MARCO JURÍDICO DE LA PROFESIÓN INFORMÁTICA EN COSTA RICA

Marta Eunice Calderón Campos

EDITORIAL UCR

MARCO JURÍDICO DE LA PROFESIÓN INFORMÁTICA EN COSTA RICA

Marta Eunice Calderón Campos

EDITORIAL UCR
2018

343.728.609.99
C146m Calderón Campos, Marta Eunice, 1965-
Marco jurídico de la profesión informática en Costa Rica / Marta Eunice Calderón Campos. –1.ª ed.– Costa Rica: Edit. UCR, 2018.
xiv, 183 p.

ISBN 978-9968-46-673-8

1. COMPUTADORES – PROTECCIÓN – COSTA RICA. 2. DERECHOS DE AUTOR – COSTA RICA. 3. SEGURIDAD EN COMPUTADORES. 4. DERECHO A LA PRIVACIDAD. 5. PROTECCIÓN DE DATOS – COSTA RICA. 6. DERECHOS DE AUTOR – COSTA RICA. 7. PERSONAS CON DISCAPACIDAD – LEGISLACIÓN – COSTA RICA. 8. REDES SOCIALES. 9. INFORMÁTICA – ASPECTOS LEGALES. I. Título.

CIP/3192
CC/SIBDI.UCR

Edición aprobada por la Comisión Editorial de la Universidad de Costa Rica.
Primera edición: 2018.

Editorial UCR es miembro del Sistema de Editoriales Universitarias de Centroamérica (SEDUCA), perteneciente al Consejo Superior Universitario Centroamericano (CSUCA).

Corrección filológica: *Mariamalia Blanco B. y la autora* • Revisión de pruebas: *Euclides Hernández P.*
Diseño: *Raquel Fernández C.* • Diagramación: *Daniela Hernández C.*
Control de calidad: *Raquel Fernández C. y Grettel Calderón A.* • Diseño de portada: *Priscila Coto M.*

Apdo. 11501-2060 • Tel.: 2511 5310 • Fax: 2511 5257
administracion.siedin@ucr.ac.cr • www.editorial.ucr.ac.cr

Impreso bajo demanda en la Sección de Impresión del SIEDIN. Fecha de aparición: abril, 2018.
Universidad de Costa Rica. Ciudad Universitaria Rodrigo Facio.

Contenido

Capítulo III. Propiedad intelectual del software

Capítulo IV. Discapacidad

Capítulo V. Redes sociales

CAPÍTULO I
PRIVACIDAD

No decir más de lo que haga falta,
a quien haga falta y cuando haga falta.

André Maurois
Novelista y ensayista francés

Resumen

La privacidad está seriamente amenazada por las tecnologías de información y comunicación. Los datos personales se recolectan de forma permanente, muchas veces sin que las personas sean conscientes de esto. El derecho a controlar los datos personales y de estar libre de intrusión y de vigilancia es difícil de disfrutar. En la *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales* se define el derecho fundamental de la autodeterminación informativa, es decir, el poder ejercer un control sustancial de los datos personales y su uso. Esta ley establece los derechos de las personas titulares de los datos y las obligaciones de aquellos responsables de las bases de datos personales; a la vez, crea la Agencia de Protección de Datos de los Habitantes, la cual tiene las funciones, entre otras, de velar por el cumplimiento de la normativa sobre protección de datos y llevar un registro de las bases de datos reguladas por la ley. Aparte de esto, la ley de delitos informáticos establece las sanciones para quienes violen correspondencia, comunicaciones y datos personales. El profesional en computación e informática tiene un papel muy importante en la protección de datos personales, pues es el llamado a establecer los protocolos de acción y las medidas

de seguridad que garanticen a las personas que sus datos no serán utilizados en su perjuicio.

Introducción

Imagine que llega usted a un comercio a comprar un artículo. Al estar en la caja para que le facturen y cobren, el cajero le pregunta si quiere la factura con o sin nombre. Usted le responde que con nombre. Inmediatamente lo interrogan sobre cuál es su número de teléfono. Sin pensarlo, usted se lo dice. Sin embargo, usted reacciona y pregunta la razón por la cual se necesita dicho número. Se trata de un requerimiento del sistema, según le indica el cajero. ¿Qué harán con ese número? ¿Cuál es el objetivo de este requerimiento en el sistema? ¿Es un requisito legal? ¿Es simplemente lo que a alguien se le ocurrió para conveniencia del comerciante?

Horas después recibe usted una llamada. Le solicitan decirle a su hijo, cuyo nombre completo le mencionan, que el Banco X le tiene una tarjeta de crédito lista para entregársela, la cual probablemente su hijo no solicitó. ¿Cómo supieron que usted es su madre y obtuvieron su número de teléfono? No es tan difícil, tomando en cuenta que el Registro Civil tiene pública la mayor parte de la información sobre los actos civiles de los costarricenses (nacer, casarse, tener hijos, divorciarse, enviudar y morir). Igualmente, pueden saber si usted o su hijo tiene carro o casa, pues el Registro Nacional permite el acceso en línea a sus bases de datos, aunque requiere del pago por cada consulta. Incluso, es sabida la existencia de empresas que recopilan toda la información sobre la gente, y la hacen accesible a las personas y organizaciones dispuestas a pagar. Si usted no está en estas bases de datos, básicamente no es sujeto de crédito. Es como si no existiera; sin embargo, estar ahí puede traerle otros inconvenientes.

Los sistemas de software de instituciones gubernamentales y empresas privadas están interconectados. Usted compra medicinas en una farmacia y, como es adulto mayor, le solicitan el número de cédula

para darle un descuento. Inmediatamente, el cajero lee su nombre en voz alta; ya le ha pasado tantas veces que usted no se sorprende.

Además, usted se inscribe en un plan de cliente frecuente, con el cual le ofrecieron maravillosos premios por sus compras, siempre y cuando le guarde fidelidad a la empresa vendedora. ¿Sabe para qué van a utilizar su información? ¿Le dijeron sus verdaderos propósitos? ¿Ha pensado en que podrían bombardearlo con enormes cantidades de publicidad, orientada hacia los gustos que ha mostrado con su comportamiento de compras anterior, por lo cual le será prácticamente imposible rehusarse a comprar?

Por la noche, realiza una búsqueda en Internet con su nombre, y descubre que está publicada información sobre una beca que le otorgó el Gobierno del país X, hace veinte años. En la página web se especifica cuánto dinero le dieron y en cuál universidad realizó sus estudios. Esto ocurrió antes de que Internet fuera de uso generalizado, pero ahí está el periódico oficial del país X en formato digital, con datos que usted no sabía que eran públicos. Probablemente, considera esta información de la beca inofensiva, pero otra podría afectarle eternamente, por ejemplo, al imposibilitarle conseguir un trabajo u obligarle a contestar interrogatorios sobre el tema publicado. Por ejemplo, suponga que usted fue confundido con un delincuente y se publicó su nombre en el periódico como sospechoso del delito. La situación se aclaró pronto, pero ahora, el medio de comunicación tiene todas sus ediciones en línea, como un registro histórico al servicio de la sociedad, para investigadores, historiadores y simples curiosos. ¿Por cuánto tiempo estará esa información disponible? ¿Cuántas veces necesitará dejar claro que todo fue un malentendido?

Además de esto, actualmente muchas personas publican en las redes sociales detalles privados de sus vidas, sin obligación alguna de hacerlo. Las "amistades" se enteran de lo que los demás expresan y lo comentan, critican o comparten. Existen aplicaciones de software que usted instala voluntariamente o están instaladas de manera previa en sus dispositivos móviles, sin su permiso ni conocimiento, las cuales recopilan información personal, tal como los

lugares que usted visita y por cuánto tiempo permanece en ellos. Esta huella digital generada es consultada por otros.

