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

Ver ficha catalográfica y créditos
editorial.ucr.ac.cr

Contenido

Capítulo III. Propiedad intelectual del software

Capítulo IV. Discapacidad

Capítulo V. Redes sociales

Introducción

En 2031, los abogados serán componentes habituales de la mayoría de los equipos de desarrollo.

Grady Booch
Uno de los creadores de UML

Quienes eligen estudiar Computación e Informática o una carrera similar, por lo general, no piensan en cómo será su trabajo ni en sus futuras responsabilidades. Han tomado su decisión basados en su experiencia personal, lo que les dicen las personas a su alrededor y cuanto la sociedad les indica por medios como el sistema educativo, la Internet y la televisión. En términos generales, son usuarios asiduos de la tecnología. Empiezan sus estudios muy ilusionados, con deseos de aprender a programar, a crear aplicaciones de software, especialmente juegos, o asegurar redes de telecomunicaciones. La materia contemplada en la mayoría de los cursos de sus planes de estudio es de naturaleza técnica; por esta razón, a lo largo de sus años como estudiantes escuchan poco sobre aspectos éticos, morales y legales de esta disciplina. En algún curso, llamado "Informática y sociedad", o algo similar, casi al final de la carrera, se tocan estos temas. En este momento, los estudiantes empiezan a comprender que su carrera profesional no se limitará a sentarse frente a una computadora sin pensar en nada más que programarla.

Las computadoras y las telecomunicaciones han invadido todas las actividades humanas; han sido utilizadas para ofrecer grandes beneficios a la humanidad y crear oportunidades en muchos ámbitos. Sin embargo, también han generado situaciones no previstas en la legislación de los diferentes países. Por esto, hay vacíos legales que impiden actuar ante actos aparentemente no éticos e inmorales.

La normativa jurídica se actualiza a un paso mucho más lento que el de la tecnología de información. Esto se agrava porque los seres humanos son muy creativos y pronto encuentran formas de uso, no todas lícitas, que no fueron pensadas por los creadores de la tecnología.

La tecnología de información y comunicación ha creado nuevas maneras de cometer viejos delitos. Sin embargo, también genera otras oportunidades laborales y de interacción social para muchas personas; por ejemplo, aquellas con alguna discapacidad, quienes han encontrado en la computadora una fuente de trabajo y un medio de comunicación. A su vez, la tecnología puede ser una nueva fuente discriminatoria, cuando el diseño es difícil o inclusoimposible de utilizar para ciertos grupos.

Aquellas personas jóvenes que ingresaron a estudiar Computación e Informática, tal vez con la ilusión de convertirse en grandes desarrolladores de videojuegos, están llamadas a convertirse en artífices de una sociedad más justa. El fruto de su trabajo debería contribuir a garantizar derechos tales como privacidad, seguridad, propiedad intelectual y no discriminación. Sin embargo, dejar todo esto a la buena voluntad de las personas puede no ser efectivo; por tanto, en Costa Rica se ha emitido una serie de normativas que regulan parte de la labor de los profesionales en computación e informática.

El derecho informático ha aportado un conjunto de leyes, normas y principios aplicables a hechos y actos derivados del uso de herramientas informáticas para el tratamiento de datos. Recientemente se ha empezado a hablar de derecho telemático, el cual, además de la informática, cubre el ámbito de las telecomunicaciones. En estas áreas del derecho se contemplan la seguridad informática, los ciberdelitos –también llamados delitos informáticos– y la privacidad. Hess (2015) presenta una lista extensa de la normativa de derecho informático de Costa Rica. Aparte de esto, la regulación de la propiedad intelectual también

aporta un amplio conjunto de convenios internacionales, leyes y decretos ejecutivos que regulan la protección del software y otros productos. Asimismo, la normativa jurídica sobre discapacidad define el derecho de acceso a la información de todas las personas, en el cual las aplicaciones de software y otras tecnologías de información y comunicación tienen un papel fundamental. Las redes sociales, medios que cada vez ganan más importancia, no están exentas de ser reguladas, especialmente en cuanto publicar información sobre el lugar de trabajo.

Es difícil para los profesionales en computación e informática conocer y poner en práctica la normativa que les corresponde, debido a la gran variedad de tópicos y la cantidad de convenios internacionales, leyes, reglamentos y decretos ejecutivos vigentes en Costa Rica que los afectan. A esto se agrega la dificultad del lenguaje de estos documentos para quien no ha estudiado Derecho. Con el afán de reunir en una sola obra, adaptada a la realidad costarricense, la normativa que se considera más relevante actualmente para la mayoría de los profesionales en computación e informática, se inició un proceso de investigación que culminó con este libro.

Los temas cubiertos en esta obra son privacidad, seguridad, derechos de propiedad intelectual, discapacidad y redes sociales. La normativa a la que se hizo referencia anteriormente se relaciona con estos temas y es la que se tratará aquí. Se hablará principalmente sobre derechos y obligaciones, no tanto sobre dirimir un conflicto en los tribunales. Lo ideal es que las partes en controversia conozcan la normativa y se pongan de acuerdo con base en esta. Así, se evitarán largos, tediosos y caros juicios.

Al elaborar este libro, se tuvo conciencia de que los profesionales en computación e informática que laboran en algunos sectores de la economía altamente regulados, como la banca, están sujetos a una legislación adicional, pero por ser esta tan específica, no se le tomó aquí en cuenta.

Los temas que se presentan en esta obra son de gran relevancia para los profesionales en computación e informática, pues las tecnologías de información y comunicación se pueden convertir en herramientas para violar los derechos de privacidad, seguridad, no discriminación y propiedad intelectual, que la legislación garantiza a los habitantes de Costa Rica. Por esta razón, se ha aprobado una serie de normativas, tanto nacionales como internacionales, para proteger los derechos mencionados que los profesionales en estos ámbitos y quienes participan en el desarrollo de tecnologías de información deben conocer y acatar.

Dichos temas no son los únicos que atañen a estos profesionales, pero son comunes a prácticamente todo su gremio, por lo cual están incluidos en los libros de texto sobre el impacto social de las tecnologías de información y comunicación utilizadas en Costa Rica. Este tipo de obras es, generalmente, escrito por autores estadounidenses que analizan la normativa de su país. No existe un libro en el cual se recopile la normativa costarricense correspondiente.

En esta obra se abordan varios temas a lo largo de cinco capítulos, a saber:

Capítulo 1. Privacidad: presenta el concepto de privacidad, su respaldo legal como derecho y las amenazas contra esta causadas por la tecnología. Se refiere, además, a la importancia de la Sala Constitucional del Poder Judicial para la protección de datos junto a algunas de las sentencias emitidas y la legislación pertinente.

Capítulo 2. Seguridad informática: describe los atributos de la seguridad, la legislación pertinente, el papel del Centro de Respuesta de Incidentes de Seguridad Informática, y los conceptos de responsabilidad objetiva y la teoría del riesgo creado, los cuales se aplican al determinar la responsabilidad de los bancos en casos de fraude electrónico.

Capítulo 3. Propiedad intelectual del software: presenta el concepto de activo intangible y su importancia, la necesidad de protección legal del software y las formas existentes para lograrla. Presenta también la normativa legal pertinente sobre derechos de autor, mecanismo legal para proteger el software en Costa Rica, otras formas de protección y el papel del Registro de Propiedad Intelectual.

Capítulo 4. Discapacidad: explica el concepto de discapacidad, expone sus cifras en el mundo y en Costa Rica, así como la legislación pertinente. Ofrece, además, una guía para el desarrollo de tecnologías de información y comunicación accesibles.

Capítulo 5. Redes sociales: describe el concepto de derecho de libertad de expresión y sus limitaciones, y expone la legislación pertinente con respecto a comentarios negativos en redes sociales sobre el lugar de trabajo, y sobre el deber de mantener la confidencialidad.

Los capítulos pueden ser leídos en cualquier orden. Los únicos dos relacionados entre sí son el dedicado a privacidad (capítulo 1) y el de seguridad informática (capítulo 2), pues comparten legislación, aunque en cada caso se analizan secciones diferentes de esta.

Se debe aclarar que esta obra es, ante todo, descriptiva. Su objetivo principal consiste en dar a conocer a estudiantes y profesionales en computación e informática el marco jurídico en el cual se van a desempeñar en el mercado laboral costarricense. Tomadores de decisiones, creadores de políticas organizacionales y administradores de proyectos también pueden encontrar útil esta obra, pues el incumplimiento de la normativa conlleva quizás la materialización de riesgos para la organización. Es responsabilidad de los distintos niveles gerenciales establecer medidas de control interno; entre estas deben implementarse controles que garanticen el cumplimiento de la legislación.

Esta obra también puede ser de utilidad para otros profesionales que participan en el proceso de desarrollo de tecnologías de información y comunicación, tales como diseñadores gráficos, comunicadores, psicólogos y sociólogos.

La autora, con estudios en computación e informática y administración de empresas, utiliza un lenguaje comprensible para el público meta e incluye, cuando es posible, ejemplos de qué hacer para cumplir con la normativa y proteger los derechos de las personas usuarias de los sistemas de software y otras tecnologías de información y comunicación.

La autora quiere agradecer muy especialmente a la licenciada Eismey Álvarez, coordinadora de informática del Registro de Derechos de Autor y Conexos; a las licenciadas Lilliana Rojas y Yorleny Campos, gestoras de innovación de la unidad Proinnova de la Universidad de Costa Rica; a la ingeniera Leidy Guillén Cordero, gerente de gobierno electrónico del Ministerio de Ciencia, Tecnología y Telecomunicaciones; a Manuel Hidalgo, graduado tanto en Derecho como en Computación e Informática; y a la doctora Gabriela Barrantes y los magisteres Braulio Solano y Luis Quesada, docentes en la Escuela de Ciencias de la Computación e Informática de la Universidad de Costa Rica, por sus valiosos aportes. También agradece a su asistente, Andrea Solano, por su colaboración.

En el segundo semestre de 2015, la autora disfrutó de una licencia sabática, la cual le posibilitó crear esta obra. Por esto, agradece profundamente a la Universidad de Costa Rica por brindarle esta valiosa oportunidad.

Esta es una obra para todas aquellas personas que escogieron la profesión de Computación e Informática, quienes enfrentan grandes retos para resolver problemas cada día más complejos. A pesar de tener la habilidad de entender el lenguaje de las computadoras y las telecomunicaciones, la mayoría no domina el lenguaje

legal. El objetivo de este libro es facilitarles el conocimiento y la comprensión del marco jurídico en el cual se desenvuelve su labor.

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 sobrela 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.° 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 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 laadministración 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.

CAPÍTULO II
SEGURIDAD INFORMÁTICA

Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los ordenadores.

Kevin Mitnick
Hacker

Resumen

Dada la gran dependencia de las computadoras y las telecomunicaciones en todos los ámbitos de la actividad humana, la seguridad informática es motivo de preocupación mundial. Es un tema complejo, pues son muchos los aspectos contemplados dentro de esta; disponibilidad, confiabilidad, integridad, responsabilidad, autenticidad y no repudio son sus principales atributos. Se han creado tecnologías con el fin de garantizar en un sistema un grado aceptable de cada uno de estos atributos; sin embargo, la existencia de un marco legal puede motivar a las personas y organizaciones a utilizar dichas tecnologías. En Costa Rica, existen varias leyes relacionadas con la seguridad informática; en particular, destaca la *Ley de Certificados, Firmas Digitales y Documentos Electrónicos,* la cual da seguridad jurídica a herramientas tecnológicas necesarias para garantizar la seguridad informática. Además, el Gobierno creó el Centro de Respuesta de Incidentes de Seguridad Informática, el cual, según el *Decreto 37052-MICIT Creación del Centro de Respuesta de Incidentes de Seguridad Informática CSIRT-CR* del 9 de marzo de 2012, tiene entre sus funciones "promover la adopción

de políticas públicas para alcanzar la mayor eficiencia y eficacia en los recursos informáticos de las entidades públicas" (p. 1). Aparte de eso, los conceptos de responsabilidad objetiva y teoría del riesgo creado, los cuales prevalecen en las sentencias de los tribunales en los casos de sustracción monetaria fraudulenta de cuentas bancarias, son el fundamento legal para que las entidades bancarias sean declaradas las responsables y se les condene a reparar el daño causado a la víctima. Sin embargo, la responsabilidad objetiva no es exclusiva de los bancos; esta corresponde a todas las organizaciones que custodien y administren bienes ajenos. Esto debe constituir un incentivo económico para que bancos y otras entidades mejoren sus medidas de seguridad. Los profesionales en computación e informática tienen un papel de gran importancia en la garantía de la seguridad informática; es su responsabilidad formarse continuamente en este campo.

Introducción

Se sabe que Internet ha tenido un efecto muy importante en la economía: ha bajado el costo de las transacciones (Tapscott, 2006). Ejemplos de estas son realizar un trámite en una institución gubernamental, pagar el recibo de un servicio público, comprar por Internet y negociar un contrato con un proveedor corporativo para recibir un servicio. El costo de una transacción para quien desea adquirir un bien o servicio está dado por tres costos: el de búsqueda –encontrar el bien y el proveedor–, el de contratación –negociar las condiciones del intercambio– y el de coordinación –engranar procesos y productos de distintas entidades– (Tapscott, 2006). Al bajar estos costos, las instituciones, empresas y personas se benefician. Lo ideal es sacar provecho de las facilidades brindadas por las

tecnologías de información y comunicaciones en un ambiente seguro, pero no siempre ocurre así.

Las noticias en los periódicos confirman que el ciberespacio, ese ámbito virtual creado con tecnologías de información y comunicación que es un "lugar de comunicación social transnacional, universal y en permanente evolución tecnológica" (Miró, 2011, p. 4), es muy propicio para cometer delitos de mucho impacto. Fraudes con tarjetas de crédito, datos confidenciales publicados sin el debido permiso, sustracción masiva de dinero de cuentas bancarias y páginas web alteradas son solo algunos ejemplos que muestran la existencia de vulnerabilidades –puntos débiles aprovechados por terceros para realizar ataques– en los sistemas de software y telecomunicaciones. Pese a que las organizaciones han establecido mecanismos de protección, estos parecen nunca ser suficientes. En la búsqueda constante de soluciones se encuentran personas cuya tarea es garantizar la seguridad informática.

En este capítulo se utilizan los términos seguridad informática y ciberseguridad indistintamente. El objetivo de la primera es "reducir la probabilidad de materialización de las amenazas; limitando los daños o averías resultantes; y logrando que se reanuden las operaciones normales tras un incidente de seguridad, en un plazo de tiempo razonable y a un coste aceptable" (Unión Internacional de Telecomunicaciones, 2007, p. v). Por su parte, la ciberseguridad tiene como objetivo "contribuir a la preservación de las fuerzas y medios organizativos, humanos, financieros, tecnológicos e informativos, adquiridos por las instituciones, para realizar sus objetivos" (Unión Internacional de Telecomunicaciones, 2007, p. v). Ambos conceptos contemplan los procesos, los métodos y las técnicas para la protección del software, el hardware, las redes de telecomunicaciones, la infraestructura tecnológica y los servicios brindados mediantes todos los anteriores.

