión o rectificación correspondiente.

Una de las reglas esenciales es la quinta, en la cual se consagra la prevalencia de los derechos de privacidad e intimidad, cuando se traten datos personales referidos a niños, niñas, adolescentes (menores) o incapaces; o asuntos familiares; o que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos; así como el tratamiento de los datos relativos a la salud o a la sexualidad; o se trate de víctimas de violencia sexual o

doméstica; o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales.

Se considera conveniente también que los datos personales de las partes, coadyuvantes, adherentes, terceros y testigos intervinientes, sean suprimidos, anonimizados o inicializados, salvo que el interesado expresamente lo solicite y ello sea pertinente de acuerdo a la legislación.

En todos los demás casos se buscará un equilibro que garantice ambos derechos. Este equilibrio podrá instrumentarse:

(a) en las bases de datos de sentencias, utilizando motores de búsqueda capaces de ignorar nombres y datos personales;

(b) en las bases de datos de información procesal, utilizando como criterio de búsqueda e identificación el número único del caso.

Se evitará presentar esta información en forma de listas ordenadas por otro criterio que no sea el número de identificación del proceso o la resolución, o bien por un descriptor temático.

El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública. Sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.

Los jueces, cuando redacten sus sentencias u otras resoluciones y actuaciones, deberán hacer sus mejores esfuerzos para evitar mencionar hechos inconducentes o relativos a terceros, buscaran sólo mencionar aquellos hechos y datos personales estrictamente necesarios para los fundamentos de su decisión, tratando no invadir la esfera íntima de las personas mencionadas. Se exceptúa de la anterior regla la posibilidad de consignar algunos datos necesarios para fines meramente estadísticos, siempre que sean respetadas las reglas sobre privacidad contenidas en esta declaración.

El texto completo de las Reglas de Heredia se adjunta a estas respuestas.

Normas sectoriales que protegen la intimidad:

En otro orden de cosas, el Reglamento de Personas Refugiadas, decreto ejecutivo No.36831 de 28 de setiembre de 2011 establece el principio de confidencialidad en su artículo 8, referente al registro y tratamiento de la información de las personas en condición de refugio, y fundamenta tal norma como un derecho humano consagrado en Costa Rica.

> *"Artículo 8º—**Principio de Confidencialidad**. La confidencialidad es el principio rector para el registro y manejo de la información de los solicitantes de la condición de refugiado y de las personas refugiadas declaradas. Encuentra su fundamento en el derecho humano a la intimidad, reconocido en diversos instrumentos internacionales suscritos por Costa Rica, esencial para garantizar una protección internacional efectiva a las personas refugiadas. La*

> *falta de observancia de este principio, puede tener serias repercusiones en materia de protección y de seguridad a las personas refugiadas y solicitantes, sus familiares y personas con las que se le pueda asociar, tanto en Costa Rica como en el país de origen."* [Los subrayados no son del original]

Puede ser de interés mencionar el Reglamento de Acceso Universal, Servicio Universal y Solidaridad de 6 de octubre de 2008, que extiende el régimen de protección de la intimidad reconocido en la Ley General de Telecomunicaciones No.8642 (ya mencionado *supra*) a los beneficiarios del Fondo Nacional de Telecomunicaciones:

> *Artículo 28.—**Trámite de quejas**. De acuerdo con lo establecido en el Capítulo II de la Ley Nº 8642, el régimen de protección a la intimidad y derechos del usuario final también aplicarán a los beneficiarios de los proyectos de FONATEL. Los artículos 47 y 48 de la Ley Nº 8642, especifican los procedimientos necesarios para recibir, procesar y atender las quejas y denuncias sobre incumplimientos de los operadores que brindan servicios financiados por el FONATEL, en cuanto a calidad, precio y características de esos servicios.* [Los subrayados no son del original]

Otra norma de acatamiento obligatorio es la emitida por el Poder Judicial en la Circular No.63 de 31 de mayo de 2011, denominada precisamente Política Judicial dirigida al Mejoramiento del Acceso a la Justicia de las Niñas, Niños, y Adolescentes en Costa Rica. Dentro de los lineamientos de esta política está la protección de la intimidad, según se ve en su contenido:

> *VI. **Lineamientos estratégicos de la Política**:*
>
> *d. **Protección de los derechos de las personas menores de edad que intervienen en los procesos judiciales**. Garantizar el pleno respeto al derecho al debido proceso de la persona menor de edad, el resguardo de su dignidad y la protección de la intimidad.*
> [Los subrayados no son del original]

Otra norma importante de mencionar es la Directriz para reducir la Revictimización de Niños, Niñas y Adolescentes en Condición de Discapacidad en Procesos Judiciales, dada mediante Circular 168 de 7 de diciembre de 2010. En ella se ordena a las autoridades judiciales proteger la intimidad y privacidad de este sector humano que podría estar en situación de vulnerabilidad dentro de un proceso judicial.

> *"XX.—**Derecho a la imagen**. La autoridad judicial encargada deberá controlar que la dignidad del/a testigo o víctima en condición de discapacidad, no sea lesionada a través de publicaciones o cualquier exposición o reproducción de su imagen, o de cualquier otro dato personal que permita su identificación. Para ello podrá dictar medidas cautelares a favor del niño, niña o adolescente*

cuando su imagen, intimidad y privacidad sean lesionadas y ordenarle al PANI abrir proceso especial de protección en sede administrativa. Igualmente no se debe promover una imagen prejuiciosa por su discapacidad. Si se lesiona este derecho, es obligación del funcionario o funcionaria denunciarlo de conformidad con del artículo 47 del Código Civil."
[Los subrayados no son del original]

C. ¿Existen en su país disposiciones de rango constitucional que se refieran o aludan a la protección de la privacidad y de los datos como, por ejemplo, disposiciones específicas sobre protección de datos, disposiciones sobre libertad de expresión o habeas data? En caso afirmativo, describa estas disposiciones y adjunte copia de los textos pertinentes.

RESPUESTA: La Constitución Política de Costa Rica, emitida el 7 de noviembre de 1949, consagra en su artículo 24 el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. De acuerdo con el contenido de dicho artículo, se consideran inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Abarca diversas manifestaciones de la vida privada - económicas, comerciales, financieras, ejercicio profesional - que únicamente podrían divulgarse a terceros si existe un evidente interés público en esa información. La existencia de ese interés público es el elemento que sirve al Estado para diferenciar entre la información pública, la cual es de acceso general y; la información privada, la cual debe ser declarada confidencial.

Las leyes de Costa Rica contienen un rango amplio de lo que debe entenderse por documentos privados. En este sentido, derivada directamente del artículo 24 constitucional, se emitió la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones No.7425 del 09 de agosto de 1994 en cual establece los que deben considerarse documentos privados: la correspondencia epistolar, por fax, télex, telemática o cualquier otro medio; los videos, los casetes, las cintas magnetofónicas, los discos, los disquetes, los escritos, los libros, los memoriales, los registros, los planos, los dibujos, los cuadros, las radiografías, las fotografías y cualquier otra forma de registrar información de carácter privado, utilizados con carácter representativo o declarativo, para ilustrar o comprobar algo.

Así mismo, la libertad de expresión se encuentra incluida en el numeral 28 de nuestra Carta Constitucional, donde se garantiza que nadie puede ser inquietado ni perseguido por la manifestación de sus opiniones ni por acto alguno que no infrinja la ley. De igual manera, el artículo 29 establece que todos los ciudadanos pueden comunicar sus pensamientos de palabra o por escrito, y publicarlos sin previa censura, aunque haciéndolos responsables de los abusos que cometan en el ejercicio de este derecho.

La Constitución Política no incluye en su contenido alguna disposición que trate expresamente de la protección de datos personales o del procedimiento del hábeas data, dado que la autodeterminación informativa es un derecho nuevo, nacido con el advenimiento de las tecnologías de la información y las comunicaciones, que aún no encuentra eco en el nivel constitucional, a pesar de que otros países sí la han contemplado en sus respectivas constituciones.

Si bien aún ahora los académicos, jueces y operadores jurídicos intentan encontrar sustento para la protección de la autodeterminación informativa en los institutos constitucionales de la protección de la privacidad y la intimidad, aquella es más amplia y trascendente que éstos, pues se refiere a la protección de datos personales que no necesariamente son íntimos o privados.

D. ¿Existen en su país códigos de conducta de autocontrol u otros sistemas semejantes de responsabilidad por la privacidad y la protección de datos? En caso afirmativo, describa brevemente estos sistemas y adjunte copia de las disposiciones y documentos pertinentes que describan su operación.