Reig (2012) señala que toda la información debería ser compartida, pues ello ayudaría a resolver los grandes problemas de la humanidad, a generar enormes cantidades de datos disponibles para la investigación científica, a tener Gobiernos más transparentes y comprometidos con los ciudadanos y a mantener una relación más equilibrada entre los consumidores y las empresas. ¿Pero, realmente nos conviene que todos nuestros datos sean públicos?

Estamos siendo observados permanentemente. El Gobierno es el primero en querer saberlo todo sobre todos, so pretexto de la seguridad de la ciudadanía, la lucha contra el crimen organizado o el cobro de impuestos. En Costa Rica, por ejemplo, el Gobierno le solicita a la gente pagar con tarjeta de crédito para calcular cuánto deben cancelar de impuesto por sus ganancias los comerciantes y proveedores de bienes y servicios. El fin de esto parece bueno para la sociedad, porque así cada persona pagaría impuestos de acuerdo con sus ingresos. Sin embargo, la información puede ser útil para otros fines.

Es difícil, si no imposible, escapar de esta constante vigilancia. La única forma de lograrlo es estar totalmente desconectado de la red, pero esto no es siempre una opción. Después de todo, quien no está conectado está en desventaja. El trabajo o la necesidad de comunicación con otros obliga a las personas a exponerse, o bien se requiere de un marcapasos con geolocalizador que constantemente reporta la ubicación del portador.

¿Existe alguna forma de salvaguardar la privacidad? Las tecnologías de información y comunicación dificultan hacerlo. La mayoría de las personas ni siquiera sabe cuáles datos almacenan otros sobre ellas, ni en qué momento van a ser usados en su beneficio o perjuicio. ¿Obtuvo una respuesta negativa a su solicitud de crédito en un banco? Esto ocurre porque alguien con su mismo nombre ha fallado en sus pagos, pero el expediente crediticio manchado ha sido el suyo. ¿Por qué sucedió esto? Porque las computadoras son usadas por humanos que se equivocan, los sistemas de software

están mal diseñados y, además, usted no sabe cuál información suya almacenan, por lo cual no puede corregir lo que no conoce, entre otras razones.

Además de esto, a nivel mundial el temor al terrorismo y al crimen organizado ha generado cierto grado de aceptación de parte de la gente de que se violente su privacidad, en aras de la seguridad. ¿Se ha conseguido el nivel de seguridad deseado? No es fácil responderlo, pero sí es probable que se haya alcanzado un nivel de pérdida de privacidad del cual la gente no es consciente.

La legislación que resguarda la privacidad se actualiza a paso lento, comparado con el vertiginoso ritmo de avance tecnológico. Por eso, se debe apelar a la responsabilidad ética de los profesionales en el campo de las ciencias de la computación e informática, para que, desde su posición de diseñadores y desarrolladores de aplicaciones de software, hagan lo necesario para no violentar la privacidad de los usuarios. También es importante para las organizaciones crear políticas de privacidad, las cuales contemplen un conjunto de controles que permitan garantizar la privacidad de los datos custodiados, y en cuya definición participen distintos actores de dichas organizaciones. Adicionalmente, en Costa Rica se cuenta con la *Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales* y la *Ley 9048 Reforma de varios Artículos y Modificación de la Sección VIII, denominada Delitos Informáticos y Conexos, del Título VII del Código Penal*, más conocida como la ley de delitos informáticos.

En este capítulo se repasa el concepto de privacidad, se analizan las fuentes de las amenazas contra esta causadas por la tecnología de información y comunicaciones, y se exponen los principios de la protección de datos. Además, se presenta el papel que ha jugado la Sala Constitucional de la Corte Suprema de Justicia para el fortalecimiento del concepto de protección de datos, y se analizan la *Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales,* y la Ley 9048, conocida como de delitos informáticos, para comprender en qué forma estas afectan el desempeño de la profesión informática. Finalmente, se expone una lista de principios

recomendados a seguir para los profesionales en esta disciplina, autoridades en la toma de decisiones y administradores de proyectos para contribuir a que el derecho a la autodeterminación informativa sea respetado.

El concepto de privacidad

La privacidad se define como el derecho de un individuo a controlar los términos en los cuales se recolecta y usa su información personal (Karyda, Gritzalis y Park, 2007). Baase (2012) menciona los tres aspectos claves de la privacidad:

1. Estar libre de intrusión, es decir, que la persona es dejada sola y en paz.

2. Estar libre de vigilancia, esto significa que la persona no es vigilada por otros, sea con cámaras, micrófonos, llamadas telefónicas, geolocalizadores o cualquier otra tecnología.

3. Poseer el control de la información personal, el cual se refiere al derecho a la autodeterminación informativa que se explicará posteriormente.

Algunos investigadores han tratado de identificar diferentes categorías de privacidad. Por ejemplo, Roger Clarke (2006) fue el primero en definir una taxonomía de esta, la cual consta de cuatro categorías, a saber: datos personales, comunicaciones, experiencia y comportamiento. Posteriormente, Finn, Wright y Friedewald (2013) extendieron esta taxonomía a siete categorías, con el fin de cubrir el rango de preocupaciones potenciales sobre la privacidad en un mundo digital. Estas son:

1. Privacidad de la persona: es el derecho a mantener privadas las funciones y características del cuerpo, por ejemplo: la temperatura corporal y el código genético.

2. Privacidad del comportamiento y la acción: se refiere al derecho a comportarse de acuerdo con sus preferencias y hábitos sexuales, actividades políticas, prácticas religiosas, forma de vestir y hábitos en general. La persona tiene el derecho a comportarse, tanto en espacios públicos como privados, sin ser controlada por otras.

3. Privacidad de las comunicaciones: el derecho a que no haya intercepción de las comunicaciones, independientemente del medio por el cual se realicen, con el fin de fomentar la discusión libre de muchos temas.

4. Privacidad de los datos y la imagen: se refiere a que datos e imágenes no estén automáticamente disponibles para otras personas u organizaciones. Esto incluye poder ejercer un grado de control sustancial de los datos y su uso, es decir, la autodeterminación informativa.

5. Privacidad de los pensamientos y sentimientos: es el derecho de las personas a no estar obligadas a compartir estos. Se refiere a la libertad de pensamiento.

6. Privacidad de la localización y el espacio: es el derecho de una persona a movilizarse en un espacio público o semipúblico sin ser identificada, sin que se le rastree ni monitoree. Incluye el derecho de la persona a estar sola y a tener privacidad en lugares como su casa, carro u oficina.

7. Privacidad de asociación (incluida la privacidad de grupo): es el derecho de la persona de asociarse con quien quiera, sin ser monitoreada. Esta asociación puede estar fuera del control de la persona, tal como pertenecer a un grupo étnico.

Probablemente sea necesario agregar más categorías de privacidad conforme se introduzcan nuevas tecnologías.