Otro concepto relacionado con los dos previamente mencionados es el de la seguridad de la información, el cual se refiere a las medidas tomadas para proteger los datos según su grado de importancia y criticidad. La seguridad de la información se interseca con los otros dos conceptos expuestos anteriormente, pero no está contenida en ninguno de ellos, pues no toda la información se almacena o transmite por medios digitales.

Anderson (2001) califica las debilidades en la seguridad de la información no solo como un problema tecnológico, sino como el resultado de la existencia de una serie de incentivos económicos perversos. Ejemplos de estos son los sistemas jurídicos que exoneran de responsabilidad a los bancos, la tendencia a crear aplicaciones de software inseguras para facilitar el trabajo de los desarrolladores, el uso de tecnologías propietarias inseguras con el fin de atar a los usuarios y aumentarles el costo de cambio de proveedor o producto, y la estructura de los mercados favorecedora al primer proveedor en ingresar al mercado, por lo cual se descuida la seguridad con tal de sacar un producto al mercado antes que la competencia.

Aunado a lo anterior, muchos usuarios no tienen conciencia de la importancia de la seguridad, por lo cual no están dispuestos a pagar por ella. Por tanto, esta debe afrontarse de manera integral; se debe considerar no solo el punto de vista tecnológico, sino también el humano, el legal y el económico (Unión Internacional de Telecomunicaciones, 2007). Una estrategia de seguridad organizacional debe tomar en cuenta todas estas aristas.

La seguridad informática y la de la información se han convertido en temas de seguridad nacional. Los Gobiernos de muchos países, incluido el de Costa Rica, están conscientes del riesgo que representan las violaciones de la seguridad, por su impacto potencialmente dañino. Por ello, además de crear políticas para fortalecer la seguridad de los sistemas y de fomentar la formación en este campo, han

promulgado normativa legal que debe servir como contrapeso a los incentivos perversos.

En este capítulo, se repasan los atributos de la seguridad y se analizan las leyes costarricenses relacionadas con la seguridad informática. Además, se menciona el papel que está llamado a tener el Centro de Respuesta de Incidentes de Seguridad Informática en Costa Rica, se explica el fundamento legal de la responsabilidad bancaria en los casos de fraude electrónico, y se finaliza al describir las responsabilidades de los profesionales en computación e informática respecto al tema de la seguridad.

Los atributos de la seguridad

En el contexto de las tecnologías de información y comunicaciones, la seguridad se puede definir como la ausencia de accesos no autorizados y de modificaciones al estado de un sistema. Este concepto implica la concurrencia de tres atributos (Avižienis, Laprie y Randell, 2001), a saber:

1. Disponibilidad solo a usuarios autorizados: que no se dé denegación de acceso o servicio.
2. Confidencialidad: ausencia de revelación no autorizada de datos.
3. Integridad: ausencia de alteraciones no autorizadas.

Se habla además de tres atributos secundarios de la seguridad que también son muy importantes (Avižienis *et al.*, 2001). Estos son:

1. Responsabilidad: disponibilidad e integridad de la identidad de la persona que ha realizado una

operación en el sistema, altere o no el estado de este.

2. Autenticidad: integridad del contenido y el origen de un mensaje, también de otra información como fecha y hora de envío.
3. No repudio: disponibilidad e integridad de la identidad de la persona emisora de un mensaje o de quien lo recibe, de modo que no pueda negar haberlo enviado o recibido.

¿Por qué son importantes todos estos atributos? Porque saber de su cumplimiento da confianza a los usuarios de los sistemas, elemento necesario para usar las facilidades de las tecnologías de información y comunicación y para aprovechar sus beneficios. Por ejemplo: a nivel mundial, el gran éxito del comercio electrónico se debe a que las personas y empresas acceden a un mercado global que ofrece una mayor variedad de bienes y servicios, a menor precio en comparación con comercios locales. Sin embargo, hay un motivo adicional fundamental para su éxito. Los compradores confían en que los datos personales y los de su tarjeta de crédito están protegidos (confiabilidad), el vendedor realmente existe (responsabilidad) y recibirán aquello por lo cual pagaron. A la vez, los vendedores confían en que quienes compran no negarán haber comprado un bien (no repudio). En Costa Rica, la penetración del comercio electrónico no se dio tan aceleradamente como en otros países; entre las principales razones de esto están la falta de seguridad y la desconfianza de los compradores (Programa Sociedad de la Información y el Conocimiento, 2008).

Se han creado tecnologías para tratar de garantizar que un sistema cuenta con, al menos, un grado aceptable de cada uno de los seis atributos anteriormente mencionados. Algunos ejemplos son el cifrado y la firma digital. Sin embargo, la seguridad pocas veces es absoluta.

La seguridad informática, preocupación mundial

La seguridad informática es una preocupación presente en múltiples niveles, a saber: personal, institucional y organizacional, nacional e internacional. Las personas se interesan personalmente por la seguridad de sus datos. Las instituciones y empresas establecen mecanismos de seguridad para proteger datos bajo su custodia y transacciones tanto propias como de entes externos, tales como proveedores y clientes. Los Gobiernos de los distintos países están conscientes de la importancia de la tecnología de información y comunicación como herramienta de desarrollo y prosperidad de los pueblos, y saben que su seguridad es clave para garantizar los servicios brindados a los ciudadanos e incluso el respeto de sus derechos. A nivel internacional, las naciones trabajan conjuntamente para crear una cultura global de ciberseguridad, coordinar esfuerzos en la lucha contra el cibercrimen, colaborar en investigaciones y proveer asistencia, además de emitir normativa internacional que permita castigar los delitos contra la seguridad.

Conscientes del uso intensivo de las computadoras y las telecomunicaciones en todos los ámbitos de la sociedad, varios organismos y foros internacionales, tales como la Unión Internacional de Telecomunicaciones (UIT), las Naciones Unidas (ONU) y la Organización de Estados Americanos (OEA), han emitido múltiples resoluciones relacionadas con la ciberseguridad. Costa Rica es miembro de todos los organismos anteriormente mencionados, por lo cual estas resoluciones deben servir de guía en cuanto a lo que se debe considerar en la legislación costarricense sobre seguridad.

Legislación costarricense relacionada con seguridad

La legislación costarricense relacionada con seguridad cubre materias tales como:

1. Certificados, firmas digitales y documentos electrónicos.
2. Protección de datos personales.
3. Protección de la niñez y la adolescencia.
4. Delitos informáticos.

Como se puede notar, las materias cubiertas son de naturaleza variada, pues la seguridad es un tema muy amplio. Pese a que, a primera vista, la protección de la niñez y la adolescencia no parece un asunto de seguridad informática ni de la información, se incluye en este capítulo, pues se considera un deber de la sociedad proteger a estos grupos. La tecnología de información y comunicación ha facilitado a la población infantil y juvenil el acceso a material potencialmente dañino, tal como la pornografía o el incentivo para consumir drogas. Acceder a este contenido no solo puede poner en riesgo la seguridad personal y la integridad de las personas jóvenes, sino que puede exponer sus datos personales y los de sus progenitores, como números de tarjetas de crédito si los sitios web que visitan son de pago.

La legislación actual es relativamente nueva, pues aunque las amenazas ya existían desde antes, las violaciones a la seguridad se han hecho más comunes y destructivas con el advenimiento de las tecnologías de información y comunicación. Las siguientes subsecciones se dedican a las leyes pertinentes.

Ley 8131 de la Administración Financiera de la República y Presupuestos Públicos

Por su título, la *Ley de la Administración Financiera de la República y Presupuestos Públicos* parece no estar relacionada con el tema de seguridad informática. Sin embargo, sí lo está, a pesar de referirse únicamente al hardware y el software de las computadoras de la administración financiera y de proveeduría del sector público de Costa Rica. A continuación, se transcriben los incisos m, n y ñ del artículo 110 y el artículo 111 de esta ley, relacionados con el tema de seguridad.

> Artículo 110. Hechos generadores de responsabilidad administrativa. Además de los previstos en otras leyes y reglamentaciones propias de la relación de servicio, serán hechos generadores de responsabilidad administrativa, independientemente de la responsabilidad civil o penal a que puedan dar lugar, los mencionados a continuación:
>
> m) El ingreso, por cualquier medio, a los sistemas informáticos de la Administración Financiera y de Proveeduría, sin la autorización correspondiente.
>
> n) Obstaculizar el buen desempeño de los sistemas informáticos de la Administración Financiera y de Proveeduría, omitiendo el ingreso de datos o ingresando información errónea o extemporánea.
>
> ñ) Causar daño a los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos de la Administración Financiera y de Proveeduría.
>
> Artículo 111. Delito informático. Cometerán delito informático, sancionado con prisión de uno a tres años, los funcionarios públicos o particulares que realicen, contra los sistemas informáticos de la Administración Financiera y de Proveeduría, alguna de las siguientes acciones:
>
> a) Apoderarse, copiar, destruir, alterar, transferir o mantener en su poder, sin el debido permiso de la autoridad competente, información,

programas o bases de datos de uso restringido.

b) Causar daño, dolosamente, a los componentes lógicos o físicos de los aparatos, las máquinas o los accesorios que apoyan el funcionamiento de los sistemas informáticos.

c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas.

d) Utilizar las facilidades del Sistema para beneficio propio o de terceros.

Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos

Antes de comentar sobre la *Ley 8454 de Certificados, Firmas Digitales y Documentos Electrónicos,* se expondrán los artículos 368, 369, 370, 379 y 388 de la *Ley 7130 Código Procesal Civil* de Costa Rica, en el cual se definen conceptos fundamentales que dan sentido a la Ley 8454, a saber: documento, documento público, instrumento público y documento privado. Además, se establece el valor probatorio y el reconocimiento de estos ante un juez.

Artículo 368. Distintas clases de documentos. Son documentos los escritos, los impresos, los planos, los dibujos, los cuadros, las fotografías, las fotocopias, las radiografías, las cintas cinematográficas, los discos, las grabaciones magnetofónicas y, en general, todo objeto mueble que tenga carácter representativo o declarativo.

Artículo 369. Documentos e instrumentos públicos. Son documentos públicos todos aquéllos [*sic*] que hayan sido redactados o extendidos por funcionarios públicos, según las formas requeridas y dentro del límite de sus atribuciones.

Las fotocopias de los documentos originales tendrán el carácter que este artículo establece, si el funcionario que las autoriza certifica en ellas la razón de que son copias fieles de los originales, y cancela las especies fiscales de ley.

Es instrumento público la escritura otorgada ante un notario público, así como cualquier otro documento al cual la ley le dé expresamente ese carácter.

Artículo 370. Valor probatorio. Los documentos o instrumentos públicos, mientras no sean argüidos de falsos, hacen plena prueba de la existencia material de los hechos que el oficial público afirme en ellos haber realizado él mismo, o haber pasado en su presencia, en el ejercicio de sus funciones.

Artículo 379. Documentos privados. Los documentos privados reconocidos judicialmente o declarados como reconocidos conforme con la ley, hacen fe entre las partes y con relación a terceros, en cuanto a las declaraciones en ellos contenidas, salvo prueba en contrario.

Artículo 388. Reconocimiento de documentos privados. Los documentos privados y la correspondencia serán reconocidos ante el juez por la parte que los haya suscrito o sus causahabientes, cuando así se pida.

No será necesario dicho reconocimiento cuando la parte a quien perjudique el documento lo hubiere aceptado expresa o tácitamente.

El reconocimiento judicial de los documentos privados se hará en la misma forma que la confesión judicial.

El *Código Procesal Civil* en vigencia no se refiere a los documentos electrónicos que actualmente son de uso común. El documento tradicional está escrito en un soporte material, en general de papel, y requiere, en muchas ocasiones, de una firma ológrafa (manuscrita) como requisito para considerarle auténtico y confiable (Viega y Rodríguez, 2005).

Los documentos electrónicos introducen un nivel de complejidad mayor por varias razones (Viega y Rodríguez, 2005). La primera es que un documento electrónico puede estar únicamente almacenado en una memoria, pero también pueden existir copias en papel; además, no hay diferencia entre el original y una copia. Un documento electrónico puede haberlo generado una persona, quien lo

creó y almacenó en algún medio, o una computadora a partir de una serie de instrucciones (software) y un conjunto de datos, como, por ejemplo, un estado de cuenta bancario que un sistema genera automáticamente el último día de cada mes. Con los documentos electrónicos, surgió la necesidad de contar con un sustituto para la firma ológrafa: la firma digital.

La Asamblea Legislativa aprobó un nuevo Código Procesal Civil (Ley N.° 9342) en diciembre de 2015, el cual entrará en vigencia 30 meses después de su publicación en *La Gaceta*, es decir, en octubre del 2018. Los conceptos relacionados con documentos cambian, pues en la nueva ley se hace mención a las tecnologías de información y comunicación. Dichas modificaciones no invalidan el resto de este apartado, pues más bien se fortalecen algunas de las herramientas tecnológicas expuestas a continuación, como es la firma digital. Por ejemplo, el inciso 27.1 del artículo 27 del nuevo código señala, con respecto a la firma:

> Artículo 27. Gestiones escritas y efectos
>
> 27.1. Firma. Cuando las gestiones de las partes deban hacerse por escrito llevarán su firma. Si una persona estuviera imposibilitada, otra lo hará a su ruego, su rúbrica será autenticada por un abogado y el gestionante estampará su huella digital, salvo imposibilidad absoluta.
>
> *Cuando se utilicen medios telemáticos, informáticos o de nuevas tecnologías, la autorización del documento se hará de la forma establecida por la ley o por la Corte Suprema de Justicia* [resaltado añadido], según se dispone en la Ley N.° 7333, Ley Orgánica del Poder Judicial, de 5 de mayo de 1993.

Ante el uso cada vez más intensivo de las computadoras para generar documentos y de las telecomunicaciones para realizar transacciones de toda índole, y dadas las características de los documentos electrónicos, se requiere de un marco legal que dé seguridad jurídica a las herramientas tecnológicas necesarias para garantizarla a

nivel informático. La *Ley de Certificados, Firmas Digitales y Documentos Electrónicos* es fundamental en este sentido. Su artículo 1 define el ámbito de esta ley:

> Artículo 1. Ámbito de aplicación. Esta Ley se aplicará a toda clase de transacciones y actos jurídicos, públicos o privados, salvo disposición legal en contrario, o que la naturaleza o los requisitos particulares del acto o negocio concretos resulten incompatibles.
>
> El Estado y todas las entidades públicas quedan expresamente facultados para utilizar los certificados, las firmas digitales y los documentos electrónicos, dentro de sus respectivos ámbitos de competencia.

Sobre esta ley, es importante destacar lo siguiente:

> La ley tiene por objeto regular la utilización de la firma digital, otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad, es decir, se equipara la firma digital a la firma manuscrita, en cuanto a su validez jurídica y se autoriza al Estado y a todas las entidades públicas para su utilización (Artículo segundo). Se valida así el uso de documentos electrónicos en materia contractual, notificaciones, certificaciones, constancias, trámite de documentos en el Registro Nacional, entre otros (Artículo quinto) (Mora y Guzmán, 2008, p. 113).