RESPUESTA: Los códigos de conducta (ética profesional) son relativamente comunes en los diferentes gremios profesionales y pretenden una autoregulación en ciertos temas de su competencia. No obstante, en materia de autodeterminación informativa no existen códigos de conducta que incidan directamente en el tema, aunque sí pueden abarcar derechos colaterales como la privacidad o la intimidad. Así, el Colegio de Periodistas de Costa Rica emitió un Código de Ética para los y las profesionales en comunicación, mediante el Reglamento No.158 de 16 de agosto de 2011. Allí se establece, en su numeral 24, la obligación que tienen los periodistas en cuanto conducirse de manera respetuosa en la obtención de las informaciones, con respeto al dolor ajeno, la privacidad y la intimidad. Similar conducta se recoge en su artículo 38, que se obliga a dichos profesionales a respetar el derecho a la privacidad e intimidad, así como la imagen de los sectores socialmente vulnerables, las personas físicas y jurídicas. Se trata quizás del único ejemplo en que una entidad del sector privado procura respetar ambas garantías, aunque no referida expresamente a la autodeterminación informativa.

Por demás, no existe ningún código de naturaleza similar que se aplique a la empresa privada o elaborada por ella que pretenda respetar la autodeterminación informativa, sino que tal sector debe ajustar sus actuaciones al contenido de las normas jurídicas positivas.

II. NORMATIVIDAD Y CUMPLIMIENTO

A. ¿Cuál es el mecanismo o los mecanismos para hacer efectivo el cumplimiento de las leyes, normas o procedimientos sobre privacidad y protección de datos arriba referidos, y qué recursos pueden interponerse? Describa todos los mecanismos que existan y adjunte copia de los textos o documentos pertinentes.

RESPUESTA: De acuerdo con los términos de la Ley de protección de la persona frente al tratamiento de sus datos personales No. 8968 de 07 de julio de 2011, se está en espera de establecer, en el corto plazo, el procedimiento que busca precisamente hacer efectivo el cumplimiento de las normas sobre datos personales de los habitantes. Con la creación de la Agencia de Protección de Datos de los Habitantes (Prodhab), se establece un principio de denuncia mediante el cual se da la posibilidad de que cualquier persona que tenga un derecho subjetivo o un interés legítimo pueda denunciar, ante la Prodhab, que una base de datos pública o privada actúa en contravención de las reglas o los principios básicos para la protección de los datos y la autodeterminación informativa

establecidas en la ley, ello de acuerdo con el artículo 24. Una vez recibida la denuncia, se conferirá al responsable de la base de datos un plazo de tres días hábiles para que se pronuncie acerca de la veracidad de tales cargos. La persona denunciada deberá remitir los medios de prueba que respalden sus afirmaciones junto con un informe, que se considerará dado bajo juramento. De acuerdo con el artículo 25, en caso de que se omita rendir el informe en el plazo estipulado de tres días, los hechos acusados se tendrán por ciertos.

En cualquier momento, la Prodhab podrá ordenar a la persona denunciada la presentación de la información necesaria, según se ha indicado. Asimismo, podrá efectuar inspecciones directamente en el sitio en que se encuentren los archivos o bases de datos. Para salvaguardar los derechos de la persona interesada, puede dictar, mediante acto fundado, las medidas cautelares que aseguren el efectivo resultado del procedimiento.

A más tardar un mes después de la presentación de la denuncia, la Prodhab deberá dictar el acto final. Contra su decisión cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido.

El artículo 26 señala que, si se determina que la información del interesado es falsa, incompleta, inexacta, o bien, que de acuerdo con las normas sobre protección de datos personales esta fue indebidamente recolectada, almacenada o difundida, deberá ordenarse su inmediata supresión, rectificación, adición o aclaración, o bien, impedimento respecto de su transferencia o difusión. Si la persona denunciada no cumple íntegramente lo ordenado, estará sujeta a las sanciones previstas en esta y otras leyes.

Por otra parte, es posible que, de oficio o a instancia de parte, la Prodhab podrá iniciar un procedimiento tendiente a demostrar si una base de datos regulada por esta ley está siendo empleada de conformidad con sus principios; para ello, deberán seguirse los trámites previstos en la Ley General de la Administración Pública para el procedimiento ordinario. Contra el acto final cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido.

Finalmente, y previo a la normalización de los procedimientos, se establece en el artículo 23 que, supletoriamente y en todo lo no previsto expresamente por la ley de marras, serán aplicables las disposiciones del Libro II de la Ley General de la Administración Pública No.6227 de 02 de mayo de 1978, y en tanto sean compatibles con la finalidad de la ley No.8968.

Temporalmente, mientras la Agencia de Protección de Datos de los Habitantes no entre en funcionamiento pleno, el canal por el que un ciudadano pueda proteger sus datos personales debe ser mediante la interposición de un recurso de amparo ante la Sala Constitucional, órgano que desde su creación en 1989 y hasta la fecha ha sido el que ha resuelto en lo posible las violaciones que se dan en contra de datos personales de los habitantes, especialmente por parte de empresas privadas, quienes durante años se han dedicado de manera ilegítima e inimputable a la recolección, tratamiento, trasiego y venta de los datos personales de los ciudadanos de Costa Rica. Así las cosas, el individuo que desee defender su derecho de autodeterminación informativa deberá acudir a las instancias constitucionales mediante el procedimiento de amparo que se establece en el artículo 29 y siguientes de la Ley de la Jurisdicción Constitucional No.7135 de 11 de octubre de 1989, recurso que carece absolutamente de formalidades y puede ser interpuesto por cualquier persona.

B. ¿El ordenamiento jurídico interno de su país prevé la interposición de recursos en el sistema nacional de órganos jurisdiccionales para personas que han sido perjudicadas por violaciones a su privacidad o a la protección de datos? ¿Les otorga a las autoridades gubernamentales facultades para asegurar el cumplimiento de las leyes y normas pertinentes sobre privacidad y protección de datos? En caso afirmativo, describa y adjunte copia de los textos o documentos pertinentes.

RESPUESTA: Véase la respuesta II-A, donde se indica el procedimiento que deberá seguirse ante la Agencia de Protección de Datos de los Habitantes, cuando dicha entidad entre en pleno funcionamiento, pues aún está en fase de creación.

Por otra parte, y dentro de la lógica de la pregunta, una resolución de un órgano judicial o administrativo bien puede traer como consecuencia la posibilidad de que un ciudadano que considere afectados sus derechos y cuente con una resolución administrativa o judicial que así lo indique, plantee una demanda ante el órgano jurisdiccional correspondiente, sea en materia civil, penal o contencioso administrativo.

Así las cosas, y para efectos de responsabilidad civil, podría ser que se enderece la demanda como de responsabilidad civil extracontractual, dentro de lo que cabe la culpa in vigilando o culpa in eligiendo. Existiría con ello base más que suficiente para dirigirse contra cualquier infractor negligente una demanda por responsabilidad civil extracontractual, basada en los artículos 1045 y 1048 del Código Civil costarricense En este supuesto, toda empresa que maneje datos personales debería tener diversos niveles de seguridad, según la generalidad o no de ellos [(3)]. En caso de una situación no resuelta por la Agencia de Protección de Datos, igual podría plantearse la demanda por infracción a las normas civiles, estableciendo el afectado cuáles son exactamente los daños y perjuicios que ha sufrido. Dichos artículos, sobre los que se funda toda la teoría de responsabilidad civil extracontractual, indican:

([3]) En España, por ejemplo, el artículo 9 de la Ley Orgánica de Protección de Datos de Carácter Personal 15/1999 de 13 de Diciembre de 1999 (reiterado por el Real Decreto 994/1999 de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad) exige una serie de obligaciones para las empresas que manejen datos personales. En otros países habría que esperar que, al menos en un eventual contrato entre partes, la entidad que recolecte datos se comprometa a cumplir con una exigencia técnica relativa al nivel de seguridad, según sea el tipo de datos que se custodie, y en términos que al menos se asemejen a la ley ibérica. Así, el denominado nivel básico de seguridad incluiría los datos personales de carácter general. En el nivel de seguridad medio habría datos relativos a la hacienda pública, servicios financieros, transgresiones penales y administrativas y en general aquellos datos que, estudiados globalmente, puedan mostrar la personalidad del sujeto registrado. Por último, en el nivel de seguridad superior estarían los datos relativos a la ideología, religión, creencias, raza, orientación sexual, salud o datos de investigación policial sobre la persona.

> *ARTÍCULO 1045.- Todo aquel que por dolo, falta, negligencia o imprudencia, causa a otro un daño, está obligado a repararlo junto con los perjuicios.*
>
> *ARTÍCULO 1048.- (...) El que encarga a una persona del cumplimiento de uno o muchos actos, está obligado a escoger una persona apta para ejecutarlos y a vigilar la ejecución en los límites de la diligencia de un buen padre de familia, y si descuidare esos deberes, será responsable solidariamente de los perjuicios que su encargado causare a un tercero con una acción violatoria del derecho ajeno, cometida con mala intención o por negligencia en el desempeño de sus funciones, a no ser que esa acción no se hubiere podido evitar con todo y la debida diligencia en vigilar. (...)* [(4)] (Los subrayados no son del original)

La interposición de una demanda basada en los numerales vistos, 1045 y 1048 del Código Civil no es obstáculo para presentar paralelamente o con posterioridad (suponiendo que exista una sentencia favorable al ciudadano demandante) un recurso de amparo, según veremos seguidamente, con el fin de proteger además los derechos fundamentales de la víctima.