Amenazas contra la privacidad causadas por la tecnología

Diferentes tecnologías de información y comunicación actuales y emergentes ponen en riesgo las distintas categorías de privacidad mencionadas anteriormente. Se utilizan aquí dos ejemplos de tecnologías para mostrar las amenazas que genera cada una de ellas. Muchas personas necesitan usar un marcapaso. Actualmente, algunos cuentan con un sistema de posicionamiento global (GPS, por su nombre en inglés) para saber dónde está el portador en el caso de un accidente cardiovascular; ello puede poner en riesgo las categorías de privacidad de la persona y de localización y espacio. Los escáneres corporales, como los utilizados en los aeropuertos, pueden generar una imagen del cuerpo desnudo y descubrir el estado de salud de una persona; esto atenta contra la categoría de privacidad de la persona, pero también causa preocupación en cuanto a la de datos e imágenes, pues las imágenes del cuerpo generadas por los escáneres podrían ser de muy alta resolución y mostrar muchos detalles. Además, pueden almacenarse, transmitirse y ser publicadas. Por tanto, también se podría deducir información sobre el comportamiento sexual (categorías de privacidad del comportamiento y de la acción), por ejemplo, si la persona se ha realizado una cirugía para aumentar alguno de sus órganos sexuales. Por todas estas razones, quienes fabrican y compran escáneres corporales tienen el deber de minimizar todas las amenazas, con la adopción de medidas tales como mostrar una representación estilizada del ser humano que no muestre detalles corporales y no permitir la posibilidad de almacenar las imágenes detalladas. Sin embargo, es importante contar con legislación que guíe a diseñadores, productores y consumidores sobre cuáles derechos de los usuarios deben ser respetados.

Los grandes bancos de datos e imágenes existentes en la actualidad –alimentados muchas veces, sin saberlo, por las mismas personas conforme interactúan en la red con aplicaciones de software–, son fuente valiosa de información personal y, por tanto, también de amenazas contra la privacidad. Las personas proveen, consciente

o inconscientemente, sus datos personales a cambio de acceder a bienes y servicios que necesitan, pero la mayoría de las veces no son conscientes de los riesgos a los cuales se exponen. La huella digital creada por cada persona la deja al descubierto, pues de ella se pueden derivar hábitos (categoría de privacidad del comportamiento y la acción) y lugares visitados (privacidad de la localización y el espacio); a la vez, se pueden hacer públicas actuaciones que no deberían serlo (categorías de privacidad de asociación y de datos e imagen).

Adicionalmente, con toda esta información almacenada, las libertades de intrusión y de vigilancia que menciona Baase (2012) son prácticamente imposibles; por ejemplo, las personas recibirán, sin solicitarlos, mensajes publicitarios muy bien adaptados a sus gustos para que les sea imposible rehusarse a comprar y, constantemente, serán vigiladas con el fin de registrar sus movimientos para derivar sus hábitos y gustos.

Aunque en la Constitución Política de Costa Rica se protege la privacidad, realmente la legislación está muy atrasada con respecto al avance tecnológico. Seguidamente, se expone cuál es el respaldo legal del derecho a la privacidad.

Respaldo legal del derecho a la privacidad

En Costa Rica, el artículo 28 de la Constitución Política garantiza el derecho a la privacidad:

> Artículo 28. (...) Las acciones privadas que no dañen la moral o el orden público, o que no perjudiquen a tercero, están fuera de la acción de la ley.

Asimismo, la protección de los datos personales se fundamenta en lo establecido en los artículos 23 y 24 de la Constitución Política, los cuales indican:

> Artículo 23. El domicilio y todo otro recinto privado de los habitantes de la República son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o para impedir

> la comisión o impunidad de delitos, o evitar daños graves a las personas o a la propiedad, con sujeción a lo que prescribe la ley.
>
> Artículo 24. Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier tipo de los habitantes de la República.

Existen varios instrumentos internacionales sobre derechos humanos, en los cuales también se consagra el derecho a la privacidad. Por ejemplo, el artículo 12 de la *Declaración Universal de los Derechos Humanos* (adoptada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948) indica:

> Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

El artículo 5 de la *Declaración Americana de los Derechos y Deberes del Hombre*, adoptada en la IX Conferencia Internacional Americana de 1948, reza:

> Artículo V. Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

Finalmente, los incisos 2 y 3 del artículo 11 de la *Convención Americana sobre Derechos Humanos*, también conocida como Pacto de San José (Ley 4534 del 23 de febrero de 1970), indican:

> Artículo 11. Protección de la Honra y de la Dignidad.
>
> 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
>
> 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

En cuanto a legislación costarricense, el artículo 203 del *Código Penal* indica con respecto a la divulgación de secretos:

> Artículo 203. Divulgación de secretos. Será reprimido con prisión de un mes a un año o de treinta a cien días multa, el que teniendo noticias por razón de su estado, oficio, empleo, profesión o arte, de un secreto cuya divulgación puede causar daño, lo revele sin justa causa.
>
> Si se tratare de un funcionario público o un profesional se impondrá, además inhabilitación para el ejercicio de cargos y oficios públicos, o de profesiones titulares, de seis meses a dos años.

La Constitución Política de Costa Rica prevé dos recursos para proteger los derechos de las personas, previstos también en instrumentos internacionales sobre derechos humanos, a saber: el Recurso de *habeas corpus* y el Recurso de amparo. El primero es para defender los derechos de libertad e integridad personales; el segundo, para los demás. Ambos recursos son de conocimiento de la Sala Constitucional de la Corte Suprema de Justicia, también denominada Sala Cuarta. Sin embargo, en Costa Rica no se cuenta explícitamente con un recurso de *habeas data* para proteger la información personal y saber quién tiene contacto con esta, cuándo y con qué fines.

A pesar de lo anterior, sí existen mecanismos legales que tienen como objetivo garantizar a las personas el derecho a la autodeterminación informativa, como se verá en las siguientes secciones. Se expone a continuación qué es necesario para tener certeza de disfrutar de este derecho y de que los datos personales están seguros.

Principios de la protección de datos

De acuerdo con Sarra (citado por Chen, 2010), los principios generales de la protección de datos son:

> 1. Legitimidad y buena fe: los datos deben ser procesados en forma legítima.

> 2. Especificación de la finalidad, racionalidad y duración: el tratamiento de los datos debe darse con fines determinados, explícitos y legítimos. La racionalidad se refiere a que los datos son usados para los fines especificados. Los datos serán conservados durante un tiempo razonable para los fines.
>
> 3. Pertinencia y exactitud: los datos deben ser exactos, pertinentes para los fines y no excesivos.
>
> 4. No discriminación: el tratamiento de los datos no debe llevar a la consecución de actos discriminatorios.
>
> 5. Confidencialidad y seguridad de la información: los datos solo serán tratados por personas autorizadas y serán protegidos para evitar su pérdida y cualquier uso ilegítimo (p. 117).

En Costa Rica, la Sala Constitucional definió los principios básicos de la protección de datos en el voto 5802-99 del 27 de julio de 1999. De este se extraen los siguientes:

1. Derecho de información en la recolección de datos: la persona debe ser informada previamente de la existencia de un archivo digital o manual de datos personales, de si puede o no negarse a responder las preguntas que le planteen, de las consecuencias de no suministrar los datos y de sus derechos de acceso a estos, rectificación, actualización, cancelación y confidencialidad, entre otros.

2. Consentimiento del afectado: la persona debe consentir entregar sus datos.

3. Calidad de los datos: los datos que se solicitan deben ser adecuados, pertinentes y no excesivos para los fines del tratamiento que se les dé. Además, deben ser exactos, mantenerse actualizados y eliminarse cuando dejen de ser pertinentes. Con esto último se define el derecho al olvido.

4. Prohibición relativa a categorías particulares de datos: los datos como origen racial, opiniones políticas, convicciones religiosas

y espirituales; relativos a la salud, vida sexual y antecedentes delictivos, no podrán almacenarse de manera automática ni manual en archivos privados. Además, en archivos públicos serán de acceso restringido.

5. Principio de seguridad de los datos: se deben adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida y tratamiento o acceso no autorizado.

6. Reglas para la cesión de datos: los datos de carácter personal solo podrán ser cedidos a terceros para fines que se relacionen directamente con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del afectado.

7. Derechos y garantías de las personas: cualquier persona puede conocer que hay un archivo de datos de carácter personal y sus fines, y obtener la confirmación de la existencia de datos suyos en archivos o bases de datos, entre otros.