A continuación se repasa uno de los puntos mencionados en la cita anterior. En lo respectivo a documentos electrónicos, se les da reconocimiento de equivalencia funcional, es decir, se les equipara con los documentos en medios físicos mencionados en el *Código Procesal Civil,* tal como se indica en el artículo 3 de la *Ley de Certificados, Firmas Digitales y Documentos Electrónicos.* Además, en el artículo 4 se reconoce que los documentos electrónicos tienen fuerza probatoria para procesos judiciales. Ambos artículos se transcriben seguidamente.

Artículo 3. Reconocimiento de la equivalencia funcional. Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos.

En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los electrónicos como los físicos. No obstante, el empleo del soporte electrónico para un documento determinado no dispensa, en ningún caso, el cumplimiento de los requisitos y las formalidades que la ley exija para cada acto o negocio jurídico en particular.

Artículo 4. Calificación jurídica y fuerza probatoria. Los documentos electrónicos se calificarán como públicos o privados, y se les reconocerá fuerza probatoria en las mismas condiciones que a los documentos físicos.

En cuanto a la firma digital, de la definición dada en la ley se deduce que es una herramienta de seguridad útil para garantizar los siguientes atributos primarios y secundarios de la seguridad: integridad, responsabilidad, autenticidad y no repudio de los mensajes y las comunicaciones. El artículo 8 define el concepto de firma digital.

Artículo 8. Alcance del concepto. Entiéndese por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico.

Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.

En la definición de firma digital presente en la ley no se hace referencia al cifrado, también llamado criptografía. Sin embargo, la Dra. Gabriela Barrantes, catedrática de la Universidad de Costa Rica y especialista en seguridad,

afirma que, con el estado actual de la tecnología, la única forma de garantizar los atributos de seguridad antes mencionados es mediante el uso de criptografía asimétrica, conocida también como de llave pública y de dos llaves –pública y privada– (comunicación personal, 15 de octubre de 2015). Si en el futuro apareciera una nueva técnica que ofrezca un nivel de seguridad igual o mayor, no sería necesario cambiar la ley.

La criptografía de llave pública sirve tanto para cifrar un mensaje como para firmarlo digitalmente. En este último caso, la llave privada, de uso exclusivo del titular de la firma digital, se usa para generar dicha firma cuando se va a enviar un mensaje. La llave pública es del conocimiento de terceros y la utilizan los destinatarios para verificar que el mensaje o documento digital recibido proviene de quien dice ser el remitente.

El artículo 9 de la ley equipara los documentos con firma digital con los que tienen firma manuscrita en términos de valor y eficacia probatoria. Además, obliga a los documentos públicos electrónicos a llevar firma digital certificada. El artículo 9 indica lo siguiente:

> Artículo 9. Valor equivalente. Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.
>
> Los documentos públicos electrónicos deberán llevar la firma digital certificada.

Una firma digital certificada se asocia con un certificado digital. Este es un mecanismo criptográfico de seguridad fundamental para que distintas organizaciones o personas tengan confianza entre ellas mismas. Los certificados digitales son también materia de la *Ley de Certificados,*

Firmas Digitales y Documentos Electrónicos; estos son emitidos por entidades llamadas certificadores.

Los certificados digitales son necesarios para dar confiabilidad a las firmas digitales. Cualquier persona puede tener una firma digital no certificada con la cual suplante la identidad de otra. El certificado garantiza la verdadera pertenencia de una firma digital a la persona física o jurídica que dice ser.

Se considerará como autor y responsable de toda comunicación electrónica que se asocie con una firma digital certificada al titular del certificado digital correspondiente; así se especifica en el artículo 10 de la ley. Esto implica que las personas físicas y jurídicas son responsables de salvaguardar la información necesaria para crear la firma digital. En el estado actual de la tecnología, esta información es la llave privada. El artículo 10 señala así:

> Artículo 10. Presunción de autoría y responsabilidad. Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.
>
> No obstante, esta presunción no dispensa el cumplimiento de las formalidades adicionales de autenticación, certificación o registro que, desde el punto de vista jurídico, exija la ley para un acto o negocio determinado.

El artículo 11 de esta misma ley identifica los propósitos para los cuales los certificados digitales serán utilizados como garantía, confirmación o validación técnica; el artículo 12 establece que todas las organizaciones y las personas tienen la facultad de establecer los mecanismos de certificación convenientes para sí mismas. Ambos artículos se transcriben a continuación.

Artículo 11. Alcance. Entiéndese por certificado digital el mecanismo electrónico o digital mediante el que se pueda garantizar, confirmar o validar técnicamente:

a) La vinculación jurídica entre un documento, una firma digital y una persona.

b) La integridad, autenticidad y no alteración en general del documento, así como la firma digital asociada.

c) La autenticación o certificación del documento y la firma digital asociada, únicamente en el supuesto del ejercicio de potestades públicas certificadoras.

d) Las demás que establezca esta Ley y su Reglamento.

Artículo 12. Mecanismos. Con las limitaciones de este capítulo, el Estado, las instituciones públicas y las empresas públicas y privadas, las personas jurídicas y los particulares, en general, en sus diversas relaciones, estarán facultados para establecer los mecanismos de certificación o validación que convengan a sus intereses.

Para tales efectos podrán:

a) Utilizar mecanismos de certificación o validación máquina a máquina, persona a persona, programa a programa y sus interrelaciones, incluso sistemas de llave pública y llave privada, firma digital y otros mecanismos digitales que ofrezcan una óptima seguridad.

b) Establecer mecanismos de adscripción voluntaria para la emisión, la percepción y el intercambio de documentos electrónicos y firmas asociadas, en función de las competencias, los intereses y el giro comercial.

c) De consuno, instituir mecanismos de certificación para la emisión, la recepción y el intercambio de documentos electrónicos y firmas asociadas, para relaciones jurídicas concretas.

d) Instaurar, en el caso de dependencias públicas, sistemas de certificación por intermedio de particulares, quienes deberán cumplir los trámites de la Ley de contratación administrativa.

e) Fungir como un certificador respecto de sus despachos y funcionarios, o de otras dependencias públicas, en el caso del Estado y las demás instituciones públicas.

f) Ofrecer, en el caso de las empresas públicas cuyo giro lo admita, servicios comerciales de certificación en condiciones de igualdad con las empresas de carácter privado.

g) Implantar mecanismos de certificación para la tramitación, gestión y conservación de expedientes judiciales y administrativos.

Acerca de cómo se acreditan los certificadores, se tiene que:

> A pesar de que las tendencias actuales apuntan hacia esquemas de autorregulación, prevaleció la posición de que el Poder Ejecutivo mantuviera un papel en el proceso, mediante la creación de la Dirección de Certificadores de Firmas Electrónicas, órgano adscrito al Ministerio de Ciencia y Tecnología, que será la entidad administradora y supervisora del Sistema de Certificación. Las empresas que ofrezcan el servicio de certificación deberán cumplir con normas internacionales que serán supervisadas por el Ministerio de Ciencia y Tecnología (MICIT) mediante la Dirección de Certificadores de Firma Digital y el Ente Costarricense de Acreditación (ECA) (Mora y Guzmán, 2008, p. 116).

Según el artículo 23 de la Ley 8454, la Dirección de Certificadores de Firma Digital, adscrita al Ministerio de Ciencia, Tecnología y Telecomunicaciones, es la encargada de administrar y supervisar el sistema de certificación. El Sistema Nacional de Certificación Digital (s. f.) informa sobre la gestión de certificados. Las personas jurídicas públicas o privadas, nacionales o extranjeras, que deseen emitir certificados digitales deberán inscribirse ante dicha entidad; los requisitos y trámites para convertirse en un certificador se especifican en los artículos 18 al 22 de esta misma ley. Además, su capítulo quinto plantea sanciones a los certificadores que incumplan con la normativa.

La *Ley de Certificados, Firmas Digitales y Documentos Electrónicos* se complementa con su reglamento, la Política de Certificados para la Jerarquía Nacional de Certificadores Registrados, la Política de Formatos Oficiales de los Documentos Electrónicos Firmados Digitalmente y la directriz número 067-MICITT-H-MEIC Masificación de la Implementación y el Uso de la Firma Digital en el Sector Público Costarricense. Esta directriz tiene como objetivo que las personas físicas puedan utilizar, en las instituciones del sector público, la firma digital certificada para cualquier trámite. Esto implica ajustar los sistemas de software de las instituciones.

La firma digital, además de ser un instrumento de seguridad, sirve para simplificar, agilizar y bajar el costo de los trámites, en términos de tiempo y recursos, tanto del lado de las organizaciones oferentes de bienes y servicios como de las personas físicas y jurídicas que los demanden.

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

El tema de la seguridad está, de distintas formas, estrechamente relacionado con el de la privacidad. Por ejemplo, para mantener esta última en un conjunto de datos, es necesario, entre otras acciones, implementar mecanismos de seguridad que impidan el acceso a personas no autorizadas. En este caso, la seguridad ayuda a reforzar la privacidad. Aparte de eso, para combatir el terrorismo y el crimen organizado y para brindar mayor seguridad a la población, se han establecido mecanismos que operan en detrimento de la privacidad de las personas; en este caso, se sacrifica una en beneficio de la otra. En esta sección, se analiza la *Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales,* la cual contempla tanto el tema de seguridad como el de privacidad.

Anteriormente, en el capítulo dedicado a la privacidad, se mencionaron dicha ley y su reglamento, pues en ellos se definen los derechos de las personas titulares. Sin embargo, además de los derechos, en la sección III, titulada "Seguridad y confidencialidad del tratamiento de los datos", se establecen las responsabilidades de la persona a cargo de una base de datos en lo referente a la seguridad de estos, confidencialidad y protocolos de actuación. Parte de estas responsabilidades recaerán sobre profesionales en computación e informática. Se transcribe seguidamente el artículo 10 de la ley:

> 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.

Las medidas de seguridad mencionadas en el artículo anterior deben estar acordes con las características de los datos, el historial de vulnerabilidades ocurridas y el impacto de estas y de las futuras, entre otros, según lo especifica el artículo 35 del reglamento de la ley. Además, dichas medidas deben actualizarse en función de cambios

en los procesos de tratamiento de los datos, las vulnerabilidades y la plataforma tecnológica utilizada, tal como se indica en el artículo 37 del mismo reglamento. Los artículos 35 y 37 se transcriben a continuación.

> Artículo 35. Factores para determinar las medidas de seguridad. El responsable determinará las medidas de seguridad, aplicables a los datos personales que trate o almacene, considerando los siguientes factores:
>
> a) La sensibilidad de los datos personales tratados, en los casos que la ley lo permita;
>
> b) El desarrollo tecnológico;
>
> c) Las posibles consecuencias de una vulneración para los titulares de sus datos personales.
>
> d) El número de titulares de datos personales;
>
> e) Las vulnerabilidades previas ocurridas en los sistemas de tratamiento o almacenamiento;
>
> f) El riesgo por el valor, cuantitativo o cualitativo, que pudieran tener los datos personales; y
>
> g) Demás factores que resulten de otras leyes o regulación aplicable al responsable.
>
> Artículo 37. Actualizaciones de las medidas de seguridad. Los responsables deberán actualizar las medidas de seguridad cuando ocurran los siguientes eventos:
>
> a) Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable;
>
> b) Se produzcan modificaciones sustanciales en el tratamiento o almacenamiento, que deriven en un cambio del nivel de riesgo;
>
> c) Se modifique la plataforma tecnológica;

d) Se vulneren los sistemas de tratamiento o almacenamiento de datos personales, de conformidad con lo dispuesto en la Ley y el presente Reglamento; o,

e) Exista una afectación a los datos personales, distinta a las anteriores. En el caso de datos personales sensibles, cuando la ley lo permita, el responsable deberá revisar y, en su caso, actualizar las medidas de seguridad correspondientes, al menos una vez al año.

En los artículos 31 y 32 del capítulo IV del reglamento a la ley –titulado "Del Tratamiento de los Datos Personales y Medidas de Seguridad"– se establecen con detalle, entre otros, los pasos a seguir para el tratamiento de los datos, las condiciones para este, los deberes del encargado y los protocolos mínimos de actuación. El capítulo IV es de interés para aquellos profesionales en computación e informática que sean responsables de bases de datos. Se transcriben a continuación estos artículos.

Artículo 31. Obligaciones del encargado. El encargado tendrá las siguientes obligaciones en el tratamiento de las bases de datos personales:

a) Tratar únicamente los datos personales conforme a las instrucciones del responsable;

b) Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;

c) Implementar las medidas de seguridad y cumplir con los protocolos mínimos de actuación conforme a la Ley, el presente Reglamento y las demás disposiciones aplicables;

d) Guardar confidencialidad respecto de los datos personales tratados;

e) Abstenerse de transferir o difundir los datos personales, salvo instrucciones expresas por parte del responsable.

f) Suprimir los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones del

responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

Artículo 32. De los protocolos mínimos de actuación. Los responsables deberán confeccionar un protocolo mínimo de actuación, el cual deberá ser transmitido al encargado para su fiel cumplimiento y donde al menos, se deberá especificar lo siguiente:

a) Elaborar políticas y manuales de privacidad obligatorios y exigibles al interior de la organización del responsable.

b) Poner en práctica un manual de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales.

c) Establecer un procedimiento de control interno para el cumplimiento de las políticas de privacidad.

d) Instaurar procedimientos ágiles, expeditos y gratuitos para recibir y responder dudas y quejas de los titulares de los datos personales o sus representantes, así como para acceder, rectificar, modificar, bloquear o suprimir la información contenida en la base de datos y revocar su consentimiento.

e) Crear medidas y procedimientos técnicos que permitan mantener un historial de los datos personales durante su tratamiento.

f) Constituir un mecanismo en el cual el responsable transmitente, le comunica al responsable receptor, las condiciones en las que el titular consintió la recolección, la transferencia y el tratamiento de sus datos. Estas medidas, así como sus posteriores modificaciones, deberán ser inscritas ante la Agencia como protocolos mínimos de actuación.

En cuanto a políticas y medidas de seguridad, realmente el reglamento no plantea nada desconocido para quienes han estudiado computación e informática. Lo novedoso es la obligación de inscribir la base de datos ante la Agencia de Protección de Datos de los Habitantes (Prodhab), y la de informar a esta y al titular cuando se dé una irregularidad en el tratamiento de sus datos, tal como se indica en los artículos 38 y 39.

Artículo 38. Vulnerabilidad de seguridad. El responsable deberá informar al titular sobre cualquier irregularidad en el tratamiento o almacenamiento de sus datos, tales como pérdida, destrucción, extravío, entre otras, como consecuencia de una vulnerabilidad de la seguridad o que tuviere conocimiento del hecho, para lo cual tendrá cinco días hábiles a partir del momento en que ocurrió la vulnerabilidad, a fin de que los titulares de estos datos personales afectados puedan tomar las medidas correspondientes.

Dentro de este mismo plazo deberá iniciar un proceso de revisión exhaustiva para determinar la magnitud de la afectación, y las medidas correctivas y preventivas que correspondan.

Artículo 39. Información mínima. El responsable deberá informar al titular y a la Agencia, en caso de vulnerabilidades de seguridad, al menos lo siguiente:

a) La naturaleza del incidente;

b) Los datos personales comprometidos;

c) Las acciones correctivas realizadas de forma inmediata; y,

d) Los medios o el lugar, donde puede obtener más información al respecto.