En efecto, el interesado podría plantear, además de la acción civil en sede judicial que mencionamos, un recurso de amparo (mientras no entre en funcionamiento la Agencia de Protección de Datos de los Habitantes y el procedimiento indicado anteriormente) para pedir la protección de sus datos personales, especialmente en lo que se refiere al acceso del ciudadano a los datos que sobre él sean mantenidos en las bases de datos de cualquier entidad, su transferencia a terceras personas (incluso cuando la transferencia se haya dado por negligencia, descuido o con consentimiento de la empresa recolectora de datos) y su bloqueo o eliminación de cualquiera de ellas. Dicho recurso se regula, según se indicó anteriormente, en la Ley de Jurisdicción Constitucional No.7135 de 11 de octubre de 1989, artículos 29 y siguientes [(5)] y su aplicación se encuentra debidamente reconocida por los tribunales constitucionales, según veremos.

Sin embargo, el paso previo que debe cumplir el afectado, antes de recurrir a la vía del amparo, es pedir formalmente a la empresa que utiliza sus datos personales que éstos sean debidamente eliminados, actualizados o bloqueados, para que no se utilicen para fines distintos de los que fueron recopilados, según los principios de la autodeterminación informativa. Según el decir de las propias empresas recolectoras de datos de Costa Rica, ellas efectúan ese trámite gratuitamente a gestión de parte, aunque en la práctica ello haya sido diferente.

([4]) Código Civil de Costa Rica, Ley No.63 de 28 de septiembre de 1887, artículos 1045 y 1047 (párrafo segundo), correspondiente a la culpa in vigilando e in eligiendo http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=15437&strTipM=TC

([5]) Texto completo en el Sistema Nacional de Legislación Vigente de Costa Rica http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=38533&strTipM=TC

Así pues, si la petición efectuada ante la empresa recolectora de datos no fuese ejecutada o si el ciudadano estuviese insatisfecho con la respuesta, podría entonces acudir directamente a la Sala Constitucional y presentar un recurso de amparo.

Vale la pena aclarar que este recurso se caracteriza por la ausencia total de requisitos y formalidades, sin que la víctima tenga necesidad siquiera de invocar la norma constitucional quebrantada, pudiendo presentarse en cualquier tipo de papel, escrito a mano y con sólo la firma del afectado, sin necesidad de que sea autenticado por abogado. Inclusive, es posible presentarlo por vía remota, por telegrama gratuito, fax, etc.

> *ARTÍCULO 38. En el recurso de amparo se expresará, con la mayor claridad posible, el hecho o la omisión que lo motiva, el derecho que se considera violado o amenazado, el nombre del servidor público o del órgano autor de la amenaza o del agravio, y las pruebas de cargo.*
> *No será indispensable citar la norma constitucional infringida, siempre que se determine claramente el derecho lesionado, salvo que se invoque un instrumento internacional.*
> *El recurso no está sujeto a otras formalidades ni requerirá autenticación. Podrá plantearse por memorial, telegrama u otro medio de comunicación que se manifieste por escrito, para lo cual se gozará de franquicia telegráfica.*

Por tanto, el ciudadano interesado debería solicitar en su acción de amparo, aparte del bloqueo y eliminación de sus datos, que el demandado proporcione además la información con la que cuente del ofendido. Tomando en cuenta que las empresa dedicadas en Costa Rica a la recolección de datos personales tienen presencia en Internet, lo propio es que tenga mecanismos sofisticados de administración en sus servidores Web para averiguar la identificación de las personas que ingresan allí mismo, ya sea a través de bitácoras, "cookies", direcciones IP o de algún otro mecanismo de individualización de los usuarios remotos.

Seguidamente, el demandante podría solicitar allí mismo a la empresa demandada que proceda exigirles a sus administradores de red que actualice, bloqueen o eliminen el nombre o cualquier dato del cliente ofendido. Recuérdese además que, antes de la promulgación de la ley No. 8968, las empresas que se han dedicado a la recolección de correos electrónicos y datos en general por Internet nunca han tenido problema ni impedimento moral para recopilar, vender, negociar o simplemente traspasar la información personal de los ciudadanos costarricenses con otros terceros deseosos de mostrar sus productos y servicios a la mayor cantidad posible de personas, sobre todo en el caso de empresas en cuyos territorios no existe legislación de protección de datos personales.

Otro tipo de medidas cautelares que podría solicitar el ofendido es que la empresa demandada acuerde con el proveedor de servicios de Internet (si fuese otro tercero) que no se acepten o se bloqueen correos y mensajes de esos terceros infractores dirigidos a la dirección o cuenta del ofendido.

Todo ello siempre dentro del supuesto que, hasta la fecha, ha sido la Sala Constitucional quien ha intentado, de alguna manera y no siempre con resoluciones felices, la protección de los datos ciudadanos.

C. ¿Cuáles son en su país las principales autoridades gubernamentales responsables de la aplicación de las leyes y normas sobre privacidad y protección de datos? Describa su relación con (o independencia de) el gobierno, indique su tamaño en términos de dotación de personal y presupuesto y adjunte copia de los textos o documentos pertinentes.

RESPUESTA: Según la recién promulgada ley No. 8968 de 07 de julio de 2011, la función de aplicar tales garantías ciudadanas recaerá directamente en la Agencia de Protección de Datos de los Ciudadanos. Según se estatuye en el artículo 15 de la ley de creación, se trata de una entidad adscrita al Ministerio de Justicia y Paz que gozará de una desconcentración máxima y con personalidad jurídica instrumental en el desempeño de las funciones que le asigna su ley, además de la administración de sus recursos y presupuesto. Podrá suscribir los contratos y convenios que requiera para el cumplimiento de sus funciones. Además, tendrá independencia de criterio.

En cuanto a la dotación de recursos humanos, aún no posible establecer con cuánto personal contará la Agencia Prodhab. Sí se establece en el artículo 18 que contará con el personal técnico y administrativo necesario para el buen ejercicio de sus funciones, designado mediante concurso por idoneidad, según el Estatuto de Servicio Civil o bien como se disponga en el reglamento a la ley, mismo que aún no ha sido emitido. Se ordena que el personal de la Agencia esté obligado a guardar secreto profesional y deber de confidencialidad de los datos de carácter personal que conozca en el ejercicio de sus funciones.

Dado esa situación de conformación en que se encuentra la futura Agencia, se ha suscrito recientemente el Acuerdo No.212 de 22 de noviembre de 2011, posterior a la aprobación de la ley No.8969, en que declara de interés público y nacional la conformación de la Agencia de Protección de Datos de los Habitantes (Prodhab). El texto de acuerdo indica que, para la puesta en marcha de la Agencia, se conforma la Comisión de Integración de la Prodhab, la cual tendrá como objetivo coordinar, planificar y definir todos los aspectos necesarios para la debida implementación de la referida Agencia. Dicha Comisión de Integración de la Prodhab, estará conformada por la Directora Jurídica del Ministerio de Justicia y Paz, la Directora Jurídica del Registro Nacional, un representante del Despacho del señor Ministro de Justicia y Paz, un representante de la Dirección de Apoyo al Consumidor, un representante del Ministerio de Ciencia y Tecnología, un representante del Ministerio de Comercio Exterior, un representante de la Procuraduría de la Ética Pública, así como un representante de la Defensoría de los Habitantes de la República en calidad de observador, y será coordinada por la Directora Jurídica del Ministerio de Justicia y Paz. Debe aclararse que los funcionarios públicos nombrados sólo lo serán para la conformación de Agencia, entendiéndose que cuando la Prodhab esté conformada, dicha comisión integradora no será parte del personal de la entidad.

Por otra parte, la Comisión de Integración de la Agencia de Protección de Datos de los Habitantes, será, además, responsable de redactar el Reglamento a Ley de Protección de la Persona Frente al

Tratamiento de sus Datos Personales, cuerpo normativo que deberá estar finalizado en un plazo máximo de 6 meses, contados a partir de la puesta en marcha de la Agencia de Protección de Datos.

Se señala también que las dependencias e instituciones del sector público y privado, podrán contribuir con la puesta en marcha de la Agencia de Protección de Datos de los Habitantes (Prodhab), en la medida de sus posibilidades y dentro del marco legal respectivo.

Es necesario aclarar que, a la fecha, la Agencia no cuenta aún con un presupuesto cierto, pues como se explicó está en proceso de creación y establecimiento. No obstante lo anterior, la ley No.8968, en su artículo 20, regula el tema del presupuesto con que contaría la entidad, en cual estará constituido de la forma en que se indica. Tal regulación muestra que no es posible establecer un presupuesto cierto, sino que ello dependerá de las circunstancias que concurran en cada escenario, lo que incidirá en una mayor o menor dotación de recursos financieros:

a) Los cánones, las tasas y los derechos obtenidos en el ejercicio de sus funciones.
b) Las transferencias que el Estado realice a favor de la Agencia.
c) Las donaciones y subvenciones provenientes de otros estados, instituciones públicas nacionales u organismos internacionales, siempre que no comprometan la independencia, transparencia y autonomía de la Agencia.
d) Lo generado por sus recursos financieros.