8. Derecho de acceso a la información: se garantiza a la persona acceder directamente a los datos relativos a ella, conocer los fines para los cuales estos se recolectan y el uso que se les haya dado, solicitar que se rectifiquen, actualicen, cancelen o eliminen, y obtener la correspondiente indemnización por daños y perjuicios causados por el uso de sus datos personales.

Se quieren resaltar aquí dos derechos que se consideran muy importantes para la autodeterminación informativa, los cuales no están entre los principios definidos por la Sala Constitucional. Estos son el derecho a prohibir la interconexión de archivos y el derecho a impugnar valoraciones basadas solo en datos procesados automáticamente (citado por Chen, 2010, pp. 123-124). El primero se refiere a que terceros no puedan consultar y vincular distintas bases de datos que contengan información personal. De esta forma, se evita

crear perfiles personales y obtener datos sobre cualquier aspecto de la vida de una persona. El segundo tiene el objetivo de asegurar a la persona que las decisiones tomadas con respecto a ella no se basen únicamente en los resultados que genera el procesamiento automático de los datos. Por ejemplo, si a una persona se le niega un crédito bancario, esta situación no debe darse solo porque un sistema no lo reporta como posible sujeto de crédito; la persona debe poder presentar datos y evidencias que le permitan contar con una nueva oportunidad para ser valorada.

La Sala Constitucional y la protección de datos

Antes del año 2011, la Sala Constitucional aplicó de manera amplia el *habeas data* como un instrumento de tutela reactivo (Chen, 2010), con base tanto en la *Ley de Jurisdicción Constitucional,* como en lo denominado por Chen (2010) una "interpretación amplia" (p. 131) del artículo 24 de la Constitución Política de Costa Rica. A lo largo de aproximadamente 20 años, la Sala Constitucional emitió una larga serie de sentencias en las que definió los derechos relacionados con el tratamiento de los datos personales. Estos son el derecho a la intimidad, a la confidencialidad, a la protección de los datos personales y al acceso a estos. Por tanto, una persona tiene derecho a saber cuáles datos sobre ella están almacenados, a actualizarlos, a controlar el uso abusivo de estos y a exigir su exclusión de archivos, en particular, de datos sensibles. La Sala Constitucional abrió la posibilidad de tutelar todos estos derechos por la vía del Recurso de amparo.

Ya en 1997, en el voto 4154-1997, la Sala Constitucional mencionó el *habeas data* como un "amparo especial", "cuyo objetivo esencial consiste en el ejercicio de una facultad de corrección de los datos que se hallan en bancos de datos públicos y privados" (Chirino y Carvajal, s. f., p. 36). Para esto, la Sala Constitucional se basó

en el artículo 11 del Pacto de San José (Chirino y Carvajal, s. f.). En el voto 1998-1345, la Sala estableció por primera vez los peligros generados por el uso tan extendido de tecnología de la información, al establecer una "relación inequívoca entre los peligros de la 'sociedad informatizada' y el derecho a la intimidad" (Chirino y Carvajal, s. f., p. 33).

Con respecto a la autodeterminación informativa, la Sala Constitucional tiene claro que su "objetivo no es detener ese flujo de informaciones, sino hacerlo transparente al ciudadano y empoderarlo para que pueda controlar aquél [*sic*] flujo de informaciones que lo afecte directamente en su esfera de intereses" (Chirino y Carvajal, s. f., p. 40).

A lo largo de todos estos años, la Sala Constitucional ha demostrado poseer un profundo conocimiento del problema y ha entendido la necesidad de evolucionar con respecto a protección de los datos conforme avanza el desarrollo tecnológico. Con este nivel de madurez alcanzado, el siguiente paso fue materializar la jurisprudencia en una ley, la de *Protección de la Persona frente al Tratamiento de sus Datos Personales.*

Legislación costarricense relacionada con privacidad

En Costa Rica, la normativa legal relacionada con la protección del derecho a la privacidad es relativamente nueva. Se incluyen en esta la *Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales* y la *Ley 9048 Reforma de varios Artículos y Modificación de la Sección VIII, denominada Delitos Informáticos y Conexos, del Título VII del Código Penal*, más conocida como la ley de delitos informáticos. En las siguientes dos subsecciones, se detallan ambas.

Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales

En el año 2011, la Asamblea Legislativa de Costa Rica aprobó la *Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales*. Su reglamento fue publicado en el *Alcance Digital* N.º 42 del periódico oficial *La Gaceta*, el 5 de marzo de 2013. Esto representa un gran avance en la protección de datos personales. Seguidamente, se revisarán aquí algunos de los artículos de la ley y su reglamento, y su importancia para los profesionales en computación e informática, creadores de políticas organizacionales y administradores. Cuando no se hace referencia a si el artículo del cual se habla es de la ley o del reglamento, entiéndase que se refiere a la primera.

El artículo 1 describe el objetivo de esta ley. Lo más notable es que se eleva la autodeterminación informativa a la categoría de derecho fundamental, es decir, uno de "aquellos derechos humanos reconocidos por la norma constitucional" (Badilla, 2007, p. 155). El artículo 1 se transcribe a continuación.

> Artículo 1. Objetivo y fin. Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, *el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa* [resaltado añadido] en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

El capítulo II de esta ley define los principios de la protección de datos. En el artículo 4 se define el concepto de autodeterminación informativa y se reconoce esta como un derecho fundamental:

> Artículo 4. Autodeterminación informativa. Toda persona tiene derecho a la autodeterminación informativa, la cual abarca el conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección.

> *Se reconoce también la autodeterminación informativa como un derecho fundamental* [resaltado añadido], con el objeto de controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias.

El artículo 5 establece el principio de consentimiento informado, según el cual, cuando se soliciten datos de carácter personal, deberá informarse a la persona de los fines para los cuales se recolectan sus datos, de quién tendrá acceso a estos y del tratamiento que se dará a los datos, entre otros. El mismo artículo establece la obligatoriedad de obtener el consentimiento expreso del titular de los datos, es decir, de la persona a quien estos se refieren. El titular puede revocar el consentimiento.

El artículo 6 establece el principio de calidad de la información, el cual se refiere a que los datos que se recolecten, almacenen o empleen deben ser actuales, veraces, exactos y adecuados para el fin que se recolectaron. El tratamiento posterior de los datos con fines históricos, estadísticos o científicos no se considera incompatible con los fines de los cuales se informó a la persona titular, siempre y cuando se respeten los derechos que otorga la ley.

Es fundamental tomar en cuenta el artículo 6 cuando se trabaja en el desarrollo de aplicaciones de software, pues, muchas veces, su diseño vuelve obligatorio el ingreso de datos totalmente innecesarios para el fin que se recolectan. Por tanto, el profesional en computación e informática debe cuestionarse y cuestionarle a los dueños de la aplicación la pertinencia de los datos solicitados a los usuarios. Entiéndase por dueños de la aplicación la unidad o unidades organizacionales para las cuales esta se desarrolla, por ejemplo, mercadeo o producción.

Es importante también resaltar que garantizar que los datos estén actualizados y sean veraces y exactos también es, aunque no exclusivamente, deber de profesionales en computación e informática. Para conseguirlo, se debe garantizar la existencia tanto de mecanismos de seguridad como de un proceso de validación de datos en el

momento en el cual son ingresados en el sistema, para evitar que los usuarios introduzcan errores. Ambos aspectos se relacionan estrechamente, pues se sabe que un adecuado proceso de validación de datos es requisito necesario, aunque no suficiente, para garantizar la seguridad del software y de los datos vinculados.