Quienes toman decisiones sobre sistemas de información en una entidad deben impulsar acciones para crear, ejecutar y revisar permanentemente una estrategia de seguridad que permita garantizar la seguridad de los datos personales que custodia, mientras cumple al mismo tiempo con la *Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales.*

Ley 8934 de Protección de la Niñez y la Adolescencia frente al Contenido Nocivo de Internet y otros Medios Electrónicos

Los niños y los adolescentes están entre los grupos etarios más vulnerables en cuanto a seguridad informática; por su poca malicia, son muchas veces incapaces de detectar el peligro al cual están expuestos cuando navegan por Internet. Por ello, podrían acceder a sitios potencialmente dañinos o donde les solicitan información personal o de sus progenitores sin percatarse del riesgo; esto podría exponerlos a un alto grado de vulnerabilidad. En muchas ocasiones, los niños y los jóvenes asisten a locales públicos para acceder a lo que tal vez tienen prohibido ver en su casa de habitación.

La *Ley 8934 de Protección de la Niñez y la Adolescencia frente al Contenido Nocivo de Internet y otros Medios Electrónicos* tiene como objetivo proteger a este sector del acceso a la pornografía, el lenguaje obsceno, el fomento de la violencia y las agresiones, el incentivo al uso de drogas, la promoción de racismo, la xenofobia y otras formas discriminatorias; esto se debe lograr mediante el bloqueo a páginas web con este tipo de contenido. El artículo 1 de la ley dice:

> Artículo 1. Ámbito de aplicación y definiciones. Esta Ley será aplicable a los locales con acceso al público, destinados al uso público de computadoras conectadas a Internet u otras formas de comunicación en red, sea por medio de computadoras y de cualquier otro medio electrónico, que sean utilizados por personas menores de edad.

La ley establece las obligaciones de las personas propietarias y de las encargadas de administrar los establecimientos regulados, como, por ejemplo, instalar filtros; también establece la sanción de multa de uno a cuatro salarios base, según la gravedad de la falta, para quienes no las cumplan.

El Estado se compromete a facilitar el acceso a filtros y programas necesarios de forma gratuita o a bajo costo. La responsabilidad de fiscalizar, regular y controlar los requerimientos y las estipulaciones establecidos en esta ley

corresponde a la Superintendencia de Telecomunicaciones (Sutel), las municipalidades y al Ministerio de Salud. El Patronato Nacional de la Infancia, en coordinación con el Ministerio de Educación Pública, el Ministerio de Ambiente y Energía, el Ministerio de Ciencia, Tecnología y Telecomunicaciones y la Sutel, debe desarrollar campañas educativas para concienciar a padres y madres de familia y otros adultos a cargo de personas menores de edad sobre la importancia de velar por el material al cual los menores acceden, vía Internet u otro medio electrónico de comunicación.

Es de conocimiento general que los filtros no son perfectos; sin embargo, conforme ha pasado el tiempo, estos han mejorado. Es importante que los profesionales en computación e informática que tengan a su cargo instalar este tipo de software mantengan versiones actualizadas, con el objetivo de sacar provecho de sus avances. Además, los administradores de los locales con acceso al público deben establecer la política de mantener filtros actualizados y velar por el cumplimiento de la *Ley 8934 de Protección de la Niñez y la Adolescencia frente al Contenido Nocivo de Internet y otros Medios Electrónicos.*

Ley 9048 de delitos informáticos

Anteriormente, en el capítulo sobre la privacidad se mencionó 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; esta ley también es importante para el tema de seguridad.

Los artículos 217 bis, 229, 229 bis, 229 ter, 230, 231, 232, 233, 234, 235 y 236 de dicha ley tipifican, respectivamente, los delitos informáticos de estafa informática, daño agravado, daño informático, sabotaje informático, suplantación de identidad, espionaje informático,

instalación o propagación de programas informáticos maliciosos, suplantación de páginas electrónicas, facilitación del delito informático, narcotráfico y crimen organizado, y difusión de información falsa, todos los cuales amenazan la seguridad; en seguida se transcriben algunos de los artículos. El resaltado no es del original, pero tiene el objetivo de destacar que la pena es mayor cuando el delito lo comete un empleado que podría ser un profesional en computación e informática, dadas las tareas descritas en la ley. La finalidad de mencionar esto es crear conciencia de que el trabajo de dichos profesionales reviste una gran responsabilidad.

Estafa informática

Artículo 217 bis. Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, *o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos* [resaltado añadido].

Daño informático

Artículo 229 bis. Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información

contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.

Sabotaje informático

Artículo 229 ter. Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

La pena será de cuatro a ocho años de prisión cuando:

a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.

b) *La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos* [resaltado añadido].

c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.

d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.

Espionaje informático

Artículo 231. Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio.

Aunque la ley de delitos informáticos fue muy criticada, esta constituye un gran aporte, pues existe una herramienta legal para denunciar delitos que afectan la seguridad de sistemas de telecomunicaciones y bases de datos. Sin embargo, el tema de delito informático es muy complejo, pues muchas veces es cometido desde otros países, por lo cual la entidad o persona delincuente se encuentra fuera de la jurisdicción de la ley costarricense; por esta razón, son importantes los convenios de extradición entre países. Finalmente, también es difícil probar que un delito de esta clase fue cometido.

Convenio Europeo sobre la Ciberdelincuencia

E*l Convenio Europeo sobre la Ciberdelincuencia* (CEC), también conocido como el Convenio de Budapest, se firmó en noviembre de 2001. La Asamblea Legislativa de Costa Rica lo aprobó el 17 de febrero de 2017 en primer debate; se espera que pronto sea aprobado en segundo debate y se convierta en ley de la República. De esta forma, se fortalecerá la legislación costarricense para combatir el delito informático.

En el preámbulo del CEC, se menciona que "se reconocía la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional que tenga debidamente en cuenta las exigencias específicas de la lucha contra la ciberdelincuencia". Su importancia radica en ofrecer acceso a cooperación internacional y asistencia mutua en caso de ocurrir un delito informático. El CEC incluye medidas legislativas que se deben adoptar a nivel nacional, procedimientos que es necesario establecer para efectos investigativos y medidas para la cooperación internacional.

Con el aumento de eventos globales de ciberdelincuencia, como el ocurrido en mayo de 2017, en el cual miles de computadoras en 150 países resultaron afectadas con el virus WannaCry, se hace evidente que la cooperación

internacional en materia de delitos informáticos es indispensable.

Otra normativa internacional que conviene también al país que la Asamblea Legislativa ratifique es el *Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia*, firmado por la Conferencia de Ministros de Justicia de los Países Iberoamericanos. Según el artículo 1 de este convenio, su objetivo es "reforzar la cooperación mutua de las Partes para la adopción de medidas de aseguramiento y obtención de pruebas para la lucha contra la ciberdelincuencia".

Centro de Respuesta de Incidentes de Seguridad Informática

Por medio de decretos ejecutivos, el Gobierno de Costa Rica ha creado varias instancias cuyo fin es crear políticas de seguridad y de prevenir y actuar en caso de que se materialicen amenazas contra la seguridad cibernética. Específicamente, se han creado la Comisión Internet Costa Rica (2004) y la Comisión Nacional de Seguridad en Línea (decreto N.º 36274-MICIT de noviembre del 2010). La instancia creada de forma más reciente es el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) por medio del Decreto N.º 37052-MICIT (marzo del 2012). El propósito de este se explicita en el artículo 1 de este decreto:

> Artículo 1. Créase el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) con sede en las instalaciones del Ministerio de Ciencia y Tecnología, con facultades suficientes para coordinar con los poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad informática y cibernética y concretar el equipo de expertos en seguridad de las

> Tecnologías de la Información que trabajará para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales.

En el artículo 2 se especifican los objetivos a nivel nacional del CSIRT-CR, entre los que se incluyen:

1. Promover a nivel nacional la cultura de seguridad cibernética.
2. Coordinar acciones para mejorar la seguridad cibernética.
3. Fomentar la adopción de políticas públicas para alcanzar mayor eficiencia y eficacia en los recursos informáticos de las entidades públicas.
4. Promover proyectos y actividades para investigar, capacitar y difundir sobre la materia de seguridad de tecnologías de la información y la comunicación.

El ministro de Ciencia y Tecnología o su representante preside el Consejo Director del CSIRT, el cual también está formado por el ministro de la Presidencia, el ministro de Seguridad Pública, el fiscal general de la República, el ministro de Relaciones Exteriores, el ministro de Justicia y Paz y el presidente de la Academia Nacional de las Ciencias, todos los cuales pueden ser sustituidos por su representante.

La gestión administrativa y técnica del CSIRT-CR está a cargo del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT). Según la ingeniera Leidy Guillén Cordero, gerente de gobierno electrónico del MICITT, el CSIRT-CR está conformado por dos ingenieros, quienes están en constante capacitación en el tema de ciberseguridad (comunicación personal, 16 de setiembre de 2015). Además, en dicho ministerio se trabaja en la Estrategia Nacional de Ciberseguridad, en la cual se

plantearán lineamientos generales a manera de política pública, de los cuales se desprenderán acciones específicas más adelante. En su desarrollo se participa a todos los sectores del país, con el fin de cubrir de forma completa sus necesidades y preocupaciones. Además, uno de los objetivos es apoyar a cada uno de los ministerios del Poder Ejecutivo con el fin de que hayan iniciado a más tardar en el año 2018 el proceso de creación de su propio plan de ciberseguridad; esta es una de las metas establecidas por el MICITT en el Plan Nacional de Desarrollo Alberto Cañas Escalante 2014-2018.

El CSIRT-CR aspira a ser un centro en el cual se coordinen las acciones en casos de incidentes de seguridad, para agilizar así el intercambio de información entre las organizaciones que hayan sufrido este tipo de incidentes y otras organizaciones que puedan aportar información valiosa, tales como los proveedores de servicios de internet (ISP, por su nombre en inglés).

Según la ingeniera Guillén, lo ideal es que, en el futuro cercano, sectores como las instituciones de educación superior o los bancos creen sus centros de respuesta de incidentes de seguridad informática. Sin embargo, en primer lugar es necesario crear conciencia en cada uno de los sectores, principalmente, en las instituciones públicas, mediante capacitaciones, talleres y otras actividades que el CSIRT-CR organiza.

Se destacan dos puntos que la ingeniera Guillén considera importantes con respecto a la normativa nacional de ciberseguridad. El primero es la instauración de varias comisiones que, en la práctica, no han logrado su objetivo. Es conveniente modificar el decreto que creó el CSIRT-CR, con el fin de eliminarlas y establecer la rectoría en materia de gobierno electrónico y ciberseguridad en el MICITT. La segunda consideración es la necesidad de ratificar en la Asamblea Legislativa de Costa Rica el Convenio Europeo sobre la Ciberdelincuencia, conocido también como el

Convenio de Budapest. Esto es importante debido a la cooperación internacional y la asistencia mutua en caso de que ocurra un delito informático o para obtener pruebas en el extranjero, lo cual es muy importante para Costa Rica.

Responsabilidad de los bancos en situaciones de fraude electrónico

En esta sección, se analiza la responsabilidad de los bancos en las situaciones de sustracción monetaria fraudulenta de las cuentas bancarias. En Costa Rica, son varios los casos en los cuales una persona ha denunciado una entidad bancaria ante los tribunales por la sustracción de dinero de una de sus cuentas. En gran parte de los casos, los jueces han condenado a los bancos a resarcir los fondos a las cuentas de la víctima; los bancos, en primera instancia, se resisten a hacerlo y presentan ante la Sala Primera recursos de casación –con los cuales se busca anular una sentencia judicial previa–. Con ello, intentan dejar sin efecto la condena.

En muchos de los casos, el recurso de casación es declarado sin lugar y el banco no tiene más remedio que resarcir el dinero a la víctima. ¿Cuál es el razonamiento en el cual se respaldan las sentencias? Para responder esta pregunta, es necesario comprender los conceptos de responsabilidad objetiva y teoría del riesgo creado. A modo de ejemplo se toma aquí la sentencia 300-F-S1-2009 de la Sala Primera del 26 de marzo de 2009, correspondiente a un recurso de casación presentado por un banco. Se extraen distintas secciones de esta sentencia para explicar los conceptos que ayudarán a entender de dónde deriva la responsabilidad de las entidades bancarias. En primer lugar, en la sentencia se presentan las definiciones de

responsabilidad objetiva y responsabilidad subjetiva, tal como se lee en la sentencia:

> *En lo que se refiere a la responsabilidad, se pueden ubicar dos grandes vertientes, una subjetiva, en la cual se requiere la concurrencia, y consecuente demostración, del dolo o culpa por parte del autor del hecho dañoso (v.gr. el cardinal 1045 del Código Civil), y otra objetiva, que se caracteriza, en lo esencial, por prescindir de dichos elementos, siendo la imputación del daño el eje central sobre el cual se erige el deber de reparar* [resaltado añadido]. Como ejemplo de lo anterior, se encuentra el numeral 35 de la Ley de Defensa Efectiva del Consumidor, en donde el comerciante, productor o proveedor, responderá por aquellos daños derivados de los bienes transados y los servicios prestados, aún y cuando en su actuar no se detecte negligencia, imprudencia, impericia o dolo.

Por tanto, se puede ser responsable de algo sin haberlo causado; esa es justamente la responsabilidad objetiva. La misma sentencia introduce la teoría del riesgo creado, en la cual se sustenta la responsabilidad objetiva en este ejemplo. Según esta teoría, quien haga uso de algo peligroso, pueda o no generar un daño patrimonial, está en la obligación de reparar los perjuicios que genere, aun cuando no haya hecho nada ilícito. El respaldo de esto proviene de una ley que, a primera vista, parece ajena al tema de seguridad informática; se trata de la *Ley 7472 de la Promoción de la Competencia y Defensa Efectiva del Consumidor*, específicamente de su artículo 35, titulado "Régimen de responsabilidad". En la sentencia 300-F-S1-2009, este se incluye completo y entre comillas, tal como se puede leer a continuación:

> En lo que se refiere a los distintos criterios de imputación, para los efectos del presente caso, interesa la teoría del riesgo creado, la cual fue incluida, en forma expresa, en la Ley de Defensa del Consumidor. El esquema objetivo por el que se decanta la ley, así como la aplicación del criterio de imputación citado, se desprenden de la simple lectura de la norma en cuestión, la cual estipula: *"el productor, el proveedor y el comerciante deben responder, concurrentemente, e independientemente de la existencia de culpa, si el*

consumidor resulta perjudicado por razón del bien o el servicio, de informaciones inadecuadas o insuficientes sobre ellos o de su utilización y riesgos. / Solo se libera quien demuestre que ha sido ajeno al daño. / Los representantes legales de los establecimientos mercantiles o, en su caso, los encargados del negocio son responsables por los actos o los hechos propios o por los de sus dependientes o auxiliares. Los técnicos, los encargados de la elaboración y el control responden solidariamente, cuando así corresponda, por las violaciones a esta Ley en perjuicio del consumidor" [resaltado añadido].