El artículo de ley respectivo ordena que los montos provenientes del cobro de las multas señaladas en esta ley sean destinados a la actualización de equipos y programas de la Prodhab.

Además, para el control apropiado en la asignación de recursos, la Agencia estará sujeta al cumplimiento de los principios y al régimen de responsabilidad establecidos en los títulos II y X de la Ley No.8131, Administración Financiera de la República y Presupuestos Públicos, de 18 de setiembre de 2001. Además, deberá proporcionar la información requerida por el Ministerio de Hacienda para sus estudios. En lo demás, se exceptúa a la Agencia de los alcances y la aplicación de esa ley. En la fiscalización, la Agencia estará sujeta, únicamente, a las disposiciones de la Contraloría General de la República.

D. ¿Qué volumen de quejas relacionadas con violaciones de la privacidad y de la protección de datos reciben sus autoridades gubernamentales correspondientes? ¿Estas autoridades abordan individualmente cada queja o tienen discrecionalidad respecto a los asuntos que investigan o procesan?

RESPUESTA: Debido a que ha sido la Sala Constitucional la entidad que se ha encargado de solventar los casos en que se ven lesionados los derechos ciudadanos en cuanto datos personales, privacidad e intimidad y no una entidad especializada, como será la Agencia de Protección de Datos de los Habitantes, no se han llevado registros sobre la naturaleza de las acciones planteadas, aunque lógicamente, como quedó explicado antes, se tramita a través de recursos de amparo.

No obstante, mediante una búsqueda aproximada en el Sistema Costarricense de Información Jurídica (SCIJ) realizada por los personeros de la Sala Constitucional a petición nuestra para el presente estudio, se ha encontrado el siguiente resultado, aunque no ordenado por años:

Tipo de queja	Cantidad
Violación a la intimidad	1396
Privacidad o Datos personales	266

En otro orden de cosas, es menester aclarar que cada queja de un ciudadano interesado en proteger sus datos personales debe abordarse individualmente, pues no existe en la legislación costarricense en esta materia la posibilidad de algún tipo de "discrecionalidad" respecto a asuntos sometidos a su conocimiento o alguna opción de que la Prodhab ignore, posponga, deje de procesar o deseche sin el cumplimiento del debido proceso casos concretos en que se ordene su intervención, bajo consecuencia de incurrir en alguna falta administrativa o penal, tales como incumplimiento de deberes.

E. ¿Las investigaciones y acciones para asegurar la observancia de la privacidad y de la protección de datos son emprendidas por sus autoridades exclusivamente en respuesta a quejas, o tienen esas autoridades otras bases o criterios para seleccionar e iniciar una investigación o acción de este tipo (por ejemplo, auditorías proactivas o requisitos de presentación de documentos)? Explique.

RESPUESTA: Tal y como se indicó en la respuesta II-A, la ley No. 8968 de 07 de julio de 2011, en su numeral 27, referente al procedimiento sancionatorio, da la posibilidad a la Agencia Prodhab a actuar tanto de oficio o a instancia de parte. Ello implica que, en caso de existir un indicio de violación a los datos personales de los ciudadanos, la Agencia podrá iniciar un procedimiento con miras a analizar si una base de datos regulada por la ley está siendo empleada de conformidad con sus principios. Como indicamos anteriormente, en lo que resulte pertinente y no contradiga los términos de la actual ley, deberán seguirse los trámites previstos en la Ley General de la Administración Pública para el procedimiento ordinario. Contra el acto final cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido.

F. ¿Las quejas relacionadas la privacidad de datos comerciales se pueden sujetar a posible enjuiciamiento penal? En caso afirmativo, explique la relación, en su caso, entre los responsables de las normas sobre privacidad y los fiscales en tales casos, así como el volumen general y la naturaleza de los procesos penales.

RESPUESTA: Efectivamente, en Costa Rica es considerado delito el uso inadecuado de los datos íntimos o privados de terceras personas, sin su autorización. El artículo 196 bis del Código Penal No.4573 de 4 de mayo de 1970 castiga la violación de comunicaciones electrónicas. Allí se establece una pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes

electrónicos, informáticos, magnéticos y telemáticos. Asimismo, la pena será de uno a tres años de prisión, si las acciones descritas anteriormente son realizadas por personas encargadas de los soportes electrónicos, informáticos, magnéticos y telemáticos.

Las denuncias por este tipo de acciones punitivas son tramitadas por la fiscalía de fraudes del Ministerio Público, dentro de una acusación penal por violación a las comunicaciones de los ciudadanos, siempre y cuando se cumplan los requisitos del tipo penal, esto es, la intención del sujeto activo de vulnerar la intimidad de la víctima o descubrir sus secretos, o bien, que la acción se realice sin la autorización del titular del derecho.

Por otra parte, el Departamento de Estadísticas del Poder Judicial es el ente encargado de llevar el registro respectivo de los delitos que se denuncien. En el caso concreto de la violación de comunicaciones electrónicas, se reportan un total de 169 denuncias, desde el año 2001 (fecha de promulgación del nuevo tipo penal) hasta el año 2010, de acuerdo con el siguiente cuadro estadístico:

DELITO DE VIOLACIÓN DE LAS COMUNICACIONES ELECTRÓNICAS
DENUNCIADOS DE 2001 A 2010

Tipo de delito	Año 2001	Año 2002	Año 2003	Año 2004	Año 2005	Año 2006	Año 2007	Año 2008	Año 2009	Año 2010	TOTAL
Violación de Comunicación Electrónica	0	0	0	7	5	11	21	32	51	42	169

Ahora bien, nótese que el tipo penal contiene una gran cantidad de verbos activos, tales como apoderar, accesar, modificar, alterar, suprimir, interceptar, interferir, utilizar, difundir o desviar de su destino. A su vez, los elementos que se protegen son los mensajes, datos e imágenes personales contenidas en soportes de naturaleza electrónica, informática, magnética y telemática. Todo ello puede llevar a concluir que no necesariamente podríamos encontrarnos ante delitos que involucren exclusivamente datos personales, sino otro tipo de bienes jurídicos tutelados, especialmente la intimidad o la privacidad.

Por otra parte, el Ministerio Público ha comenzado a recibir denuncias de usuarios de redes sociales en que se alega que los datos que ellos han puesto a disposición de personas de su confianza han sido reproducidos y utilizados por terceros sin la debida autorización del titular. Ante tal situación, la fiscalía ha optado por aplicar el artículo 196 bis para iniciar el respectivo proceso penal.

III. JURISPRUDENCIA

A. ¿Cuál es el papel de la jurisprudencia en la protección de la privacidad de las personas en su país? Adjunte los casos de tribunales superiores o de apelaciones en su país.

RESPUESTA: Sin duda alguna, ha sido la jurisprudencia nacional, especialmente la constitucional, el medio por el cual los ciudadanos de Costa Rica han podido de alguna manera paliar la inexistencia de ley en su momento, o la falta de aplicación de la normativa recién aprobada, en lo referente a la defensa de sus derechos frente al tratamiento indiscriminado de sus datos personales.

Precisamente por la confusión y desafío que representaba para los jueces la existencia reciente de un nuevo derecho como la autodeterminación informativa, apadrinado por corrientes de pensamiento igualmente novedosas que lo apartaban de los conceptos tradicionales de la privacidad o intimidad, se estuvo emitiendo jurisprudencia confusa y contradictoria que en realidad no ayudaba a definir la defensa a favor de los ciudadanos, aunado ello además a la presencia fuerte de empresas que procuraron desde siempre impedir que se legislara sobre el tema, pues ello afectaba sus intereses económicos. Por ello, era común encontrar sentencias constitucionales que avalaban las prácticas violatorias de dichas empresas, pues se partía del supuesto de que lo que interesaba proteger era sólo la intimidad o privacidad del demandante, pero no sus demás datos personales.