El artículo 7 establece los derechos de la persona de acceder a sus datos personales, rectificarlos, suprimirlos y consentir que sean cedidos a terceros. Es responsabilidad de los profesionales en computación e informática desarrollar aplicaciones que permitan a las personas ejercer sus derechos. Para ello, deben evitarse ciertas situaciones, por ejemplo, que un dato no pueda ser rectificado porque, en el momento de definir la estructura de una tabla en la base de datos, se haya definido que el campo en el cual se almacena el dato no se pueda modificar porque es llave o clave (*primary key*), es decir, identifica de forma única cada registro. También puede darse el caso en el cual un dato no pueda ser suprimido porque el campo o columna en el cual se almacena no permite valores nulos. Diseñar una base de datos no es un asunto sencillo si la aplicación de software es compleja. Muchas veces, para mantener la consistencia en la base de datos, se toman decisiones que posteriormente podrían dificultarle a una persona ejercer sus derechos. Este es un aspecto más a considerar cuando se define la estructura de una base de datos. Se debe trabajar de forma conjunta con los dueños de la aplicación de software para identificar cuáles datos personales que deberían poder rectificarse y suprimirse se almacenan.

El artículo 11 del reglamento establece el derecho al olvido y se introduce el concepto de disociación de los datos; este consiste en que no pueda vincularse a una persona con sus datos. En cuanto al derecho al olvido, se establece un plazo máximo de diez años para conservar los datos personales. Es factible cumplir este periodo para bases de datos, que es en lo que se centra la ley. Sin embargo, es un derecho también deseable en Internet, contexto en el cual no es fácil lograrlo, pues los buscadores arrojan resultados que pueden causar problemas a las personas por la presencia de hechos,

reales o falsos, publicados hace varios años, para los cuales no se ha dado un proceso de disociación efectivo. El artículo 11 de la ley indica:

> Artículo 11. Derecho al olvido. La conservación de los datos personales, que puedan afectar a su titular, no deberá exceder el plazo diez años, desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que establezca otro plazo o porque el acuerdo de las partes haya establecido un plazo menor. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados los datos personales de su titular.

Según el artículo 6 de la Ley 8968, conservar los datos más allá del plazo máximo estipulado podría justificarse por fines históricos, estadísticos o científicos. Los profesionales en computación e informática serán parte del equipo a cargo de implementar los procedimientos para disociar los datos cuando esto ocurra; en este equipo, también participarán los dueños de la aplicación. Para disociar los datos, se requiere de un proceso que incluya los siguientes pasos:

1. Identificar aquellas columnas de las tablas de una base de datos que deben ser disociadas de forma irreversible.

2. Seleccionar una técnica de disociación de los datos que genere valores genéricos, lo suficientemente robusta con el objetivo de que no sea fácil reversar el proceso.

3. Programar la técnica de disociación seleccionada (software) y definir las pruebas por realizar (*testing*).

4. Ejecutar las pruebas y corregir los defectos encontrados.

5. Ejecutar el programa de disociación.

6. Revisar los datos disociados.

No todos los datos se pueden disociar de su titular. Por ejemplo, en un sistema de expediente médico, los datos registrados hace más

de diez años podrían ser todavía importantes. Situaciones posibles de mencionar son, por ejemplo, que una persona haya sido sometida a una cirugía de corazón o padezca una enfermedad incurable del sistema inmunológico; estos casos particulares no están contemplados explícitamente en la ley.

La *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales* no contempla los derechos relacionados con prohibir la interconexión de archivos e impugnar valoraciones basadas solo en datos procesados automáticamente. El primero de estos derechos "se refiere a que no se permite interconectar diferentes archivos para procesar datos personales con el fin de crear perfiles de gustos, preferencias o de simple consumo, de la persona" (Chen, 2010, p. 134). El segundo derecho es importante porque "el procesamiento automático de datos personales no garantiza que se consideren todos los elementos importantes de una persona para valorar o tomar una decisión sobre ella" (Chen, 2010, pp. 134-135). Es conveniente considerar en el futuro la modificación de la ley para incluir ambos derechos.

El artículo 9 de la ley establece cuatro categorías de datos, las cuales definen el tratamiento que se debe dar. Las categorías son:

1. Datos sensibles: lo más importante sobre estos datos es que nadie está obligado a suministrarlos y, por tanto, es mejor no incluirlos cuando se desarrolla una aplicación de software. Estos datos podrían utilizarse para discriminar a las personas. Se incluyen entre estos el origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas, y datos relativos a la salud, la vida y la orientación sexual.[1] Al no ser obligatorio que una persona brinde sus datos sensibles, se establece la protección de varias de las categorías de privacidad mencionadas por Finn *et al*. (2013), a saber: privacidad de la persona, del comportamiento y la acción, y de los pensamientos y sentimientos. Se establecen excepciones, como la

1 Se utiliza la expresión orientación sexual pues es la que se menciona en la ley.

posibilidad de pedir datos de la salud cuando se trate de darle un servicio médico a la persona.

2. Datos personales de acceso restringido: son los que, aunque formen parte de registros de acceso público, son de interés solo para la persona titular de los datos o para la administración pública. El tratamiento de estos será permitido solo para fines públicos o con el consentimiento expreso de su titular. La ley no da ejemplos de datos personales de acceso restringido; se pueden considerar entre estos las declaraciones de impuestos de la renta y las planillas que los patronos reportan a la Caja Costarricense de Seguro Social (París y Zamora, 2015).

3. Datos personales de acceso irrestricto: estos son los contenidos en bases de datos públicas de acceso general. No se especifica cuáles bases de datos calzan en esta categoría, pero a modo de ejemplo se tiene la del Registro Civil, la cual es pública y de acceso general. Por tanto, es posible afirmar que el número de cédula es un dato de acceso irrestricto; de igual forma se puede considerar como ejemplo la base de datos que el Instituto Nacional de Seguros publica cuando saca al cobro el seguro obligatorio de automóviles. Otros ejemplos posibles son las bases de datos de los distintos registros que conforman el Registro Nacional (París y Zamora, 2015). Según el artículo 9 de la ley, no se consideran datos de acceso irrestricto la dirección exacta de la residencia –excepto si se usa por un mandato, citación o notificación, ya sea administrativa o judicial, o en una operación bancaria o financiera–, la fotografía, los números de teléfono privados y otros de igual naturaleza. Ya que estos datos no son sensibles ni de acceso irrestricto, se supone en esta obra su pertenencia a la categoría de acceso restringido; sin embargo, esto no queda explícito en la ley.

4. Datos referentes al comportamiento crediticio: estos se rigen por las normas que regulan el Sistema Financiero Nacional, las cuales se han creado con el fin de garantizar un nivel de riesgo aceptable para las empresas.

El artículo 10, titulado "Seguridad de los datos", es de suma importancia para los profesionales en computación e informática, pues en él se establecen los lineamientos básicos en cuanto a seguridad que deberá seguir la persona responsable de la base de datos.

> Artículo 10. Seguridad de los datos. El responsable de la base de datos deberá adoptar las medidas de índole técnica y de organización necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado, así como cualquier otra acción contraria a esta ley.
>
> Dichas medidas deberán incluir, al menos, los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual, para garantizar la protección de la información almacenada.
>
> No se registrarán datos personales en bases de datos que no reúnan las condiciones que garanticen plenamente su seguridad e integridad, así como la de los centros de tratamiento, equipos, sistemas y programas.
>
> Por vía de reglamento se establecerán los requisitos y las condiciones que deban reunir las bases de datos automatizadas y manuales, y de las personas que intervengan en el acopio, almacenamiento y uso de los datos.