El artículo 35 de la *Ley 7472 de la Promoción de la Competencia y Defensa Efectiva del Consumidor* establece la responsabilidad de productores, proveedores y comerciantes cuando el consumidor resulta afectado por el uso de los bienes o servicios que aquellos le brindan; una entidad bancaria es un proveedor de servicios y, por tanto, está sujeto a esta ley.

En cuanto a la carga de la prueba, es decir, a señalar quién está obligado a probar un determinado hecho, la sentencia 300-F-S1-2009 señala:

Con base en lo expuesto hasta este punto, cabe referirse al deber de demostración que le incumbe a cada una de las partes que integran la litis, cuando el objeto del proceso es la declaratoria de un deber de reparar un daño en casos como el presente. En primer término, se advierte que la parte actora se encuentra en una situación donde le resulta muy difícil o prácticamente imposible comprobar algunos de los hechos o presupuestos esenciales para su pretensión, colocándola ante una posible indefensión. Producto de lo anterior, y según lo ha indicado esta Sala con anterioridad, se redistribuye el deber de demostración entre las partes litigantes, en donde el *"onus probandi" (deber probatorio) le corresponde a quien se encuentre en mejores condiciones para aportar la prueba al proceso* [resaltado añadido] (en este sentido, se puede ver la resolución n.° 212 de las 8 horas 15 minutos del 25 de marzo de 2008). Empero, de lo anterior no debe extraerse que la víctima se encuentra exenta del deber probatorio, ya que le corresponde acreditar, en los términos dichos, el daño sufrido y el nexo de causalidad. Por su parte, corre por cuenta del accionado probar que es ajeno a la producción del daño, es decir, debe demostrar la concurrencia de alguna de las causas eximentes de

> responsabilidad, ya sea la culpa de la víctima, el hecho de un tercero o la fuerza mayor.

Por lo tanto, el banco debe probar que la sustracción de dinero es culpa de la víctima, de un tercero o de la fuerza mayor, es decir, de una causa ajena. Ejemplos de acciones en las cuales la culpa es de la víctima son: esta ha entregado sus datos de acceso a otra persona, ha perdido de vista su tarjeta de débito o crédito y esta ha sido clonada, ha realizado compras por Internet en sitios no seguros, ha utilizado servicios de transferencia electrónica sin la protección de un antivirus actualizado y no ha reportado el extravío de su tarjeta (como se cita en Centro de Información Jurídica en Línea, s. f., p. 4). La Sala Primera considera al banco en mejores condiciones para aportar la prueba. La víctima, por su parte, debe probar haber sufrido un daño y que este ha sido causado por la sustracción. Se expone aquí el concepto de la teoría del riesgo creado:

> La cual consiste en que la persona que se beneficia de una actividad o bien peligroso, para su explotación económica, representa un peligro social, por lo que debe enfrentar los daños que por su explotación ocasione, sin consideraciones de índole subjetiva, pues una actuación diligente no evita el daño (Quesada, 2008, p. 23).

En palabras más sencillas, el riesgo creado surge cuando una persona u organización obtiene beneficios de una fuente de peligro que ha creado. Un ejemplo es la responsabilidad patronal por los riesgos laborales (como se cita en el Centro de Información Jurídica en Línea, s. f., p. 2). Al respecto, otra sección de la sentencia 300-F-S1-2009 que se utiliza aquí como ejemplo señala que la responsabilidad del banco radica en la existencia de un riesgo intrínseco al negocio, es decir, un riesgo creado:

> En el mismo sentido, luego de analizado el testimonio en comentario, quedó demostrado que la plataforma informática del Banco (…) no fue vulnerada para obtener la clave y el usuario de la señora (…), aspecto sobre el cual lleva razón el recurrente, y que la seguridad con que cuenta resulta adecuada para proteger la integridad de la base de datos y la plataforma transaccional a lo interno. No obstante lo anterior, debe tomar en cuenta la entidad financiera demandada que su función esencial es la intermediación financiera, que incluye la captación de fondos provenientes del ahorro del público, concepto que lleva implícita su custodia, tanto desde el punto de vista físico, como del registro electrónico correspondiente. No cabe duda que se encuentra sometida a una ineludible obligación de garantizar la seguridad de las transacciones realizadas, ya sea en ventanilla o mediante cualquier otro medio puesto a disposición de los clientes, la cual debe abarcar, necesariamente, el uso de todos aquellos mecanismos disponibles que le permitan contar con un mayor grado de certeza en cuanto a la identificación de las personas que se encuentran facultadas para realizar transacciones electrónicas desde las cuentas. *La responsabilidad que le fue imputada al Banco se fundamenta, no en la sustracción del dinero por un tercero, sino en la existencia de un riesgo*, según lo expuesto en el considerando III, *en el funcionamiento propio del servicio que ofrece, lo que permite imputar el origen del daño al funcionamiento del servicio* [resaltado añadido]. Lo anterior, a pesar de disponer de mecanismos que permiten mayor seguridad.

Este recurso de casación fue declarado sin lugar, por lo cual el banco se vio obligado a acatar la condena que le había sido impuesta en la sentencia recurrida; esta consistía en resarcir los fondos a las cuentas de la víctima. Esta ha sido la resolución en la mayoría de los recursos de casación que han presentado los bancos. Esta jurisprudencia de la Sala Primera constituye un incentivo económico para que las entidades bancarias fortalezcan sus sistemas de seguridad, pues ellas llevan el peso de la carga de la prueba.

Quesada (2008) y el Centro de Información Jurídica en Línea (s. f.) aportan información muy detallada sobre los dos conceptos jurídicos relacionados con la responsabilidad mencionados anteriormente, a saber: la responsabilidad objetiva y la teoría del riesgo creado.

Nótese que el artículo 35 de la *Ley 7472 de la Promoción de la Competencia y Defensa Efectiva del Consumidor* es válido siempre que haya una relación de consumo, por lo cual el razonamiento de esta sentencia también podría valer para organizaciones en otros ámbitos. Por tanto, dicho artículo también debe servir de incentivo para mejorar sus medidas de seguridad a todas las empresas cuya operación incluye custodiar y administrar bienes ajenos.

El profesional en computación e informática y la seguridad

El profesional en computación e informática tiene una función sumamente importante en la garantía de la seguridad informática. Es su deber formarse en este campo según las características de su trabajo profesional, ya sea que se dedique al desarrollo de software, el diseño y la implementación de infraestructura tecnológica u otras tareas.

Es fundamental comprender que la seguridad no se debe dejar al azar; debe planificarse. Además de conocimiento técnico, se requiere de entender el contexto en el cual se desarrolla la organización, para identificar los riesgos del negocio y los de naturaleza técnica y priorizarlos, lo cual a su vez servirá para definir una estrategia de mitigación de riesgos. Se debe establecer un proceso continuo que incluye:

1. Analizar y evaluar los activos que se deben proteger para identificar sus vulnerabilidades y amenazas.
2. Identificar los riesgos asociados –probabilidad por impacto esperado–.
3. Definir las soluciones.

4. Realizar análisis de costo-beneficio para determinar la factibilidad de las medidas propuestas.
5. Crear políticas de seguridad a seguir en la organización.
6. Implementar las soluciones y políticas seleccionadas y evaluar los resultados.

La estrategia debe valorarse y corregirse periódicamente, dado que el contexto, la tecnología y las amenazas cambian de forma constante. Administrar el riesgo no es una tarea exclusiva de los profesionales en computación e informática, sino el trabajo de un equipo multidisciplinario del cual, indiscutiblemente, deben formar parte. Los dueños de los sistemas (unidades organizacionales responsables de los datos) y quienes toman decisiones en la empresa también deben participar en definir, ejecutar y evaluar la estrategia de seguridad. Además, en la entidad se deben establecer mecanismos para capacitar y comunicar dicha estrategia con el fin de que todo el personal e incluso los usuarios externos se familiaricen con ella.

Se ha hecho mucho énfasis en la seguridad de la infraestructura, pero es sabido que muchas aplicaciones de software son, actualmente, los elementos menos seguros de sistemas complejos. El software está lleno de vulnerabilidades, tanto de diseño como de implementación, las cuales son defectos de seguridad. Los ciberdelincuentes aprovechan estas y evaden, de forma relativamente fácil, las complejas medidas de seguridad establecidas para proteger la infraestructura, tales como paredes de fuego (*firewalls*), antivirus y sistemas de detección de intrusos.

Para contar con una aplicación de software segura, no es suficiente con establecer mecanismos de seguridad como control de acceso. Se requiere, además, de un proceso seguro de desarrollo de software, para el cual se deben

educar, de manera continua, analistas, programadores, diseñadores, arquitectos de software y usuarios. Sin embargo, también es menester cambiar la forma en la cual se dividen el trabajo y las responsabilidades en las organizaciones, con el fin de vencer barreras feudales internas que impiden ver que la seguridad es un aspecto global del software. Por tanto, el nivel de seguridad requerido no se puede conseguir como si de armar un rompecabezas se tratara; un proceso de pruebas y de control de calidad también es importante, aunque no lo es todo. La seguridad del software es emergente; surge de la conjunción de muchas decisiones que, tomadas de forma aislada, pueden culminar en una consecuencia no deseada.

Esta situación se hace más difícil debido a la cualidad dinámica del software. Constantemente se le hacen modificaciones, ya sea por defectos encontrados o por nuevos requerimientos del contexto –por ejemplo, necesidades de los usuarios, legislación nueva, acciones de la competencia, gustos de los clientes y avances tecnológicos–. Cualquier cambio hecho en el software, incluso uno para eliminar una vulnerabilidad, puede crear una nueva. Por tanto, incluso para realizar una modificación, se deberá seguir un proceso integral en el cual se valore su impacto en la seguridad.

No es conveniente dejar la seguridad en manos de los usuarios, debido sobre todo a su desconocimiento de la materia. Por ejemplo, la creación de palabras de acceso (*passwords*) complejas no debe ser opcional: el software debe exigirlo así. También es conveniente que una aplicación en la cual se requiere parametrizar opciones de seguridad llegue al usuario con una configuración por defecto que provea el nivel de seguridad máximo.

Con respecto al desconocimiento de los usuarios, es responsabilidad de los profesionales en computación e informática enseñar a los demás sobre seguridad y cuáles son las acciones a realizar para que cada persona

contribuya a ella. La seguridad informática es como una cadena, la cual es tan fuerte como su eslabón más débil.

La seguridad también se puede ver como una estructura en capas, es decir, como una cebolla, en la cual el bien protegido está en lo más interno; la capa más externa es el ser humano y, pese a todo el avance tecnológico, es la más importante; si falla, las demás capas, que son barreras tecnológicas, no siempre serán capaces de detener a quien quiera violentar la seguridad. La falla en el ser humano puede venir de su desconocimiento, su ingenuidad o su voluntad de provocar un daño. Las dos primeras causas son corregibles con formación, pero la tercera no. Por lo tanto, la seguridad informática también es un asunto de ética y moral; los valores de las personas son fundamentales, pues pueden evitar que alguien conscientemente saque provecho de una vulnerabilidad; la ley, en cambio, es punitiva: castiga después de que el daño está hecho. Una persona no es capaz de cambiar los valores de los demás, pero sí los propios.

El profesional en computación e informática es quien tiene el conocimiento, mas no siempre el poder, para ofrecer seguridad a los usuarios. Por esto justamente es quien debe contar con capacidad persuasiva, para convencer a quienes toman decisiones de que la seguridad no es un lujo, sino una buena inversión; son estos últimos quienes tienen la potestad de asignar los recursos financieros y humanos necesarios.

Reflexión

Si se pudiera escoger solo un tema del cual los profesionales en computación e informática sean responsables, ese sería, sin lugar a dudas, el de la seguridad, porque gran parte de la actividad humana depende de las

computadoras y las telecomunicaciones; la gente espera que estas sean seguras y confía ciegamente, sin entender, la mayoría de las veces, los riesgos a los cuales se expone.

CAPÍTULO III
PROPIEDAD INTELECTUAL DEL SOFTWARE

Nada proporciona tanto placer a un autor como el encontrar sus propios trabajos respetuosamente citados por otros doctos autores.

Benjamin Franklin

Resumen

El tema de la propiedad intelectual es complejo, pero al hablar de la protección del software, la complejidad aumenta todavía más. El avance tecnológico ha jugado una doble función. Por un lado, ha hecho más fácil y barato reproducir y distribuir el software, pero por otro, ha facilitado el desarrollo de medidas tecnológicas de protección que impidan acceder, crear y ejecutar copias ilegales de programas de computadoras. La legislación internacional respecto a derechos de propiedad intelectual es muy amplia. Costa Rica, inmersa en la economía globalizada, ha suscrito normativa internacional y ha emitido leyes, reglamentos y decretos para establecer los derechos de los dueños de la propiedad intelectual y garantizar su observancia, al establecer sanciones contra los actos considerados violaciones. Parte de toda esta normativa se aplica al software, el cual se protege en Costa Rica por medio de los derechos de autor; sin embargo, esta no es la única forma de protección para el software. En la ley se establecen excepciones que no constituyen violaciones a los derechos de autor, pero también existen vacíos que dan espacio a que sea necesaria la interpretación

para aplicarla, lo cual constituye un riesgo, principalmente para los usuarios del software. El acceso a la información y el conocimiento es un elemento fundamental para el desarrollo de una sociedad.

Introducción

Cuenta una anécdota que un joven costarricense fue a estudiar a una universidad en Estados Unidos; sus compañeros le preguntaron si sabía usar una aplicación de software y él lo afirmó. Lo interrogaron por otras aplicaciones y en todas las ocasiones su respuesta fue positiva. Sus compañeros le dijeron que él debía tener mucho dinero para saber usarlas todas; él no entendió la razón del comentario; entonces preguntó. Le respondieron que comprarlas era muy caro. Nada estaba más lejos de la realidad, pero los jóvenes estadounidenses no podían concebir como posible usar software sin pagar por él.

¿Recuerda usted cuando un amigo muy generosamente le "prestó" una aplicación de software conseguida de forma no muy legal?, ¿cuando el vendedor de su computadora portátil le facilitó un número de licencia para instalar el software X?, ¿o se acuerda de aquel compañero de trabajo quien se dedicaba furtivamente a instalar software a sus propios clientes, usando las licencias que había comprado su empleador? ¿Son legales o ilegales todas estas acciones?

El tema de este capítulo es la propiedad intelectual del software. Este es un tópico complejo y de mucha importancia, dada la globalización en que está inmersa Costa Rica, el auge del comercio internacional y la lucha de intereses en torno a la propiedad y el control de la información y el conocimiento.

Según la Organización Mundial de la Propiedad Intelectual (OMPI), "la propiedad intelectual se refiere a

creaciones de la mente, tales como invenciones, trabajos literarios y artísticos, diseños, y símbolos, nombres e imágenes usados en comercio" (Organización Mundial de la Propiedad Intelectual, s. f., p. 2). En muchos países, entre ellos Costa Rica, la propiedad intelectual se divide en dos categorías: la propiedad industrial y los derechos de autor. La primera incluye, entre otros, la protección mediante patentes por invenciones y diseños industriales. La segunda contempla los trabajos literarios, las películas, la música, los trabajos artísticos y los diseños arquitectónicos.