En efecto, la Sala Constitucional daba esta inquietante y desalentadora respuesta antes de rechazar un recurso, no sólo exigiendo de previo al interesado que acudiera primeramente ante la base de datos que contenía la información, sino además indicando además que:

> *"...En la especie no se ha producido la acusada violación a los derechos fundamentales de la amparada, toda vez que la información que a terceros ha brindado la recurrida sobre la recurrente ha sido sólo la estrictamente necesaria para los efectos de protección del crédito, en lo cual tiene evidente interés el banco ante el que la aquí gestionante solicitó crédito. La información brindada sólo abarca la que se encuentra en registros públicos -no privados- y si ésta resulta insuficiente o errónea, bien puede la interesada solicitar su rectificación, lo que no ha hecho. No estima esta Sala que la recurrente haya sido objeto de una invasión ilegítima a su intimidad, ni que se le haya discriminado o violado algún otro derecho fundamental, como el de la imagen por tenerse una foto suya, pues ello es para su correcta identificación.* ***La empresa accionada se limita a sistematizar la información que sobre una determinada persona existe en diversas fuentes públicas, sin crearla ni incursionar en comunicaciones o registros privados o confidenciales, a fin de brindar información de interés para terceras personas sobre la solvencia económica o crédito de un solicitante****. Asimismo, pone en conocimiento de quien requiere sus servicios, las limitaciones que puede tener la información brindada, para que ésta sea tomada con las reservas del caso, sin que ello constituya trasgresión de derecho fundamental alguno. En todo caso, si la amparada estima que se le ha causado perjuicio con la información que de su persona se ha brindado, puede acudir, si a bien lo tiene, a la vía legal correspondiente, sea la civil, a hacer valer sus derechos. En consecuencia, el recurso resulta improcedente y así debe declararse.* ***Por tanto:*** *Se declara sin lugar*

el recurso. [6]

Para tranquilidad de muchos ciudadanos, ese criterio judicial (que afirmaba la inexistencia de derechos fundamentales violados) tuvo un cambio de visión importante en sentencias posteriores. En este sentido, véase la sentencia No.5802 de 27 de julio de 1999 en que se realiza un estudio pormenorizado de la autodeterminación informativa como instituto de derecho fundamental, y que constituye un hito en las resoluciones de protección de datos personales en Costa Rica. Por su importancia, se adjunta como anexo a estas respuestas. Allí se indicó que los principios que debían regir la autodeterminación informativa eran los siguientes:

> *a.) La transparencia: la persona debe tener la posibilidad de ser informada de la totalidad de los datos existentes sobre su persona en un determinado archivo, de manera que le permita hacerse una idea integral de la información recopilada. Al mismo tiempo debe ser informada del tipo de tratamiento al que serán sometidas sus informaciones, a fin de que logre determinar si sus datos serán compartidos por otras instituciones o centro de procesamiento de datos.*
> *b.) Especificación de los fines del banco de datos: consiste en la obligación de especificar los fines, contenidos, usuarios autorizados, plazos de caducidad de los datos contenidos en los bancos de datos, requisitos sin los cuales no puede ser autorizado el funcionamiento de este centro de acopio de datos.*
> *c.) Organismo de control: requiere la creación de un órgano de control que vele porque el tratamiento automatizado de los datos se observen preceptos legales que protegen su derecho de los ciudadanos a su autodeterminación informativa.*
> *d.) Limitaciones a la recolección: debe haber una limitación de los datos recogidos para que éstos se adecuen a solo los necesarios para el cumplimiento del fin que se haya especificado en la legislación.*
> *e.) Limitación del uso: la utilización de los datos recogidos debe limitarse a la finalidad para la que fueron recogidos.*
> *f.) Plazos de validez: los datos no pueden permanecer en la base de datos en forma indefinida sino que debe fijarse un plazo, dentro del cual los datos serán mantenidos, así como el fin con que son conservados y el fin con que son guardados, transcurrido este plazo la información debe ser destruida.*
> *g.) Obligación de confidencialidad: debe crearse una obligación jurídica de que los datos que se manejan sean tratados en forma confidencial de manera que se limite el acceso de terceros a la información y la tergiversación de los fines por los que fue creado el registro.*

([6]) Sala Constitucional de la Corte Suprema de Justicia de Costa Rica. Resolución No.2563-99 de 9 de abril de 1999. Los subrayados no son del original.

> *h.) Exigencias relativas a la calidad de los datos: deben crearse los mecanismos para asegurar la máxima veracidad y precisión de las informaciones contenidas en el banco de datos, manteniéndose completas y actualizadas.*
> *i.) Información al interesado sobre la finalidad y uso de los datos así como el derecho de acceso y rectificación de la información que sobre su persona constan en el registro.*
> *j.) Derecho de bloqueo: derecho de la persona registrada a bloquear los datos almacenados, mientras se determina su exactitud o su caducidad.*
> *k.) Justificación social: los datos deben tener un propósito general y de uso específico socialmente aceptable.*
> *l.) Principio de limitación de los medios de recolección: los mecanismos de recolección de información deben ser lícitos, es decir con el consentimiento del sujeto o con la autorización de la ley.*

Sin embargo, no debe perderse de vista que la jurisprudencia es siempre casuística y no siempre tiene la aplicación general que sí tienen las leyes. Además recuérdese que, en el caso de la jurisprudencia constitucional de Costa Rica, la propia Sala IV ha dicho que sus resoluciones no son vinculantes. En suma, la jurisprudencia constitucional no puede llenar una laguna legal ni ser la llamada a regular un instituto que corresponde proteger a la Asamblea Legislativa. Incluso sería violatorio del Principio de Legalidad, de Reserva de Ley o incluso el de división de poderes.

En otras oportunidades, la Sala Constitucional ha indicado, en sentencia número 1991-678 de de 27 de marzo de 1991, que la Administración debe abstenerse de suministrar información que resulte confidencial en razón del interés privado presente en ella. La divulgación de esa información puede afectar los derechos de la persona concernida y concretamente, el derecho a la intimidad, entendida como el derecho del individuo a tener una esfera de su vida inaccesible al público, salvo voluntad contraria del interesado

También ha expresado, en la resolución N° 4847-99 de de 22 de junio de 1999, reproducida, entre otras, en la N. 910-2009 de 23 de enero de 2009, que:

> *"VI. El derecho de autodeterminación informativa tiene como base los siguientes principios: el de transparencia sobre el tipo, dimensión o fines del procesamiento de los datos guardados; el de correspondencia entre los fines y el uso del almacenamiento y empleo de la información; el de exactitud, veracidad, actualidad y plena identificación de los datos guardados; de prohibición del procesamiento de datos relativos a la esfera íntima del ciudadano (raza, creencias religiosas, afinidad política, preferencias sexuales, entre otras) por parte de entidades no expresamente autorizadas para ello; y de todos modos, el uso que la información se haga debe acorde con lo que con ella se persigue; la destrucción de datos personales una vez que haya sido cumplidos el fin para el que fueron recopilados; entre otros..."*

Otro voto que es importante considerar para los efectos de esta respuesta es el número 014835-09 de 18 de setiembre de 2009, en que la Sala Constitucional hace referencia a una cierta jerarquía de datos personales, de acuerdo con su categoría.

Con un nivel de protección superior o primario se encontrarían los datos sensibles, referentes a la afinidad sexual, grupo étnico y afiliación política, considerados como aspectos propios e inherentes de la personalidad. En estas circunstancias, se requiere del consentimiento total y expreso del individuo.

En un segundo nivel están las "*informaciones que, aún formando parte de registros públicos o privados no ostentan el carácter de "públicas", ya que –salvo unas pocas excepciones- interesan solo a su titular, pero no a la generalidad de los usuarios del registro. Ejemplo de este último tipo son los archivos médicos de los individuos, así como los datos estrictamente personales que deban ser aportados a los diversos tipos de expedientes administrativos. En estos casos, si bien el acceso a los datos no está prohibido, sí se encuentra restringido a la Administración y a quienes ostenten un interés directo en dicha información."* En este supuesto, igualmente se requeriría el permiso del titular, siempre que la recopilación y tratamiento tenga un fin específico y lícito.

En tercer nivel "*se encuentran los datos que, aún siendo privados, no forman parte del fuero íntimo de la persona, sino que revelan datos de eventual interés para determinados sectores, en especial el comercio. Tal es el caso de los hábitos de consumo de las personas…, el simple acceso a tales datos no necesariamente requiere la aprobación del titular de los mismos ni constituye una violación a su intimidad, como tampoco su almacenamiento y difusión."*

La cuarta categoría de defensa lo tendrían los datos que, aun siendo personales, revisten un marcado interés público, tales como *"los que se refieren al comportamiento crediticio de las personas; no son de dominio público los montos y fuentes del endeudamiento de cada individuo, pero sí lo son sus acciones como deudor, la probidad con que haya honrado sus obligaciones y la existencia de antecedentes de incumplimiento crediticio, datos de gran relevancia para asegurar la normalidad del mercado de capitales y evitar el aumento desmedido en los intereses por riesgo.*

Los niveles tercero y cuarto mantienen ciertas características que deberán respetarse, especialmente en cuanto a *"la forma cómo tales informaciones sean acopiadas y empleadas sí reviste interés para el Derecho, pues la misma deberá ser realizada de forma tal que se garantice la integridad, veracidad, exactitud y empleo adecuado de los datos. Integridad, porque las informaciones parciales pueden inducir a errores en la interpretación de los datos, poniendo en eventual riesgo el honor y otros intereses del titular de la información. Veracidad por el mero respeto al principio constitucional de buena fe, y porque el almacenamiento y uso de datos incorrectos puede llevar a graves consecuencias respecto del perfil que el consultante puede hacerse respecto de la persona. Exactitud, porque los datos contenidos en dichos archivos deben estar identificados de manera tal que resulte indubitable la titularidad de los mismos, así como el carácter y significado de las informaciones. Además, el empleo de tales datos debe corresponder a la finalidad (obviamente lícita) para la que fueron recolectados, y no para otra distinta."*