Tal como se menciona en este artículo, las obligaciones del responsable de la base de datos se establecen con detalle en el artículo 31 (capítulo IV) del reglamento de la ley. En el artículo 12 de la ley y en el 32 del reglamento, se define el deber de establecer los protocolos mínimos de actuación –políticas, procedimientos, medidas y mecanismos que se adoptarán al recolectar, almacenar y manejar los datos personales–. En el capítulo IV del reglamento, también se definen todas las demás acciones necesarias para garantizar la seguridad de los datos y del tratamiento de estos.

En caso de que ocurra una irregularidad que vulnere la seguridad, de manera de que esto produzca pérdida, destrucción, extravío u otro daño a los datos, el artículo 38 del reglamento indica el deber

de realizar un análisis forense conducente a determinar la magnitud de los efectos y definir las medidas correctivas y preventivas necesarias. Muy probablemente los profesionales en computación e informática participarán en dicho análisis, para lo cual necesitarían capacitación específica.

El capítulo II de este libro se dedica al tema de la seguridad, por lo cual todo lo detallado al respecto en el *Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales* será visto en dicho capítulo con más detalle. Sin embargo, es importante resaltar que, muy probablemente, estará en manos de profesionales de computación e informática crear los protocolos de actuación y ponerlos en práctica. Para la creación de estos protocolos, es de suma importancia el apoyo de quienes toman decisiones en la organización, pues esta tarea requiere recursos humanos y financieros.

El artículo 11 de la Ley 8968 establece la exigencia del secreto profesional, es decir, el deber de confidencialidad de todas las personas participantes en el proceso de tratamiento de los datos. Es común que los profesionales en computación e informática tengan acceso a los datos personales, pues son responsables de implementar los procesos de tratamiento. Por tanto, la confidencialidad es una característica importante para este gremio profesional.

El capítulo III de la ley se refiere a la transferencia de datos personales. La autorización expresa de la persona titular de los datos es necesaria para transferirlos, tal como lo indica el artículo 14.

> Artículo 14. Transferencia de datos personales, regla general. 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.

El capítulo IV de la ley crea la Agencia de Protección de Datos de los Habitantes (Prodhab), adscrita al Ministerio de Justicia y Paz, la cual tiene una larga lista de atribuciones descritas en el artículo 16 de la misma ley. Entre ellas están velar por el cumplimiento de

la normativa sobre protección de datos y llevar un registro de las bases de datos reguladas por la ley. La Prodhab se encuentra en un proceso de estructuración; se calcula que para el año 2023 la agencia habrá alcanzado un nivel de madurez similar al europeo actual (Ávalos, 2015).

¿Cómo saber si una base de datos está regulada por la ley? Dado que en la normativa legal hay contradicción al respecto, se sugiere atender lo indicado por la Prodhab (Agencia de Protección de Datos de los Habitantes, 2014), según la cual las bases de datos que se deben registrar son:

1. Las que se comercializan, transfieren, comparten, difunden, publican o cualquier hecho similar.

2. Aquellas que contienen datos personales de acceso público y brindan dicho acceso.

3. Las que comprenden algunos datos de acceso público y restringido y brindan el servicio de acceso a título oneroso.

4. Las que son compiladas y se utilizan con prospección comercial.

Además, si se da un servicio de información de las personas y las fuentes de las cuales se nutre la base de datos, esta se debe inscribir.

Aunque una base de datos sea de uso interno, se debe aplicar la normativa de protección de datos, es decir, los titulares de estos deben poder ejercer su derecho de autodeterminación informativa y, además, el responsable de la base de datos debe cumplir con lo referente a seguridad.

El artículo 45 del reglamento a la ley plantea la obligatoriedad de brindarle a la Prodhab un superusuario de consulta cuando se registra una base de datos; este es uno de los puntos más preocupantes para los profesionales en computación e informática. El nombre de este usuario podría ser lo que causa dicha preocupación, pues generalmente al mencionar la palabra *superusuario*, se piensa en la posibilidad de evadir todas las comprobaciones de

permisos de acceso y en ser capaz de realizar cualquier operación. La Prodhab aclara que el superusuario existe solo para efectos de consulta y se usaría para fiscalizar que las bases de datos personales cumplan con la normativa y con los estándares de calidad requeridos (Agencia de Protección de Datos de los Habitantes, 2014). Según la ley, se recurriría al superusuario cuando se haya interpuesto una denuncia o se sepa del mal manejo de una base de datos personales. Además, la Prodhab tendría acceso solamente a un espacio compartido que la empresa responsable de la base de datos pondría a su disposición, en el cual no sería posible realizar modificaciones; será responsabilidad de los profesionales en computación e informática asegurarse de que sea así. El artículo 45 señala:

> Artículo 45. Superusuario. El responsable deberá proporcionar a la Agencia un superusuario con perfil de consulta, aún cuando los datos estén siendo tratados por un encargado. La creación y puesta en funcionamiento de este superusuario debe ser diseñada y financiada por el responsable de la base de datos personales y debe operar a partir de la inscripción del registro de la base de datos ante la Agencia.
>
> La Agencia podrá en cualquier momento y de oficio consultar dicha base de datos sin restricción alguna, cuando exista denuncia presentada ante la Agencia o se tenga evidencia de un mal manejo de la base de datos o sistema de información. Para tales efectos, la Agencia deberá establecer lineamientos que garanticen el debido cumplimiento del secreto profesional o funcional, y para todos los casos llevar una bitácora en donde al menos se consignen el motivo, los accesos y consultas realizadas, así como el funcionario asignado que los realice.

La *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales* y su reglamento merecen una lectura minuciosa de todos aquellos profesionales del área informática que laboren en actividades de desarrollo de software, transferencia de datos y seguridad, así como de los dueños de las aplicaciones y de quienes tomen decisiones. La revisión de la página web de la Prodhab también es recomendable, pues brinda información valiosa para los responsables

de las bases de datos; asimismo, es importante definir una estrategia organizacional de seguridad para garantizar la privacidad, que incluya protocolos de seguridad y planes de contingencia y de capacitación sobre el tema para todo el personal de la organización, entre otros.

Ley 9048 de delitos informáticos

La *Ley 9048 Reforma de Varios Artículos y Modificación de la Sección VIII, denominada Delitos Informáticos y Conexos, del Título VII del Código Penal*, más conocida como la ley de delitos informáticos, debe ser también de conocimiento para los profesionales en computación e informática. Para algunos delitos se establecen penas más altas si las personas implicadas tienen a su cargo la administración o el apoyo técnico a los sistemas o redes informáticas; por este motivo, según la pena que imponga el juez, puede ser imposible librarse de ir a prisión.

Con la promulgación de esta ley, se reformaron los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la *Ley 4573 Código Penal*, además de agregarse el inciso 6 al artículo 229 y el artículo 229 ter y modificarse la sección VIII del título VII de la Ley 4573; con esto, se tipificaron algunos comportamientos como delitos. La ley sufrió cambios posteriores que no afectaron los artículos tratados a continuación.

Se transcriben los artículos 196 y 196 bis, los cuales se refieren, respectivamente, a la violación de correspondencia o comunicaciones y a la de datos personales. La definición legal de los verbos que se indican como acciones delictivas en estos artículos puede ser consultada en Lemaitre (2011).

> Artículo 196. Será reprimido con pena de prisión de uno a tres años a quien, con peligro o daño para la intimidad o privacidad de otro, y sin su autorización, se apodere, acceda, modifique, altere, suprima, intervenga, intercepte, abra, entregue, venda, remita o desvíe de su destino documentación o comunicaciones dirigidas a otra persona.
>
> La misma sanción indicada en el párrafo anterior se impondrá a quien, con peligro o daño para la intimidad de otro, utilice o

difunda el contenido de comunicaciones o documentos privados que carezcan de interés público.

La misma pena se impondrá a quien promueva, incite, instigue, prometa o pague un beneficio patrimonial a un tercero para que ejecute las conductas descritas en los dos párrafos anteriores.