Las sociedades han creado los derechos de propiedad intelectual con el objetivo de permitir a los creadores o dueños de los activos protegidos beneficiarse de su trabajo o invención (Organización Mundial de la Propiedad Intelectual, s. f.). El artículo 27 de la *Declaración Universal de los Derechos Humanos* provee el derecho de beneficiarse de los intereses morales o materiales que resulten de la autoría de producciones artísticas, literarias o científicas (Organización Mundial de la Propiedad Intelectual, s. f.).

Las razones con las cuales se ha justificado promover y proteger la propiedad intelectual son varias (Organización Mundial de la Propiedad Intelectual, s. f.):

1. El progreso y el bienestar de la sociedad dependen de su capacidad para crear.
2. El amparo legal de las nuevas creaciones motiva a invertir recursos adicionales para más innovación.
3. La protección legal impulsa el crecimiento económico.

No necesariamente se debe estar de acuerdo con estas razones. Sin embargo, es importante conocer qué motivó, en sus inicios, la protección de la propiedad intelectual. En la actualidad, estos derechos son vistos por muchos como

un obstáculo para la innovación. Como lo indica Díaz (2008), con respecto a las patentes:

> No es efectivo, entonces, que mientras más se proteja la propiedad intelectual, mayor será la innovación. Siempre llegará un momento en que el beneficio social marginal a que da lugar una patente adicional comenzará a ser inferior al costo social marginal de crear un monopolio, frenar las innovaciones posteriores o impedir la difusión del progreso tecnológico (Díaz, 2008, p. 30).

La protección de la propiedad intelectual tiene una función muy importante en las relaciones de comercio internacional. Estados Unidos, a través de tratados de libre comercio, ha conseguido hacer más rígidas las reglas de esta materia en otros países. La Oficina Mundial del Comercio (OMC) también está muy interesada en este tema; según esta entidad, la existencia de grandes diferencias en cuanto al grado de protección y observancia de los derechos de propiedad intelectual causa distorsiones y obstáculos para el comercio internacional. Por este motivo, esta organización ha creado normativa internacional cuyo objetivo es estandarizar las medidas y procedimientos de protección.

Muchas creaciones de la mente son activos intangibles que las empresas y las personas valoran altamente. El software es una de ellas, como también lo es la música, pero se diferencia de esta y de otras en que “hace” algo. Esta característica, la cual ya no es sorprendente por lo familiarizadas que están las personas con él, da al software su singularidad.

El advenimiento de las tecnologías de información y comunicación redujo prácticamente por completo el costo marginal de reproducir y distribuir la información, el software y otros bienes intangibles –por ejemplo: libros y canciones– (Díaz, 2008). Esto significa que reproducir una

copia adicional tiene un costo muy bajo; por lo tanto, crear copias ilegales es muy barato.

En este capítulo se hace énfasis en el software, activo intangible. Se identifica la importancia de los activos intangibles para las empresas y se cuestiona la necesidad de proteger el software; además, se describen las distintas formas para protegerlo y se presenta la normativa vigente en Costa Rica para salvaguardar derechos de propiedad intelectual aplicable al software. Asimismo, se analizan las desventajas que causan estos derechos a los usuarios del software y se presenta el software libre como una opción para acceder, usar y modificar software sin riesgo de ser sancionado.

Importancia de los activos intangibles

En la actualidad, los activos intangibles son cada vez más valiosos para las empresas y los Gobiernos de los países están conscientes de ello. La razón es que son sumamente rentables (Wiederhold, 2014), es decir, dejan mucha ganancia a las empresas. Entre más activos intangibles participen en la producción de un bien o servicio, mayor será la ganancia de un negocio.

Las empresas en las industrias de desarrollo de software, productos electrónicos de consumo masivo y farmacéuticos, finanzas y servicios generan gran parte de sus ganancias a partir de los activos intangibles con que cuentan (Wiederhold, 2014); estos son de naturaleza muy variada. Entre ellos se incluyen el personal altamente calificado, procesos técnicos de desarrollo y manufactura, listas de clientes y distribuidores, marcas registradas, posición competitiva, prestigio, contratos exclusivos, investigación y desarrollo realizados internamente o adquiridos –por ejemplo, en forma de patentes–,

documentos de diseño, software y bases de datos (Wiederhold, 2014); todos estos forman el capital intelectual de una empresa. Por lo general, no aparecen en los registros contables pero agregan valor. Se pueden vender o ceder los derechos de uso de algunos de los activos intangibles, tales como las marcas registradas y las patentes.

Para efectos de vender o ceder, ¿cuánto vale un activo intangible? No es fácil determinarlo. No siempre existen mercados competitivos –muchos vendedores y compradores– en los cuales se pueda adquirir activos similares (Wiederhold, 2014). Por ejemplo, no es fácil valorar una aplicación de software estratégica creada a la medida por un equipo interno de desarrollo, pues será difícil saber cuál sería su precio en un mercado competitivo; tan solo se puede contabilizar el costo de haberla creado.

El tema de precios de transferencia se vuelve muy importante cuando se habla de activos intangibles. Un precio de transferencia es el precio que pactan dos entidades (empresas) vinculadas para transferir entre ellas bienes, servicios o derechos. Las entidades están vinculadas cuando comparten dueños o cuando una entidad es dueña de la otra. Si se vuelve al caso de la aplicación de software estratégica creada por el equipo de desarrollo interno, la empresa que lo produjo podría cederle los derechos de uso a una compañía vinculada, a cambio de un precio de transferencia. ¿Cómo se calcula este precio? Es muy difícil valorarlo de manera objetiva.

Por esta razón, las grandes corporaciones incrementan sus ganancias mediante cesiones y ventas de activos intangibles, o de sus derechos de uso, entre distintas entidades vinculadas, utilizando precios de transferencia que pueden ser, según convenga, exageradamente altos o bajos (Wiederhold, 2014). En un mundo globalizado, los productos no tienen nacionalidad. Las corporaciones dividen sus operaciones entre distintos países, en procura

de obtener las máximas ganancias para sus accionistas. Aprovechan las condiciones favorables presentes en cada país para instalar sus procesos de diseño, producción y distribución; para esto, toman en cuenta factores como el precio de la mano de obra, la tasa impositiva sobre las utilidades y los incentivos fiscales que da el Gobierno a aspectos como la repatriación de capitales o la investigación (Wiederhold, 2014). El precio de transferencia dependerá de todas estas variables.

Por ejemplo, si A, en el país X, y B, en el país Y, son empresas vinculadas, en X se tiene una tasa impositiva de 30 por ciento sobre las utilidades, en Y la tasa impositiva es de 15 por ciento y A le vende a B un bien, lo más conveniente para la corporación como un todo es que A le venda a B a un precio bajo, pues así A obtendrá utilidades bajas y deberá pagar menos impuestos en el país X. Efectivamente, se puede calcular cuál es el precio de transferencia generador del mínimo impuesto global (de A y B). Nótese que, además de la evasión de impuestos, un ejemplo como el descrito puede poner en desventaja a competidores de B, pues este podría vender su bien a precios más bajos, tanto en el país Y, como en el mercado internacional. Por esta razón, se podría dar competencia desleal.

Las grandes corporaciones diseñan cadenas de abastecimiento, es decir, procesos que incluyen desde la compra de la materia prima hasta la entrega del producto terminado a los clientes; dichas cadenas suelen ser complejas, pues abarcan varias empresas y países. Por ejemplo, se presenta el caso del software integrado (empotrado) en un dispositivo electrónico de función específica, usualmente conocido como *gadget*; el software se diseña en un país, se programa en otro, se ensambla un producto físico en el cual se integra el software en otro y se distribuye este producto al mundo entero desde otro país. Las empresas que realizan cada tarea podrían estar

vinculadas y se ubican, muy probablemente, en países con reglas fiscales (impuestos) diferentes.

Surgen varias preguntas. ¿A cuál de las entidades pertenecen los derechos de propiedad intelectual del software del ejemplo? Solo una de las empresas, que podría ser la casa matriz de la corporación, será inicialmente la dueña de los derechos de propiedad intelectual y tendrá la potestad de venderlos o cederlos a las empresas vinculadas. ¿Por qué puede la empresa que ensambla el producto físico utilizar el software diseñado y creado por otras? Porque se ha dado previamente una venta o una cesión de derechos de uso del software, lo cual implica un precio de transferencia pactado para sacar provecho de las condiciones que establece cada Gobierno.

Los Gobiernos están conscientes de las transferencias de bienes y servicios dadas dentro de las corporaciones y de la posible evasión fiscal que estas implican. Por ello, han emitido normativa para que las empresas paguen en cada país lo que correspondería, como si los bienes y servicios fueran transferidos entre entidades no vinculadas en un mercado competitivo. En la normativa se establecen métodos para calcular precios de transferencia razonables, basados en los precios o los márgenes de utilidad que se darían en casos de intercambio de un bien o servicio igual o similar entre dos entidades independientes. Si la autoridad fiscal de un país sospecha de que, en un caso de transferencia de un bien entre dos entidades vinculadas, se usó un precio de transferencia que le afecta negativamente, puede establecer uno que considere razonable para calcular el monto de impuestos a pagar, en lugar de usar los datos provistos por las empresas involucradas. En el caso de Costa Rica, está en vigencia el *Decreto N.º 37898-H Disposiciones sobre Precios de Transferencia.*

A pesar de la existencia de normativa, para las autoridades fiscales es difícil establecer precios de transferencia razonables para los activos intangibles,

porque no existen mercados competitivos con los cuales se pueda hacer la comparación para bienes o servicios iguales o similares. Por tanto, la normativa es poco efectiva en estos casos, lo cual puede resultar en grandes ganancias para las empresas. Proteger legalmente los activos intangibles garantiza a sus dueños los ingresos necesarios para funcionar y crecer, pues les permite amortizar, es decir, distribuir en el tiempo, el costo inicial de los activos intangibles (Wiederhold, 2014).

Existen diferentes instrumentos para proteger los derechos de propiedad intelectual de aquellos activos intangibles que pueden ser objeto de protección. La normativa internacional ha estandarizado los instrumentos disponibles para esta causa; entre ellos se encuentran los derechos de autor, las patentes y las marcas. En el caso particular de Costa Rica, el Registro Nacional, dependiente del Ministerio de Justicia y Paz, es el ente gubernamental autorizado para inscribir derechos sobre propiedad intelectual. Además, a nivel internacional existe la Organización Mundial de la Propiedad Intelectual (OMPI), organismo de las Naciones Unidas encargado de promover la protección de dichos derechos, a la cual Costa Rica está adscrita desde 1981.

Derechos de autor y patentes de invención

Los derechos de autor y las patentes son parte de los instrumentos que ofrece la legislación en distintos países para proteger la propiedad intelectual. Los derechos de autor surgieron para proteger obras literarias, pero posteriormente se ampliaron a obras artísticas; las patentes de invención se crearon para proteger procesos industriales y máquinas recién inventadas.

La protección que da el derecho de autor es muy distinta de la brindada por una patente de invención, aunque ambas tienen en común ofrecer al creador un derecho económico. El derecho de autor, el cual se obtiene automáticamente con el hecho de que una persona cree un trabajo literario, prohíbe a otros copiarlo.

En el derecho de autor se habla de derecho moral y derecho patrimonial. En principio, quien escribe o crea una obra inicialmente será dueño de ambos derechos. El derecho moral es perpetuo, inalienable e irrenunciable y se refiere a que el autor siempre poseerá la paternidad de su obra y tiene el derecho a la integridad de esta, es decir, que no puede ser cambiada, deformada o mutilada sin permiso expreso del autor. El derecho patrimonial permite explotar económicamente la obra. No existe una sola forma de utilizarla o explotarla; dos ejemplos son el de difusión y el de ejecución. El autor puede transferir un derecho patrimonial específico a un tercero, por ejemplo, una casa editorial; esta solo podrá hacer lo explícitamente indicado en la cesión del derecho. El derecho patrimonial es, además, heredable.

Una patente de invención, a diferencia del derecho de autor, no se adquiere automáticamente con el desarrollo de una invención. Es necesario presentar una solicitud para conseguir la patente en la entidad que el Gobierno de cada país ha creado para ello.

Pese a lo contradictorio que pueda parecer actualmente, el objetivo original de las patentes era estimular la creatividad en dos sentidos, los cuales se explican seguidamente. Primero, quien desea patentar su invención, debe brindar información detallada sobre el diseño de su creación. Dicha información es pública y otras personas pueden consultarla, con lo cual pueden tomar ideas para generar mejores invenciones; esto beneficia a la sociedad como un todo. En segundo lugar, se garantiza a los creadores de la invención protegida la posibilidad de

obtener un incentivo económico como producto de su creación, aunque una patente no garantiza que su dueño lucre con su invención, pues esta puede ser un fracaso comercial. En principio, permitir el lucro no es el fin de las patentes.

Para que una invención sea patentable, debe reunir algunos requisitos especificados en la normativa legal correspondiente de cada país. Ser novedosa, es decir, agregar algo al estado de la tecnología en el momento en que se presenta la solicitud, es imprescindible. Dicha novedad no se limita a nivel nacional, sino que debe ser a nivel mundial.

Una patente garantiza un monopolio de explotación comercial en el país en el cual es registrada, pero registrarla tiene un costo. Es crucial patentar una invención en los países en los cuales se comercializará y en los cuales se producirá o será utilizada.

Necesidad de protección legal del software

El ciclo de vida de los productos como el software es cada vez más corto. Esto significa que es más frecuente la aparición de nuevas versiones y aplicaciones similares. Este aspecto afecta a los desarrolladores de software que quieren lucrar con su creación, pues tienen poco tiempo para recuperar lo invertido. Aparte de esto, el costo de producir la primera copia de una aplicación de software, como sucede con otros bienes de información, tales como libros, películas y canciones, es alto. Sin embargo, el costo de las copias adicionales es casi nulo, pues se limita al del medio en el cual se reproducen, aunque disminuye a cero cuando lo único necesario es “bajar” una copia de Internet; crear copias ilegales es, por tanto, barato y fácil. Se puede afirmar

que el valor del software es mayor que el del medio en el cual se reproduce (Baase, 2012). Por este motivo, la protección de la propiedad intelectual del software se ha vuelto un tema importante y conflictivo.

Cuando se piensa en proteger la propiedad intelectual, se espera un cierto grado de invención y de originalidad. ¿Cuánto grado de originalidad hay en una "nueva" aplicación de software? Es difícil decirlo, pues muchas veces lo que hace un desarrollador es tomar partes de algoritmos y aplicaciones creados anteriormente por él mismo o por terceros. Se podría pensar que la originalidad está en la forma de combinar los elementos.

¿Es realmente necesaria la protección legal del software? La respuesta no es única. Algunos la consideran necesaria con el fin de mantener el estímulo para crear nuevas aplicaciones. Se parte de la certeza de que las computadoras y el software son elementos fundamentales en la vida actual; el software ofrece muchos beneficios a la sociedad, en campos tan diversos como las comunicaciones, la salud, el comercio, el transporte o la educación. Por tanto, si el software no se protegiera y cualquiera pudiera copiarlo y usarlo sin riesgo de sanción alguna; entonces se reducirían los ingresos de sus desarrolladores y habría un declive en su industria. Esto resultaría en menos productos disponibles, lo cual se traduciría en menos beneficios para la sociedad.