> *"En una categoría aparte se encuentran aquellos datos de interés general y acceso irrestricto contenidos en archivos públicos, para los cuales la regla a emplear es la del artículo 30* [de la Constitución Política de Costa Rica] *y no la dispuesta en el numeral 24 constitucional. Es decir, que en relación con tales informaciones existe una autorización absoluta de acceso y un deber inexcusable de la Administración de ponerlos al alcance de quienes quieran consultarlos, como en mecanismo de control ciudadano respecto de las actuaciones estatales, derivación necesaria del principio democrático que informa todas las actuaciones públicas y moldea las relaciones entre el Estado y la sociedad civil."*
>
> *(Sala Constitucional. Sentencia No.14835-02 de 18 de setiembre de 2009)*

Finalmente, debe aclararse que esta breve referencia no refleja totalmente el criterio de la Sala Constitucional sobre el tema, pues su producción jurisprudencial puede contarse por miles, alguna de ella contradictoria o poco feliz, pero que en general ha procurado siempre solventar y proteger los derechos ciudadanos en materia de protección de datos, responsabilidad que debería recaer original y directamente sobre la Asamblea Legislativa, y que no es sino hasta el año 2011 que cumplió en parte con dicha responsabilidad al aprobar la ley indicada.

IV. COOPERACIÓN TRANSFRONTERIZA

A. ¿El ordenamiento jurídico interno de su país limita o condiciona la transferencia de cualesquiera datos personales a otros países? En caso afirmativo, explique.

RESPUESTA: Sí. De acuerdo con la ley No. 8968 de 07 de julio de 2011, numeral 14, la regla general aplicable al tema de la transferencia de datos personales es que los responsables de las bases de datos, públicas o privadas, solo podrán transferir datos contenidos en ellas cuando el titular del derecho haya autorizado expresa y válidamente tal transferencia y se haga sin vulnerar los principios y derechos reconocidos en esta ley. Se entiende que la protección en la transferencia de datos abarca no sólo la que se pueda producir internamente sino también fuera de las fronteras del país.

B. ¿Ha recibido su país una certificación de privacidad y protección de datos de la Unión Europea?

RESPUESTA: No. Debido que la ley tiene muy poco tiempo de emitida y aún se encuentra en etapa de implementación de las medidas que indica, no se ha solicitado ni obtenido una certificación tal de parte de la Unión Europea, cuyo efecto sería la posibilidad de permitir la transferencia de datos personales de ciudadanos europeos a territorio costarricense. En todo caso, el nivel de protección de datos personales en Costa Rica aún está lejos de asimilarse al nivel europeo, por lo que la posibilidad de tal certificación sería aún muy peregrina.

En todo caso existen ejemplos de permisos otorgados por la Unión Europea para el trasiego transfronterizo de datos, tales como el dado a Suiza, en que se emitió la Decisión de la Comisión 2000/518/CE de fecha 26 de julio de 2000 [7], o el de Canadá, con el que existe igualmente la Decisión de la Comisión 2002/2/CE de 20 de diciembre de 2001 [8], pero no hay un caso similar con Costa Rica, al menos al día de hoy.

C. ¿Es parte su país de algún instrumento o arreglo internacional relacionado con los principios de privacidad y el flujo transfronterizo de información (por ejemplo, las directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales; el Marco de Privacidad y las Reglas de Privacidad Transfronterizas del APEC; la Convención ETS No. 108 del Consejo de Europa). En caso afirmativo, enumere los instrumentos o arreglos de los que es parte su país, la fecha en que adquirieron fuerza de ley en su jurisdicción y las acciones que ha adoptado su país, en su caso, para su aplicación.

RESPUESTA: Costa Rica no forma parte ni ha suscrito ninguno de los instrumentos internacionales citados.

No obstante, Costa Rica participó en el II Encuentro de Protección de Datos Personales en junio de 2003. En dicho evento se emitió la Declaración de La Antigua Guatemala (de la cual nuestro país es suscriptor) y se creó además la Red Iberoamericana de Protección de Datos. Allí se visualizó a la protección de datos personales:

> *"…como un auténtico derecho fundamental de las personas, sobre todo en orden al respeto a su intimidad y de su facultad de control y disposición sobre los mismos."*

Sin embargo, la Declaración de La Antigua no es un instrumento de derecho positivo ni ha sido formalmente aprobado como tal por la Asamblea Legislativa, por lo cual sólo podría tenerse como una declaración de intenciones para el Estado, pero sin verdadero efecto coercitivo.

Similar situación se presenta en el caso de las conclusiones efectuadas en la XIII Cumbre Iberoamericana de Jefes de Estado, efectuada en noviembre de 2003, en la cual se indica:

> *"45. Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la*

---

(7) Texto de la decisión del Consejo sobre Suiza en http://www.agpd.es/portalwebAGPD/internacional/adecuacion/suiza/common/pdfs/Decision_sobre_adecuacion_de_Suiza.pdf

(8) Texto de la decisión del Consejo sobre Canadá en http://www.agpd.es/portalwebAGPD/internacional/adecuacion/canada/common/pdfs/Decisionsobrelaadecuaciondelaleycanadiense.pdf

Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad"

Una vez más, si bien Costa Rica fue participante de dicha Cumbre, no se trata de un instrumento internacional especializado en la protección de datos personales, sino tan sólo de las conclusiones de una reunión de mandatarios latinoamericanos.

En otros instrumentos internacionales, tales como el Acuerdo de Diálogo Político y Cooperación entre la Comunidad Europea y sus Estados Miembros y las Repúblicas de Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá, ley No.8919 de 16 de diciembre de 2010, nuestro país se compromete a cooperar para garantizar la protección de datos personales en cuanto a su tratamiento, así como mejorar el nivel de protección y promover la libre circulación entre los Estados parte, siempre con miras a establecer normas internacionales más estrictas.

ARTÍCULO 35

Cooperación en materia de protección de datos

1. *Las Partes acuerdan cooperar para garantizar la protección de los datos personales y de otro tipo en su tratamiento, con vistas a promover las normas internacionales más estrictas.*
2. *Las Partes acuerdan también cooperar para mejorar el nivel de protección de los datos personales y trabajar en aras de su libre circulación entre las Partes, teniendo en cuenta debidamente las respectivas legislaciones internas.*

ARTÍCULO 58

Protección de los datos

A los efectos del presente Acuerdo, las Partes acuerdan dar un elevado nivel de protección al tratamiento de datos personales y de otra índole, compatible con las más estrictas normas internacionales.

D. ¿La legislación de su país permite que las autoridades pertinentes encargadas del cumplimiento de las leyes compartan información y pruebas sobre investigación y cumplimiento con autoridades homólogas en jurisdicciones extranjeras? En caso afirmativo, explique.

RESPUESTA: Sí. Efectivamente, la legislación de Costa Rica permite, como regla general, el intercambio de información con autoridades de jurisdicciones fuera del territorio, especialmente en delincuencia organizada nacional y trasnacional, tales como terrorismo, narcotráfico, trata de personas, fraudes bancarios, etc. Por ello, el artículo 11 de la Ley contra la Delincuencia Organizada

No.8754 de 22 de julio de 2009 crea la plataforma de información policial, la cual contiene las siguientes disposiciones en materia de investigación:

> *Artículo 11.- Todos los cuerpos policiales del país estarán vinculados a la Plataforma de Información Policial (PIP), a cargo de la Dirección General del Organismo de Investigación Judicial (OIJ), en la cual compartirán y tendrán acceso a la información de sus registros, bases de datos, expedientes electrónicos, redes internacionales e inteligencia policial, con la finalidad de lograr mayor eficiencia y eficacia en las investigaciones, tanto preventivas como represivas, de toda clase de delitos. Toda organización policial internacional, a la que se afilie Costa Rica, tendrá la obligación de estar vinculada en cuanto a la información de carácter delictivo.*
> *Salvo en los casos en que se requiera orden del juez para accederlos, todos los registros, las bases de datos, los expedientes de los órganos y las entidades estatales, las instituciones autónomas y las corporaciones municipales podrán ser accedidos por la Plataforma de Información Policial, sin necesidad de orden judicial.*
> *Cuando el acceso a los datos solamente pueda realizarse con la orden del juez, únicamente podrán imponerse de ellos los policías o investigadores designados previamente, así como los fiscales a cargo del caso y los jueces a quienes corresponda dictar algún auto o sentencia de ese caso; cuando la misma información se requiera en otro proceso, esta no podrá conocerse o compartirse sin la autorización previa de la autoridad judicial. Quienes conozcan tales datos legalmente, deberán guardar secreto de ellos y solamente podrán referirlos en declaraciones, informes o actuaciones necesarias e indispensables del proceso.*
> *El director del Organismo de Investigación Judicial será el responsable por los aspectos ejecutivos de la Plataforma y determinará los niveles de acceso a la información, y los cuerpos policiales y de investigación que podrán acceder a ella; para estos efectos, elaborará un protocolo de acceso y uso de la información contenida en dicha Plataforma.*
> *Respecto de la información, cualquier fuga que perjudique los resultados de las investigaciones o el uso ilegal de esta en perjuicio del investigado o de otras personas, será responsabilidad directa del funcionario o los funcionarios involucrados.*
> (Los subrayados no son del original)

Costa Rica se encuentra afiliada a la Organización Internacional de Policía Criminal (Interpol). De acuerdo con lo establecido en el artículo 12 de la misma ley, la oficina central nacional de la Interpol en el país funcionará bajo las órdenes del director general del Organismo de Investigación Judicial. Ello trae implícito el deber nacional de colaborar con las autoridades policiales de otras jurisdicciones, de acuerdo con las obligaciones que establece la Interpol. Además, el país es parte de otras redes de cooperación e información, tales como la Iber-Ius, la Iber-Red, etc. que igualmente

obligan al intercambio de datos entre diferentes plataformas policiales, administrativas y jurisdiccionales.