La pena será de cuatro a ocho años de prisión si las conductas descritas en el primer párrafo de este artículo son realizadas por:

a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.

b) *Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos* [resaltado añadido].

Artículo 196 bis. Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma:

a) *Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones, tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos y magnéticos* [resaltado añadido].

b) La información vulnerada corresponda a un menor de edad o incapaz.

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

No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos

> en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de la ley.
>
> Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en base de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley.

Como se puede notar en los artículos 196 y 196 bis, se hace diferencia en la pena por el puesto ocupado. En este sentido, se destaca que el profesional en el área de la computación adquiere poder dentro de la organización en la cual labora, pues las tareas que realiza le permiten adquirir conocimiento profundo sobre el flujo de datos y el trabajo realizado en la organización; además, puede gozar de privilegios de acceso a las bases de datos por la naturaleza de su trabajo. Si a ello se une la formación profesional recibida, difícilmente podría alegar no saber lo que hacía si cometiera un delito de los mencionados en los anteriores dos artículos.

Es notable la gran cantidad de acciones delictivas (verbos técnicos) incluidas en los artículos 196 y 196 bis; esto significa que muchas acciones distintas se agrupan en un solo tipo penal. Sin embargo, algunas de estas requieren de mayor conocimiento, ofrecen un nivel de dificultad más alto o causan más daño. Incluso, algunas de las acciones requieren que otra se haya concretado previamente; por ejemplo, para modificar datos, primero se debe acceder a ellos. Corresponderá a un juez comprender el impacto de una posible acción informática delictiva para determinar la pena, con el agravante de que los verbos son conceptos difíciles de comprender para quienes no tienen estudios en el campo de la computación e informática.

Probar que una persona realizó alguna de todas las acciones mencionadas en los artículos 196 y 196 bis no es fácil; borrar o modificar las huellas del delito sí lo es. Por tanto, existe una alta probabilidad de que una denuncia nunca llegue a juicio. Nuevamente, en este punto los profesionales en computación e informática juegan un papel importante, al ser capaces de crear mecanismos que

permitan generar evidencias reales y no manipuladas; para hacerlo bien, se requiere de formación especializada y continua en el campo de análisis forense.

Algunas sentencias recientes de la Sala Constitucional

La labor de la Sala Constitucional en cuanto a protección de datos ha sido muy amplia y constituye una valiosa fuente de jurisprudencia, es decir, un precedente, que debe ser de interés para los profesionales en computación e informática. Es muy importante conocer las sentencias de esta entidad, pues constituyen jurisprudencia vinculante, en otras palabras, de acatamiento obligatorio.

Se aclara que, en las sentencias, el recurrente es quien presenta el recurso de amparo, y el recurrido, la organización o persona contra la que se plantea. La obligatoriedad mencionada anteriormente no se limita al recurrido, sino a toda la sociedad. En caso de que la Sala Constitucional declare con lugar un recurso y lo indicado en la sentencia no se acate en el tiempo determinado, el recurrido puede recibir sanciones por desacato.

Algunos ejemplos interesantes de las resoluciones de recursos de amparo relacionados con el tema de protección de datos se resumen y comentan a continuación.

1. **Información crediticia. Niegan suministrar información crediticia**

   Sentencia 8324-2011

   Este recurso fue interpuesto contra la Cooperativa de Ahorro y Crédito Alianza de Pérez Zeledón, R. L. Indicó el recurrente que la cooperativa se negó a actualizar y suministrarle la información crediticia sobre él. La Sala Constitucional declaró con lugar el recurso y le ordenó al apoderado generalísimo sin límite de suma de la cooperativa suministrar al recurrente los datos solicitados y actualizar

de inmediato su información crediticia o eliminarla si había transcurrido el plazo del derecho al olvido.

2. **Datos personales. Se ordena a empresa eliminar ciertos datos de su base**

   Sentencia 3998-2012

Este recurso fue presentado en contra de las empresas Protectora de Crédito Comercial Sociedad Anónima y Cero Riesgo Información Crediticia Digitalizada Sociedad Anónima. El recurrente alegó que las empresas recurridas difundieron información confidencial suya sin su debido consentimiento, la cual incluso se encontraba desactualizada o era falsa. Además, acusó el deber de condenar a todas las instituciones públicas que brindaron sus datos. Luego de aprobada la *Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales*, en Costa Rica se delimitó claramente cuáles son los datos personales susceptibles de ser publicados o divulgados por terceras personas o empresas dedicadas a esta actividad. En la ley, se indica de manera expresa que la dirección exacta de la residencia de una persona, su fotografía, así como los números de teléfono privados y otros de igual naturaleza, no pueden considerarse como datos personales de acceso irrestricto. Por tanto, su divulgación por terceros no es permitida sin el consentimiento expreso y libre de su titular, el cual no se dio en este caso. Se declaró con lugar el recurso y se ordenó a los presidentes de ambas empresas eliminar de inmediato la información referida a las direcciones físicas, teléfonos celulares y fotografías a nombre del recurrente de sus bases de datos.

3. **Información sobre salario de funcionarios del Estado es un dato público**

   Sentencia 4037-2014

Este recurso se presentó contra la Caja Costarricense de Seguro Social (CCSS) por negarse a brindar al recurrente el salario reportado ante la CCSS de cada funcionario público. La funcionaria de

la CCSS a la cual se le solicitó la información le indicó al recurrente que debía dirigirse a la Junta Directiva de la entidad e indicar cuál era el interés público de los datos solicitados. Con ello, se restringió de forma injustificada el derecho de acceso que, constitucional y convencionalmente, le es garantizado. La Sala Constitucional ha llegado de manera reiterada a la conclusión de que el salario de los funcionarios es de naturaleza pública e interés general, por involucrar el adecuado control y manejo de fondos públicos. Se declaró, entonces, con lugar el recurso y se ordenó a la presidenta ejecutiva y la jefa del área de comunicación de la Caja Costarricense de Seguro Social que, máximo en un mes exacto a partir de notificarse esta resolución, informaran al recurrente cuánto tiempo se requeriría para construir una rutina informática que permitiera extraer los datos que se solicitaron, el plazo necesario para atender su solicitud y el costo que aproximadamente debería asumir el amparado.

4. **Atestados académicos de un funcionario público son de acceso público. Aplicación de la ley de protección de datos**

Sentencia 10102-2014

Este recurso de amparo fue puesto contra el director de la Escuela Nacional de Policía por negarse a informar al recurrente de los procesos de formación policial en que participaron los directores y subdirectores generales, los directores y subdirectores regionales, y la policía turística. El recurrido se negó a proporcionarla; argumentó que la *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales* define como datos de acceso restringido aquellos que, aún cuando forman parte de registros de acceso al público, no son de acceso irrestricto, por ser de interés solo para su titular o para la Administración Pública. La Sala Constitucional consideró los datos solicitados como de interés público, pues es sobre la formación académica a nivel policial de funcionarios públicos impartida por una entidad estatal. Se declaró con lugar el recurso y se ordenó al director de la Escuela Nacional de Policía proporcionar al recurrente los datos solicitados.

5. **Información de experiencia de un funcionario no es un dato sensible o de acceso restringido**

Sentencia 4268-2014

Este recurso de amparo fue puesto contra la Imprenta Nacional, pues la recurrente consideró lesionados sus derechos fundamentales porque solicitó a la jefa del Departamento de Gestión Institucional de Recursos Humanos de la Imprenta Nacional, una certificación de experiencia en manejo de personal de un tercero, la cual no se le brindó. La mayoría de los magistrados de la Sala consideró que lo solicitado no revelaba información personal. En esta sentencia, se hizo referencia a que la Sala Constitucional indicó como datos sensibles la fotografía, la dirección de la casa, la orientación sexual o religiosa, los antecedentes penales o los datos relativos a la salud de las personas (sentencias 2013-008326 y 2013-008683). Se declaró con lugar el recurso y se ordenó a la recurrida eliminar previamente los datos confidenciales y entregar a la recurrente dicha certificación.