Sin embargo, aunque algunos estén de acuerdo con que la necesidad de proteger el software, existen dudas acerca de si extender los mecanismos de protección para derechos de autor y patentes al ámbito del software es apropiado. Se ha planteado la necesidad y conveniencia de un sistema de protección *sui generis*, es decir, específico, para el software, pero todavía no se ha creado (Hess, 2004).

Una posición muy distinta es la de quienes opinan que no hace falta proteger legalmente el software, pues el dinero no es, en la actualidad, el único incentivo para desarrollarlo.

Existen motivaciones no económicas; por ejemplo, muchos desarrolladores crean software para resolver una necesidad personal y posteriormente lo comparten con el público; otros dedican su tiempo libre al desarrollo de software porque los motiva el reconocimiento público.

La corriente del software libre y el código abierto se ha fortalecido. Este movimiento se encuadra dentro de la inteligencia colectiva, una tendencia a nivel mundial facilitada por las tecnologías de información y comunicación, la cual consiste en construir colectivamente algo en beneficio de un grupo (Reig, 2012). Lo más importante de esto es que, con la colaboración voluntaria de muchas personas que no se apegan a una organización jerárquica formal, se han creado productos de muy alta calidad.

Aunque la motivación original no fuese obtener dinero, es posible lograrlo sin necesidad de cobrar por el software ni protegerlo. Existe la alternativa de ofrecer sin costo el producto, el cual incluso los usuarios pueden modificar, pero cobrar por servicios como capacitación o asesoría. También se sabe que algunas iniciativas de desarrollo de software reciben donaciones voluntarias de los usuarios.

Pese a que el debate sobre si es necesaria la protección legal del software no ha llegado a una única respuesta, lo cierto es que existen múltiples formas de protegerlo, tal como se verá seguidamente.

Formas de protección del software

Existen varias formas de proteger el software. A saber:

1. Derechos de autor
2. Patentes de invención

3. Reserva del código fuente
4. Medidas tecnológicas de protección
5. Contratos privados

En las siguientes subsecciones se describen las características de cada una de estas formas de protección de software.

Derechos de autor

El derecho de autor es la forma más extendida de protección del software. En 1980, Estados Unidos acordó proteger el software mediante derechos de autor. Una década después, hizo lo mismo la Unión Europea. A partir de 1994, tras el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, la medida de protección se extendió a nivel mundial.

La protección por medio de derechos de autor es considerada insuficiente, pues solo se protege la expresión (el código fuente y el objeto), pero no las ideas. Además, por medio de ingeniería reversa, es posible identificar elementos que no son parte de la expresión, tales como los componentes y la arquitectura. La legislación de distintos países considera excepciones en este ámbito, las cuales permiten crear copias legales para fines no lucrativos, tales como didácticos o de investigación. El derecho de autor sobre software es un activo intangible y, por tanto, parte del capital intelectual.

Patentes de invención

La patente de invención es la forma de proteger el software que más debate genera. En cuanto a esta medida de protección, se tiene que, en general, en la normativa se

consideran dos categorías de software: el integrado en un aparato, también llamado empotrado o embebido, y el aislado. Ejemplo de software integrado en un aparato podría ser el que se utiliza en un dispositivo para escuchar música, un horno de microondas o un medidor de la presión arterial; es común en la actualidad interactuar con dispositivos con software empotrado. Por su parte, el software aislado simplemente se ejecuta en una computadora de uso general, aunque este último concepto es, en la actualidad, más amplio que en el pasado, pues se puede considerar un teléfono inteligente como una computadora de uso general.

Dado que la protección que brindan los derechos de autor se considera insuficiente para el caso del software, Estados Unidos permite otorgar patentes al software, ya sea empotrado o aislado. En Europa y América Latina, se puede otorgar patente al software empotrado (Díaz, 2008), pero en Europa se acepta dicha patente solo si con el aparato se resuelven problemas técnicos o que tengan relación con procesos físicos (Díaz, 2008).

Parece que, para diferenciar entre ambos tipos de software, se usa un concepto muy limitado de computadora. Predomina la idea de que el software aislado se ejecuta en un dispositivo con una pantalla, memoria, un teclado y un ratón; se piensa en una computadora de escritorio o portátil, por ejemplo. Actualmente se sabe que lo indispensable en una computadora es la unidad central de procesamiento (UCP) y la memoria; los dispositivos de entrada y salida para usuarios humanos, como el teclado físico y la pantalla, no son requisitos para llamarle computadora a un dispositivo.

Una computadora, en efecto, requerirá dispositivos de entrada y de salida, pero estos pueden ser, respectivamente, sensores y actuadores, los cuales no requieren de la intervención humana. Un ejemplo podría verse en un sistema de control automático del nivel del agua en una

represa; los sensores reportarán el nivel del agua a la aplicación de software ejecutada en la UCP, y la misma aplicación enviará instrucciones a los actuadores para abrir o cerrar las compuertas, según los datos que haya recibido de los sensores.

Como puede notarse, cualquiera de las dos categorías de software se ejecutará en una UCP, la cual contiene la unidad de control (UC) y la unidad aritmético-lógica (UAL). La UC es la encargada de controlar el ciclo de máquina es decir, el proceso de recuperar de la memoria (*fetch*), decodificar y enviar a ejecutar las instrucciones del software. La UAL se encarga de ejecutar las instrucciones en los circuitos que tiene especialmente para ello.

Un detalle más es que la misma versión de una aplicación de software podría ejecutarse en una computadora de uso general (software aislado) o integrado en un aparato (software empotrado); sin embargo, este último tipo de software puede patentarse en algunos países, pero el aislado no. Realmente lo que no parece tener sentido es hablar de software aislado, puesto que sin UCP ni memoria, el software es completamente inútil.

Por último, es importante destacar que una patente, así como el derecho de autor, es un activo intangible y, por tanto, parte del capital intelectual.

Reserva del código fuente

La reserva parcial o de la totalidad del código fuente, es decir, mantenerlo en secreto, fue por mucho tiempo la única forma de proteger el software. Al que recibe esta forma de protección se le conoce como software propietario.

Aunque un desarrollador proteja su aplicación de software mediante derechos de autor o de patentes, no está obligado a revelar su código fuente. Sin embargo, existen

herramientas para realizar ingeniería inversa que pueden revelar el código fuente, aunque los desarrolladores de software también trabajan en dificultar esta tarea.

Para que el código fuente goce de protección legal, son necesarias dos condiciones: el código debe otorgar una ventaja competitiva al propietario de los derechos de propiedad intelectual y este debe haber hecho el esfuerzo necesario para mantener el código en reserva. El código fuente reservado es parte del capital intelectual de una empresa.

Medidas tecnológicas de protección

Las medidas tecnológicas de protección (MTP) son consideradas instrumentos para administrar los derechos digitales (Baase, 2012); esto significa que se usan para limitar el acceso y el uso dado a productos en formato digital protegidos.

En el pasado, era común que las aplicaciones de software vinieran acompañadas por MTP visibles para el usuario, cuyo propósito era impedir la copia ilegal (Baase, 2012). Ejemplos de esto son la protección anticopia en disquetes o los dispositivos físicos que debían conectarse en un puerto físico de la computadora para poder ejecutar el software. Sin embargo, dichas medidas se volvieron obsoletas o inútiles, pues no eran completamente efectivas y terminaban siendo violentadas; además, por ser tan evidentes, los usuarios de las aplicaciones las rechazaban. Por este motivo, se abandonaron muchas de estas medidas tecnológicas de protección y, por un tiempo, las empresas productoras de software prefirieron optar por forzar el cumplimiento de la ley mediante campañas contra vendedores de copias ilegales y el establecimiento de la Business Software Alliance, también llamada la “policía del software” (Baase, 2012).

Con el tiempo, han surgido MTP más eficaces, algunas de las cuales incluso pueden estar ocultas al usuario (Díaz, 2008); por esta razón, los desarrolladores de software en la actualidad recurren cada vez más a ellas. Ejemplos de algunas medidas actualmente usadas son el uso de contraseñas de acceso, el cifrado, los límites temporales de uso y las restricciones a la reproducción. Algunas de las MTP usadas en el software podrían limitar la competencia y violentar los derechos de los consumidores (Díaz, 2008).

En 1998, se aprobó en Estados Unidos la *Ley sobre Derechos de Autor en el Milenio Digital (Digital Millennium Copyright Act)*, en la cual uno de los aspectos más fuertes es la sanción por evadir las MTP, aún cuando el producto cuyas MTP se violenten no esté protegido por derechos de autor (Baase, 2012; Díaz, 2008). Esta ley causó gran controversia en Estados Unidos, pues se corre el riesgo de criminalizar actos que no violentan los derechos de autor.

Las MTP han tomado mucha fuerza en los últimos años en América Latina debido a los tratados de libre comercio firmados entre Estados Unidos y este subcontinente. Por medio de esos acuerdos internacionales, dicho país logró incorporar todas las disposiciones de su ley relacionadas con las MTP en la normativa de los demás países (Díaz, 2008). Con ello se corre el riesgo de que las excepciones definidas en los mismos tratados y otra normativa no puedan hacerse efectivas.

Contratos privados

Las licencias de software son un ejemplo de contrato privado, por medio del cual el dueño de los derechos de propiedad intelectual de una aplicación de software, llamado el licenciante, le da permiso de uso a un tercero, el licenciatario, en algunos casos por un plazo determinado; una vez transcurrido ese plazo, el uso del software se vuelve ilegal. Dado que una licencia no implica transferir los

derechos de autor, generalmente, en el contrato se prohíbe la distribución, la venta de copias y la ingeniería reversa (Díaz, 2008). En algunos casos, incluso se obliga al usuario a renunciar a su derecho de ejercer las excepciones a los derechos de autor mencionadas en la normativa, tal como sacar una copia de respaldo del software.

Por ser contratos de adhesión, es decir, que el comprador no tiene opción de negociar ni de cambiar ninguna cláusula, están sesgados totalmente a favor del propietario de los derechos. Por lo tanto, los contratos privados resultan más limitantes que la normativa internacional y nacional, pero se amparan en las leyes de comercio de cada país (Díaz, 2008).

Los contratos privados de licenciamiento se han convertido en una fuente de ingresos muy importante para muchas empresas; para esto, el contrato de licenciamiento se complementa con otro tipo de contrato privado, uno de mantenimiento del software. Este incluye la actualización de nuevas versiones y servicios de apoyo técnico en caso de que el usuario tenga problemas técnicos. De esta forma, el desarrollador no solo se asegura de recibir, por adelantado, ingresos por las mejoras realizadas en sus productos durante la duración del contrato, sino que dispone de más tiempo para amortizar el costo inicial de crear el software.

En algunos casos, si a un usuario se le vence un contrato de mantenimiento y no lo renueva, en el momento de requerir apoyo técnico, se verá obligado a pagar por todo el tiempo durante el cual suspendió el pago, a pesar de no haber recibido actualizaciones ni servicio. Es importante agregar que los contratos privados no son una garantía de respeto a los derechos de propiedad intelectual, especialmente para las aplicaciones de uso masivo (Díaz, 2008).

Situación en Costa Rica

A finales del siglo XX, se estableció en Costa Rica la Business Software Alliance (BSA), organización internacional dedicada a proteger los intereses de los fabricantes de software en todo el mundo (Business Software Alliance, s. f.). La BSA, conocida también como la "policía del software", agrupó en Costa Rica empresas transnacionales, las cuales estaban entonces recientemente establecidas en el país, y desarrolladoras de software de capital costarricense.

Antes de la instauración de la BSA, era muy común que abiertamente los vendedores de microcomputadoras ofrecieran a sus compradores el software por kilos (kilobytes). Ensamblaban los equipos y les instalaban todas las aplicaciones de software que el comprador estuviera dispuesto a pagar, sin costo por licencias de uso.

Por gestiones realizadas por la BSA, se dieron algunos allanamientos en los cuales se confiscaron las computadoras de algunas empresas. Ante el daño tan grave a la imagen de una empresa que podían causar un allanamiento y la imposibilidad de operar, paulatinamente, mayor cantidad de empresas establecieron acuerdos de pago con los productores de software.

Además, Costa Rica suscribió varios convenios internacionales y emitió normativa nacional para fortalecer la protección a la propiedad intelectual. Desde entonces, la piratería de software no desapareció completamente, pero existen recursos jurídicos para sancionarla.

Las instituciones gubernamentales y estatales de Costa Rica, ante la gran cantidad de computadoras con las cuales contaban y el altísimo monto que deberían pagar periódicamente por las licencias de uso, utilizaban software ilegal. Sin embargo, los Gobiernos no están exentos de la normativa ni de las diligencias de la BSA, por lo cual, a

finales del 2001, se empezó a regularizar la situación del software en el Gobierno Central, con el objetivo de observar los derechos de propiedad intelectual (Escoto, s. f.).

La violación de los derechos de propiedad intelectual no ha desaparecido de forma absoluta en Costa Rica, pues es imposible garantizar su respeto, máxime dado el constante avance de la tecnología. Sin embargo, el negocio de la venta de software por kilos no se anuncia abiertamente; muchas empresas decidieron apegarse a la ley, pero es muy probable que las personas instalen software ilegal en sus computadoras de uso personal.

Aparte de eso, los desarrolladores de software han optado por poner obstáculos a los usuarios para limitar las copias ilegales de software; al mismo tiempo han tomado acciones para incentivar el uso de copias legales, por ejemplo, al ofrecer versiones gratuitas de sus productos, con funcionalidad limitada, aunque la versión completa sea de pago. Shapiro y Varian (1999) se refieren a una categoría de productos, a la cual pertenece el software, denominada bienes de información, los cuales son, a su vez, bienes de experiencia. Esto significa que el usuario debe experimentar con ellos para valorarlos; las versiones limitadas permiten esta experiencia, lo que disminuye el riesgo de los usuarios de pagar por una aplicación de software que no se ajusta a sus necesidades o que finalmente no les gusta.

Protección legal del software en Costa Rica

La normativa legal costarricense relacionada con la protección de la propiedad intelectual es muy amplia; sin embargo, se enfatizará aquí en la relacionada con la

protección del software. Dada la gran importancia económica que tiene la industria de desarrollo de software en Costa Rica, la protección de este producto genera un interés especial en este país. Se hará, en primera instancia, referencia al artículo 47 de la Constitución Política de Costa Rica, el cual garantiza el derecho de proteger la propiedad intelectual y señala lo siguiente:

> Artículo 47. Todo autor, inventor, productor o comerciante gozará temporalmente de la propiedad exclusiva de su obra, invención, marca, nombre comercial, con arreglo a la ley.

La protección del software se ampara en el artículo citado anteriormente. El marco regulatorio en esta materia vigente en Costa Rica está formado tanto por convenios internacionales ratificados por Costa Rica como por normativa nacional –leyes, reglamentos y decretos–. Es importante destacar que parte de esta última ha sido adoptada para cumplir con los compromisos adquiridos en los convenios internacionales. Por eso, no es extraño encontrar copias textuales de estos en la normativa nacional.