Igualmente, Costa Rica es país suscriptor de la Convención Interamericana sobre Extradición, aprobada mediante ley No.7953 21 de diciembre de 1999, según la cual los Estados Partes se obligan a entregar a otros Estados Partes que lo soliciten, a las personas requeridas judicialmente para procesarlas, así como a las procesadas, las declaradas culpables o las condenadas a cumplir una pena de privación de libertad.

El país ha suscrito además una cantidad importante de Convenios de extradición y de cooperación bilateral en materia penal con diferentes países y cuenta con legislación interna en la materia. La Ley de Extradición No.4795 de 16 de julio de 1971 regula este tema internamente.

Además, Costa Rica es también suscriptor de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (conocida también como Convenio de Palermo del año 2000), aprobada mediante la ley No.8302 de 12 de setiembre de 2002.

Finalmente, existen otros instrumentos internacionales bilaterales en que igualmente el Estado se compromete a brindar colaboración, tal como el Acuerdo de Cooperación Ambiental con el Gobierno de Canadá, aprobado mediante ley No.8286 de 17 de junio de 2002.

ARTÍCULO 16

Protección de información

> *Las partes otorgarán cualquier información solicitada de conformidad con este acuerdo, a menos que la divulgación de esa información estuviera prohibida o exenta de divulgación bajo sus respectivas leyes y reglamentos, incluyendo aquellas concernientes al acceso de información y privacidad.*

Si bien no se trata propiamente de un acuerdo de cooperación en materia de protección de datos, es muestra de la obligación de Costa Rica de dar información dentro del inicio o transcurso de una investigación transnacional.

E. ¿Su gobierno o sus autoridades encargadas del cumplimiento de las leyes cooperan con otros gobiernos o con autoridades homólogas en asuntos de investigación o de cumplimiento relacionados con privacidad y protección de datos, por ejemplo, para hacer frente el uso fraudulento, transferencia o mal manejo de datos personales?

RESPUESTA: No. Sin embargo, ello puede depender del delito concreto de que se trate. Dada la promulgación aún reciente de una ley de protección de datos personales, y que no es sino hasta ahora que se está en proceso de establecimiento de una agencia de protección de datos, no parece posible que las autoridades encargadas de ello tengan tal objetivo, al menos a corto plazo. La ley No. 8968

de 07 de julio de 2011 no contempla tal posibilidad expresa de cooperación con gobiernos o agencias de protección de datos, ni la contempla dentro de las obligaciones de la Prodhab. Ello no significa que en el futuro no se vaya a establecer esta obligación, pues resulta lógico y deseable crear lazos de cooperación entre diferentes jurisdicciones que tengan finalidades comunes, especialmente en defensa de los derechos ciudadanos.

Ahora bien, si se trata de ciertas conductas que involucren, entre otras cosas, el uso de programas o aplicaciones informáticas para recabar datos personales para fines delictivos (por ejemplo, el *phishing*, el *pharming*, suplantación de identidad, fraudes informáticos, etc.) sí existe plena posibilidad de encontrar colaboración en las autoridades competentes, especialmente dentro del Poder Judicial, en el Departamento de Delitos Informáticos del Organismo de Investigación Judicial o la Fiscalía de Fraudes.

Resulta importante resaltar la existencia de la Oficina de Asesoría Técnica y Relaciones Internacionales (OATRI), la cual es una entidad adscrita a la Fiscalía General de la República [9]. De acuerdo con el Decreto Ejecutivo No.34501 de 28 de marzo de 2008, en que se designa a la Fiscalía General de la República como la Autoridad Central para canalizar la asistencia judicial reciproca y la cooperación técnica, previstas en el marco de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, la cual es a su vez delegada en la OATRI.

Ahora bien, no debe perderse de vista que la denominada Convención de Palermo de 2000 sólo es aplicable en los denominados "delitos graves", es decir, aquellos en que la pena por la comisión de un delito tiene como retribución o castigo una máxima de al menos 4 años de prisión o más. Por ello, tomando en cuenta que la pena para la violación de comunicaciones electrónicas contemplada en el artículo 196 bis del Código Penal (ya mencionado *supra* en la respuesta II-F) castiga tales conductas con pena de prisión de seis meses a dos años, resulta poco probable que se pueda invocar el Convenio de Palermo o algún otro instrumento internacional similar para perseguir infracciones a los datos personales de individuos fuera de nuestras fronteras.

F. En caso de existir la colaboración transfronteriza, ¿es informal esta colaboración, ocurre a través de entidades reguladoras de la privacidad y de la protección de datos, o se lleva a cabo a través de redes de cooperación transfronteriza, tales como la Red global de vigilancia de la privacidad (GPEN), el arreglo transfronterizo de vigilancia de la privacidad (Cross Border Privacy Enforcement Arrangement) de la APEC, o la Red Iberoamericana de Protección de Datos? En caso afirmativo, describa esta colaboración o la participación de su país en estas redes.

([9]) De acuerdo con la información suministrada por la oficina del Poder Judicial, los números de teléfonos de la Oficina de Asesoría Técnica y Relaciones Internacionales son (506) 2295-3458, (506) 2295-3449, (506) 2295-4495, (506) 2295-3862 y (506) 2295-4853. Para emergencias se tiene el número (506) 8841-1625. Los números de fax son los siguientes: (506) 2223-2602 y (506)2295-3449. Se atienden consultas en español, inglés, francés e italiano. La dirección electrónica de la OATRI es oatrimp@poder-judicial.go.cr.

RESPUESTA: Véase la respuesta anterior, donde se explica que tal colaboración transfronteriza es poco probable debido a la penalidad que otorga el Código Penal al delito de violación de comunicación electrónicas y la imposibilidad de invocación de la Convención de Palermo. Por otra parte, es menester indicar que Costa Rica tampoco forma parte de ninguna red de colaboración como las mencionadas en el planteamiento, aunque sí fue suscriptora de la Declaración de Antigua sobre Protección de Datos Personales, en que se creó la Red Iberoamericana de Protección de Datos, según se explicó en la respuesta IV-C. No obstante, nuestro país no es parte oficial de dicha Red ni existe norma jurídica positiva alguna que obligue al Estado a cumplir con las disposiciones que allí se acordaron.

G. De no existir, ¿podría alguna forma de colaboración transfronteriza entre los Estados miembros de la OEA ayudar al cumplimiento o a la implementación de leyes de privacidad y protección de datos en su país? En caso afirmativo, suministre sugerencias sobre lo que podría resultar más útil.

RESPUESTA: Es necesario saber que Costa Rica es una nación donde se respeta al extremo el principio de legalidad y el concepto de Estado moderno de Derecho. Por ello, cualquier decisión que se tome sobre cualquier tema deberá tener siempre un sustento en el derecho positivo, esto es, la existencia de una norma jurídica que permita la actuación estatal. Por lo tanto, nuestra sugerencia es que debe propiciarse no sólo el apoyo político y técnico de la ley No.8968 de 07 de julio de 2011sino también la necesidad de suscribir acuerdos internacionales tales como la Red Iberoamericana de Protección de Datos, seguir las directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales; o llegar a formar parte de la Convención ETS No. 108 del Consejo de Europa. Este tipo de acuerdos internacionales representan tanto un hito en la protección de datos personales sino también un compromiso de las autoridades nacionales de todo nivel para implementar las medidas a las que se han obligado.

V. HABEAS DATA

A. ¿Existen en el ordenamiento jurídico interno de su país leyes que prevean el acceso a la información sobre uno mismo, incluyendo el habeas data? En caso afirmativo, caracterice los derechos que las personas pueden ejercer a través del habeas data, describa brevemente la fuente del derecho, describa si este derecho se aplica a los contextos de los sectores privado o público y adjunte copia de las disposiciones y documentos en que esté previsto.