6. **Correo electrónico y documentos electrónicos almacenados en la computadora de un funcionario son privados**

Sentencia 7357-2015

En este recurso de amparo interpuesto contra la directora ejecutiva del Patronato Nacional de Ciegos, los recurrentes reclamaron sobre el bloqueo de sus cuentas de correo personal institucional por orden de dicha directora. Al consultarle, ella dijo que revisaría y conocería la información almacenada en sus correos; además, alegó la pertenencia de las cuentas de correo al Patronato Nacional de Ciegos. Los recurrentes sostuvieron que la acción de la directora lesiona sus derechos a la intimidad, al secreto a las comunicaciones, la inviolabilidad de los documentos privados y la autodeterminación informativa. Para la Sala Constitucional, el criterio de la recurrida no es válido. En esta sentencia se hace referencia a otras anteriores, entre ellas la 1779-2013 y la 18952-2014, en las cuales la Sala Constitucional indica que el correo electrónico y los documentos electrónicos almacenados en la computadora utilizada

por una persona están protegidos por el derecho fundamental al secreto de las comunicaciones y el control de ellos debe realizarse con las garantías establecidas por la Constitución Política. Además, la garantía del derecho es independiente de quien sea el dueño de la computadora. Se declaró con lugar el recurso y se ordenó a la directora ejecutiva no incurrir nuevamente en el hecho por el cual fue recurrida. Esta sentencia es importante para los profesionales en computación e informática, pues podría ser a ellos a quienes se les encargue la tarea de abrir el acceso a las cuentas de correo pertenecientes a otros funcionarios.

7. **Se ordena otorgar a un funcionario acceso a la información que consta en su computadora institucional para su defensa en proceso administrativo**

   Sentencia 7839-2015

En este recurso de amparo interpuesto contra el Instituto Costarricense del Deporte y la Recreación (ICODER), el recurrente indicó encontrarse separado de su puesto como medida cautelar en un procedimiento administrativo seguido en su contra. El recurrente acusó la clausura de su oficina, por lo cual él solicitó acceso a su computadora para obtener elementos probatorios necesarios para su defensa, pero, al serle denegado, quedó en estado de indefensión. Aunque el recurrido alegó que el recurrente podía acceder a la información solicitada desde otra computadora, el recurrente señaló la existencia de documentos presentes solo en su computadora. Aunque la Sala Constitucional comprendió que el motivo del ICODER para negarle acceso al recurrente era el riesgo de la alteración de los elementos probatorios, nada impedía la vigilancia de un funcionario del ICODER mientras el recurrente trabajara en la computadora. Se declaró el recurso parcialmente con lugar y se ordenó dar al recurrente acceso a lo solicitado. Es frecuente que sea a profesionales en computación e informática a quienes se les encarga impedir el acceso de su computadora a otro funcionario o empleado, vigilar a una persona mientras accede a aquella y buscar en un medio de almacenamiento electrónico elementos probatorios,

pues a veces estos han sido eliminados y deben recuperarse con herramientas especializadas.

Responsabilidad de los profesionales en computación e informática

Un profesional en computación e informática tiene el deber moral y legal de proteger los datos personales y de asegurarse de no solicitar al usuario, en una aplicación de software, más datos que los adecuados para el objetivo de esta. Para cumplir con su deber, se recomienda a los profesionales seguir principios como los siguientes:

1. Ante todo, no olvidar que la tecnología nunca debe dificultar o impedir a las personas ejercer sus derechos.

2. No abusar de su conocimiento tecnológico y de sus derechos de acceso para acceder, revelar, transferir o realizar cualquier otro acto que no sea parte de su función.

3. No requerir el ingreso de datos sensibles en una aplicación de software.

4. Minimizar la cantidad de datos recolectados, especialmente los de acceso restringido.

5. Crear aplicaciones de software lo suficientemente funcionales y flexibles para que las personas puedan ejercer su derecho de autodeterminación informativa.

6. Limitar el acceso a los datos por medio de la creación de roles de usuario y otras medidas que limiten el acceso.

7. Crear bitácoras que permitan saber quién ha accedido a cuáles datos, en cuál fecha y por cuánto tiempo. Esta información es muy útil en varias situaciones, por ejemplo, cuando se realiza un análisis forense.

8. Proveer la seguridad apropiada para el tipo de datos que se almacenan, procesan y transfieren.

9. Respetar el periodo máximo de retención de los datos y asegurar que aquellos que se deben conservar más allá de este periodo sean disociados de sus titulares.

10. Asegurar que los datos sean destruidos de forma apropiada al alcanzar el periodo máximo de retención y cuando no sea necesario conservarlos.

11. Instruir sobre la protección de datos a personas de otros campos, incluidas especialmente aquellas que tengan poder de decidir sobre tecnologías de información y comunicación, para crear conciencia de la importancia del tema.

Reflexión

La *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales* no es perfecta, pero constituye un primer esfuerzo para crear conciencia en la sociedad costarricense de la importancia de proteger los datos personales. La ley de delitos informáticos sanciona a quienes violen correspondencia, comunicaciones y datos personales. Sin embargo, más allá de la sanción que puedan recibir, los profesionales en computación e informática son capaces y responsables de garantizar el derecho fundamental de la autodeterminación informativa y hacer de este una realidad para todos los habitantes de Costa Rica.

Acerca de la autora

Marta Eunice Calderón Campos

Nació en San José, Costa Rica, en 1965. Obtuvo el bachillerado y la licenciatura en Computación e Informática en la Universidad de Costa Rica (UCR) en 1986 y 1988, respectivamente. Asimismo, obtuvo una maestría en Administración de Empresas en el INCAE en 1990 y en el 2005 una maestría en Ingeniería de Software en Texas Tech University, donde estudió gracias a una beca Fulbright. Ha laborado como docente en la Escuela de Ciencias de la Computación e Informática de la UCR desde 1988. Durante 13 años, trabajó además en el sector privado en tareas relacionadas con la gestión de recursos computacionales y la administración de proyectos para implementar sistemas de información. Sus temas de interés son la historia y los aspectos sociales de la computación, la interacción humano-computador y las diferencias de género.

En Costa Rica existe un amplio marco jurídico que afecta el ejercicio de la profesión informática. En esta obra se recopila la normativa más relevante para los profesionales en este campo y otros que participan en el desarrollo de tecnologías de información, en materia de privacidad, seguridad, propiedad intelectual, discapacidad y redes sociales. Se habla principalmente sobre derechos y obligaciones. Con respecto a la privacidad, se dieron los primeros pasos legales para asumir seriamente el tema de la protección de datos, pero todavía queda un largo camino por recorrer. En cuanto a la seguridad, la jurisprudencia costarricense ha dejado clara la responsabilidad de las organizaciones, en casos de fraude, si existe un riesgo intrínseco al negocio. Con respecto a la propiedad intelectual, hay un marco jurídico amplio que ofrece a quienes crean software instrumentos para protegerlo y determinar cómo quieren compartirlo. La legislación sobre discapacidad impone el deber de crear tecnologías que abran oportunidades a quienes no las tendrían de otra forma. Con respecto a las redes sociales, no hay legislación específica, pero sí existe una normativa que limita lo que se puede publicar a nivel general y sobre el lugar de trabajo.

ISBN 978-9968-46-673-8

9 789968 466738

EDITORIAL UCR