RESPUESTA: Sí. Tal y como se ha explicado en las respuestas anteriores, especialmente en la II-A y II-B, existe un procedimiento reglado, que correspondería a un proceso de hábeas data ("traer el dato"), para que el ciudadano pueda acceder a la información que sobre él obre en una base de datos. La ley correspondiente, la ya citada No. 8968 de 07 de julio de 2011, garantiza en su artículo 7 los derechos que asisten a la persona que considere que sus privilegios y prerrogativas en cuanto a autodeterminación informativa podrían estar siendo quebrantados.

Por ello, se garantiza el derecho de toda persona al acceso de sus datos personales, rectificación o supresión de estos y a consentir la cesión de sus datos. La persona responsable de la base de datos debe cumplir lo solicitado por la persona, de manera gratuita, y resolver en el sentido que corresponda en el plazo de cinco días hábiles, contado a partir de la recepción de la solicitud. Aquí nos encontramos con dos privilegios básicos, según corresponda al acceso a la información o a la rectificación de esta.

En el primer supuesto, es decir, el acceso a la información, se entiende que deberá ser almacenada en forma tal que se garantice plenamente el derecho de acceso por la persona interesada.

El derecho de acceso a la información personal garantiza las siguientes facultades del interesado:

> a) Obtener en intervalos razonables, según se disponga por reglamento, sin demora y a título gratuito, la confirmación o no de la existencia de datos suyos en archivos o bases de datos. En caso de que sí existan datos suyos, estos deberán ser comunicados a la persona interesada en forma precisa y entendible.
>
> b) Recibir la información relativa a su persona, así como la finalidad con que fueron recopilados y el uso que se le ha dado a sus datos personales. El informe deberá ser completo, claro y exento de codificaciones. Deberá estar acompañado de una explicación de los términos técnicos que se utilicen.
>
> c) Ser informado por escrito de manera amplia, por medios físicos o electrónicos, sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento solo comprenda un aspecto de los datos personales. Este informe en ningún caso podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con la persona interesada, excepto cuando con ellos se pretenda configurar un delito penal.
>
> d) Tener conocimiento, en su caso, del sistema, programa, método o proceso utilizado en los tratamientos de sus datos personales.

El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, les corresponderá a sus sucesores o herederos.

En segundo grupo de derechos se refiere al Derecho de Rectificación, mediante el cual se garantiza al ciudadano el derecho de obtener, llegado el caso, la rectificación de los datos personales y su actualización o la eliminación de estos cuando se hayan tratado con infracción a las disposiciones de la presente ley, en particular a causa del carácter incompleto o inexacto de los datos, o hayan sido recopilados sin autorización del titular.

Sigue indicando el artículo 7 que todo titular puede solicitar y obtener de la persona responsable de la base de datos, la rectificación, la actualización, la cancelación o la eliminación y el cumplimiento de la garantía de confidencialidad respecto de sus datos personales.

El ejercicio del derecho al cual se refiere este artículo, en el caso de datos de personas fallecidas, les corresponderá a sus sucesores o herederos.

VI. DESAFÍOS TECNOLÓGICOS Y EMPRESARIALES

A. ¿Existen tecnologías o prácticas empresariales que planteen desafíos particulares para la aplicación o la implementación de las leyes de privacidad y protección de datos o de otras leyes de protección del consumidor en su país? En caso afirmativo, descríbalas.

RESPUESTA: Probablemente sí, pero ello ha sido consecuencia de varios factores, entre los cuales los más importantes son la ausencia de una cultura social de protección a los datos personales, así como la desidia estatal de poner coto a los abusos que cometían las empresas privadas dedicadas a la recolección, tratamiento y trasiego indiscriminado de datos personales. La acción estatal debió verse reflejada en la emisión de normas jurídicas y políticas nacionales que protegieran los derechos ciudadanos, cosa que nunca ocurrió sino hasta en el año 2011 en que se promulgó la ley No.8968, la cual ha representado un avance significativo en la defensa de las garantías del ciudadano en este campo.

Precisamente por la ausencia de legislación en el pasado, en Costa Rica han existido empresas que actuaron en total impunidad y a su antojo, como Datum [10] y la llamada Protectora de Crédito [11] o Cero Riesgo [12], entre otras, a las cuales aún ahora acuden algunas entidades financieras para ver el historial crediticio de sus clientes, más otros datos adicionales que no tienen nada que ver con ello, incluyendo la fotografía o las relaciones familiares. Inclusive, se sospecha que esos datos personales se han vendido ilegalmente a empresas extranjeras. [13]

Como es fácil concluir, en el caso de Costa Rica, bastaba con inscribirse como usuario de alguno de esos sitios Web que actúan en el país, sin ninguna regulación, para enterarse de la vida de cualquier costarricense que se encuentre allí registrado, sin que medie siquiera el consentimiento o autorización de éste. Más grave aún es el panorama si se tiene en cuenta que algunas instituciones públicas, tales como el Instituto Costarricense de Electricidad, la Caja Costarricense de Seguro Social (entidad autónoma que recoge los dineros de aportes obreros y patronales para la seguridad social) o los Registros Nacionales (registros automatizados que incluyen el Registro de Propiedades Inmuebles, Bienes Muebles, Personas Jurídicas, Propiedad Industrial, etc., todos ellos dependientes del Ministerio de Justicia) han vendido, a precios ridículos a esas entidades privadas de recolección de datos, información personal delicada que obra en sus propias bases de datos, sin ningún control, de manera totalmente irresponsable y hasta violatoria del principio de legalidad.

([10]) http://www.datum.net

([11]) http://www.protectora.com

([12]) http://www.ceroriesgo.co.cr

([13]) Véase al respecto el informe preparado por el Gobierno de Costa Rica sobre el estado de la venta de datos personales en el país, de abril y mayo de 2003. En este documento también se encuentran las referencias a los proyectos de ley que existían en aquel momento en la corriente legislativa para la protección de datos personales y la regulación del hábeas data, ninguno de los cuales fue aprobado.

En esa misma corriente, véase el Reglamento al Título II de la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones, aprobado mediante decreto ejecutivo No.35148 del 24 de febrero de 2009, la cual puede constituir una violación flagrante a la protección de derechos ciudadanos pues da la posibilidad al Instituto Costarricense de Electricidad de vender información no calificado como secreto industrial o comercial.

> *Artículo 9º—El ICE definirá los procedimientos para compartir la información que obtengan de sus clientes para los fines exclusivos del negocio, pero con resguardo de los derechos de los usuarios, y según lo establecido en la Ley general de telecomunicaciones y su reglamento. Podrá asimismo establecer las políticas, procedimientos y acciones, generales y específicos, que consideren convenientes para proteger la información calificada como secreto comercial, industrial o económico, quedando facultados para suscribir contratos de confidencialidad con sus empleados, proveedores, socios o aliados estratégicos y cualquier otra persona o tercero interesado. No podrá el ICE y sus empresas negarse a suministrar, sin reserva o condicionamiento alguno, al Ministerio de Ambiente, Energía y Telecomunicaciones, Autoridad Reguladora de los Servicios Públicos, Superintendencia General de Telecomunicaciones, Contraloría General de la República u otros órganos públicos, aquella información que por Constitución o ley esas instancias pueden requerir.*
> *El ICE, de conformidad con los artículos 9º y 10 de la Ley Nº 8660 y por razones de oportunidad y conveniencia comercial, y con respeto a la Ley general de telecomunicaciones, podrá vender información no calificada en los términos señalados en primer párrafo de este artículo, según las condiciones del mercado.*
> *Los procedimientos para la clasificación, custodia, administración y venta información comprenderán los propios del ICE y los de sus empresas.* [El subrayado no es del original]

Un tema que suele ser recurrente dentro del tema de la protección de datos es la mala utilización de ellos por parte de empresas comercializadores de bienes y servicios, las cuales acostumbran aprovechar esa información para hacer contacto directo con los potenciales clientes. Infortunadamente, la posibilidad de impedir tal práctica no sólo se ha tornado difícil para el usuario afectado, sino que además el legislador común ha permitido mediante el artículo 44 de la Ley General de Comunicaciones No.8642 de 04 de junio de 2008. Allí se indica que tales prácticas no estarán prohibidas siempre que exista el consentimiento del usuario o la intención del mensaje no sea con fines de venta directa con ocultamiento de la identidad del remitente o mediante un correo no válido.

> *"ARTÍCULO 44.- Comunicaciones no solicitadas*
>
> *Se prohíbe la utilización de sistemas de llamada automática por voz, fax, correo electrónico o cualquier otro dispositivo con fines de*

venta directa, salvo la de los abonados que hayan dado su consentimiento previamente.
No obstante, cuando una persona, física o jurídica, obtenga con el consentimiento de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o servicio, esa misma persona podrá utilizar esta información para la venta directa de sus productos o servicios con características similares. El suministro de información a los clientes deberá ofrecerse con absoluta claridad y sencillez. En cualquier momento, el cliente podrá pedirle al remitente que suspenda los envíos de información y no podrá cobrársele ningún cargo por ejercer ese derecho.
Se prohíbe, en cualquier caso, la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente, o que no contengan una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones."
[Los subrayados no son del original]

- * -