En Costa Rica, al igual que en la mayoría de los países, el software se puede proteger con el mecanismo de derecho de autor, pues esto equivale a equiparlo con una obra artística, categoría en la cual se incluyen las obras literarias, las esculturas, las pinturas y las obras musicales. Sin embargo, a diferencia de una obra literaria, en la cual toda esta se hace pública, en el caso del software se puede reservar el código fuente. En otros países, tal como en Estados Unidos, el software se considera una invención patentable.

La normativa internacional sobre derechos de autor incluye el Convenio de Berna para la Protección de Obras Literarias y Artísticas –*Ley 6083 Adhesión a la Convención para la Protección de Obras Literarias y Artísticas,* del 29 de

agosto de 1977–, el Acuerdo sobre Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio –ADPIC, Anexo 1C aprobado por la *Ley 7475 Aprobación del Acta Final en que se incorporan los Resultados de la Ronda Uruguay de Negociaciones Comerciales Multilaterales*, del 20 de diciembre de 1994–, los tratados de libre comercio, tales como los de Costa Rica-México y República Dominicana-Centroamérica-Estados Unidos, y el Tratado de la OMPI sobre Derechos de Autor –*Ley 7968 Aprobación del Tratado de la OMPI sobre Derechos de Autor (WCT) 1996*, del 16 de diciembre de 1999–. A nivel mundial, las reglas sobre propiedad intelectual se han globalizado, como producto de la normativa internacional (Díaz, 2008).

La normativa nacional comprende la *Ley 6683 de Derechos de Autor y Derechos Conexos* –reformada mediante la Ley 6935 del 14 de diciembre de 1983, la Ley 7397 del 3 de mayo de 1994, la Ley 7979 del 6 de enero de 2000, la Ley 8686 del 21 de noviembre de 2008 y la Ley 8834 del 3 de mayo de 2010–, la *Ley 8039 de Procedimientos de Observancia de los Derechos de Propiedad Intelectual* –del 12 de octubre de 2002–, el *Reglamento Ejecutivo 24611-J a la Ley de Derechos de Autor y Derechos Conexos* y el *Decreto 37549-JP Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central.*

En Costa Rica, el derecho moral es perpetuo, mientras que el patrimonial está protegido por toda la vida del autor y por 70 años después de su muerte; solo entonces la obra pasa a ser de dominio público.

En las siguientes subsecciones se retoma la normativa internacional y nacional relacionada con el tema de protección de la propiedad intelectual del software. Se presenta por orden cronológico, para hacer notoria la evolución que se ha dado. Además, en algunos casos, una ley nacional ha surgido como consecuencia de un compromiso adquirido en un convenio internacional. El objetivo es dar una idea clara de la importancia que ha

adquirido el tema de propiedad intelectual y de la complejidad de este.

Convenio de Berna para la Protección de Obras Literarias y Artísticas

El Convenio de Berna para la Protección de Obras Literarias y Artísticas está vigente en Costa Rica desde 1977; este se concluyó en 1886 y es el más antiguo en materia de derechos de autor. Con él se buscaba que el derecho de autor estuviera protegido tanto a nivel de legislación nacional como internacional (Organización Mundial de la Propiedad Intelectual, 1978).

Si bien en el Convenio de Berna para la Protección de Obras Literarias y Artísticas no se hace mención al software, pues este no existía cuando fue escrito, el convenio sí es muy importante, pues se establece que las obras protegidas lo estarán en todos los países que lo suscriban, lo cual beneficia al autor y a sus derechohabientes. En este convenio se definen varios principios, como el de trato nacional –igual trato para nacionales y extranjeros– y el de protección automática –no es necesario cumplir un requisito formal para obtener la protección– (Organización Mundial de la Propiedad Intelectual, 1978); establece, además, los conceptos de derecho moral y patrimonial.

A partir del Convenio de Berna para la Protección de Obras Literarias y Artísticas, tanto la normativa internacional como la legislación nacional han evolucionado, con el objetivo de establecer condiciones mínimas de protección bajo el concepto de derechos de autor (Programa Sociedad de la Información y el Conocimiento, 2006).

Ley 6683 de Derechos de Autor y Derechos Conexos y su reglamento

La *Ley 6683 de Derechos de Autor y Derechos Conexos* se encuentra en vigencia desde 1982 y fue reformada en varias ocasiones, por última vez por la Ley 8834 del 3 de mayo de 2010; esta es la primera normativa nacional analizada en este libro. Se hará énfasis en los derechos de autor, pues los derechos conexos mencionados en el título de la ley no tienen sentido en el contexto del software, ya que recaen sobre artistas, intérpretes, ejecutantes, productores de fonogramas y organismos de radiodifusión.

En el título I, capítulo I, artículo 1 de la ley, explícitamente se menciona que los programas de cómputo, es decir, el software, están protegidos por derechos de autor. A saber:

> Artículo 1. Las producciones intelectuales originales confieren a sus autores los derechos referidos en esta Ley. La protección del derecho de autor abarcará las expresiones, pero no las ideas, los procedimientos, los métodos de operación ni los conceptos matemáticos en sí. Los autores son los titulares de los derechos patrimoniales y morales sobre sus obras literarias o artísticas.
>
> Por "obras literarias y artísticas", en adelante "obras", deben entenderse todas las producciones en los campos literario, científico y artístico, cualquiera que sea la forma de expresión, tales como: libros, folletos, cartas y otros escritos; además, *los programas de cómputo* [resaltado añadido] dentro de los cuales se incluyen sus versiones sucesivas y los programas derivados (...).

La definición de programa de cómputo utilizada en la ley de derechos de autor se encuentra en el artículo 4 e indica lo siguiente:

> Artículo 4. Para los efectos de esta Ley se entiende por:

ñ) Programa de cómputo: conjunto de instrucciones expresadas mediante palabras, códigos, gráficos, diseño o en cualquier otra forma que, al ser incorporados en un dispositivo de lectura automatizada, es capaz de hacer que una computadora –un aparato electrónico o similar capaz de elaborar informaciones– ejecute determinada tarea u obtenga determinado resultado. También, forman parte del programa su documentación técnica y sus manuales de uso.

El artículo 74 de la misma ley indica explícitamente que la reproducción de software para el uso propio, aun sin ánimo de lucro, no está permitida, pese a estarlo para obras didácticas y científicas.

Artículo 74. También es libre la reproducción de una obra didáctica o científica, efectuada personal y exclusivamente por el interesado para su propio uso y sin ánimo de lucro directo o indirecto. Esa reproducción deberá realizarse en un solo ejemplar, mecanografiado o manuscrito. *Esta disposición no se aplicará a los programas de computación* [resaltado añadido] (Así reformado por el artículo 1° de la ley N.° 7397 de 3 de mayo de 1994)

La ley de derechos de autor también contempla la inscripción de bases de datos, con las cuales trabajan conjuntamente muchas aplicaciones de software, como es posible verificar en sus artículos 8, 9 e inciso 6 del 103, los cuales se transcriben a continuación.

Artículo 8. Quien adapte, traduzca, modifique, refunda, compendie, parodie o extracte, de cualquier manera, la sustancia de una obra de dominio público, es el titular exclusivo de su propio trabajo; pero no podrá oponerse a que otros hagan lo mismo con esa obra de dominio público. Si esos actos se realizan con obras o producciones que estén en el dominio privado, será necesaria la autorización del titular del derecho. *Las bases de datos están protegidas como compilaciones* [resaltado añadido]. (Así reformado por el artículo 1° de la ley *N.° 7397 de 3 de mayo de 1994)*

Artículo 9. Los derechos de autor en compilaciones de obras pertenecen a su compilador. (Así reformado por el artículo 1° de la ley N.° 8686 del 21 de noviembre de 2008)

Artículo 103. Para inscribir una producción, el interesado presentará, ante el registrador, una solicitud escrita con los siguientes requisitos:

6) Cuando se trate de inscribir un programa de cómputo o una base de datos, la solicitud contendrá la descripción del programa o la base de datos, así como su material auxiliar.

La ley de derechos de autor está relacionada con el *Decreto N.º 24611-J Reglamento a la Ley de Derechos de Autor y Derechos Conexos* y el *Decreto N.º 34904-J Modificaciones al Reglamento a la Ley de Derechos de Autor y Derechos Conexos.* El decreto N.º 24611-J dedica el capítulo I del título III al software, tal como se muestra a continuación:

TÍTULO III

Disposiciones especiales para ciertas obras

CAPÍTULO I Programas de Cómputo

Artículo 6. Se presume, salvo prueba en contrario, que es productor del programa de cómputo, la persona natural o jurídica que publique la obra bajo su responsabilidad o que aparezca indicada como tal en la misma de la manera acostumbrada.

Artículo 7. Salvo en los casos en que se trate de una obra individual, o que haya sido publicada con el nombre de los autores, se presume, salvo prueba en contrario, que el programa de cómputo es una obra colectiva, cuya titularidad corresponde, en los términos del artículo 6º de la Ley, al productor, quien además de los derechos de orden patrimonial, tiene la facultad de defender al derecho moral, en la medida que ello sea necesario para la explotación de la obra.

Artículo 8. Salvo cuando se trate de una obra individual, o publicada bajo el nombre de sus autores, el derecho sobre el programa de cómputo se extingue, en los términos del artículo 60 de la Ley, a los cincuenta años de su primera publicación, contados, de acuerdo al artículo 65, a partir del 31 de diciembre del año en que se dio inicio a dicha publicación.

> Artículo 9. A menos que el contrato de enajenación del soporte material que contiene el programa de cómputo o la licencia de uso expedida por el titular del derecho, disponga otra cosa, es permitida al adquirente o licenciatario, según los casos, la reproducción de una sola copia de la obra, exclusivamente con fines de resguardo o seguridad, así como la introducción del programa en la memoria interna del equipo, a los únicos efectos de su utilización por el usuario.
>
> Artículo 10. No constituye modificación de la obra, la adaptación de un programa de cómputo realizada por el propio usuario del ejemplar legítimo y para su utilización exclusivamente personal, salvo que se contemple otra cosa en el contrato de enajenación de dicho soporte material o en la licencia de uso expedida por el titular del derecho sobre la obra.

Es importante destacar los siguientes aspectos sobre los artículos anteriores:

1. El artículo 7 indica que el software es, en general, una obra colectiva. Dada la complejidad que han alcanzado las aplicaciones de software, es imposible para una sola persona crearlas; a pesar de ser colectiva, la dueña de los derechos patrimoniales puede ser una persona jurídica.
2. El artículo 9 señala como permitido tener una copia del software como respaldo, siempre y cuando el productor lo permita.
3. La legislación, lamentablemente, no avanza al mismo ritmo que la tecnología. Por tanto, pronto se vuelve obsoleta, pues los términos utilizados en ella ya no se emplean en el contexto actual. Por ejemplo, en el artículo 9 se menciona el soporte material; esto se refería, en el pasado, al disquete o el disco compacto en el cual se recibía el software. En la actualidad, muchas aplicaciones se descargan de Internet. Además, en la nube (*cloud computing*) han surgido esquemas, como el de “software como un servicio”,

más conocido como *software as a service* (SaaS). En la nube, la persona u organización cliente no recibe copia de la aplicación utilizada, sino que esta se hospeda en un servidor, propio o de terceros, al cual se accede mediante Internet. Bajo estos esquemas, la persona u organización cliente no tiene posibilidad de modificar la aplicación de software ni de sacarle copia.

4. En el artículo 10 se habla de la adaptación de un programa de cómputo, sin aclarar qué significa esto. Es posible entender por adaptación modificar el código fuente, pero podría tener otro significado.

El artículo 40 de la *Ley 6683 de Derechos de Autor y Derechos Conexos* resuelve una pregunta frecuente: ¿a quién pertenecen los derechos del software hecho por una persona empleada durante una relación laboral? Este artículo califica claramente al empleador como el dueño patrimonial; sin embargo, se recomienda a este incluir en el contrato de trabajo de sus empleados una cláusula expresa, en la cual estos reconozcan que los derechos patrimoniales del software que desarrollan son del empleador. El artículo 40 establece lo siguiente:

> Artículo 40. Cuando uno o varios autores se comprometen a componer una obra, según un plan suministrado por el editor, únicamente pueden pretender los honorarios convenidos. El comitente será el titular de los derechos patrimoniales sobre la obra, pero los comisarios conservarán sobre ella sus derechos morales; asimismo, cuando el autor sea un asalariado el titular de los derechos patrimoniales será el empleador. (Así reformado por el artículo 1° de la ley N.° 7397 de 3 de mayo de 1994)

Lo anterior está respaldado por el voto número 415, del 22 de diciembre de 1994, de la Sala Segunda de la Corte Suprema de Justicia, el cual hace una analogía de este caso con el de la obra por encargo. El derecho moral es de la

persona que desarrolla el software, pero esto no le autoriza a impedirle el acceso al código fuente al dueño patrimonial del software, es decir, al empleador. Sin embargo, el empleado autor del software sí puede exigir al patrono consignar su autoría.

El mismo artículo 40 aclara el tema de quién es el titular de los derechos patrimoniales del software cuando una o varias personas desarrollan uno a la medida a solicitud de un cliente; si bien quienes lo desarrollan conservan los derechos morales, los patrimoniales son de quien encarga el software.

Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio

El Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, conocido como el Acuerdo sobre los ADPIC, es un convenio internacional suscrito por Costa Rica en diciembre de 1994. Este es de la Organización Mundial del Comercio (OMC) y es de acatamiento obligatorio para todos los países miembros de este organismo. Surgió con la intención de uniformar el grado de protección y observancia de los derechos de propiedad intelectual, pues existían grandes diferencias entre los países que dificultaban las relaciones comerciales internacionales (Organización Mundial del Comercio, s. f.).

El Acuerdo sobre los ADPIC define principios de no discriminación; estos son: el de trato nacional y el de nación más favorecida (Organización Mundial del Comercio, s. f.). El primero establece, en materia de protección de la propiedad intelectual, un trato igual a nacionales y extranjeros de países miembros del acuerdo. Por su parte, el segundo significa que cualquier ventaja concedida por un país miembro del acuerdo a los

nacionales de otro país se otorgará a los de todos los demás países parte del acuerdo.

El artículo 10 del acuerdo establece la protección del software como obra literaria y la de las bases de datos (compilaciones de datos) que sean creaciones de carácter intelectual, como obra intelectual. La protección no abarca los datos en sí mismos, aunque estos podrían protegerse mediante derechos de autor; esto parece indicar que lo protegido de una base de datos es su estructura. El artículo 10 se transcribe seguidamente.

> Artículo 10. Programas de ordenador y compilaciones de datos
>
> 1. Los programas de ordenador, sean programas fuente o programas objeto, serán protegidos como obras literarias en virtud del Convenio de Berna (1971).
>
> 2. Las compilaciones de datos o de otros materiales, en forma legible por máquina o en otra forma, que por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, serán protegidas como tales. Esa protección, que no abarcará los datos o materiales en sí mismos, se entenderá sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales en sí mismos.

El artículo 11 del Acuerdo sobre los ADPIC define el derecho de los dueños de los derechos de propiedad intelectual de autorizar o prohibir el arrendamiento comercial de aplicaciones de software y obras cinematográficas. Se transcribe el artículo a continuación.

> Artículo 11. Derechos de arrendamiento. Al menos respecto de los programas de ordenador y de las obras cinematográficas, los Miembros conferirán a los autores y a sus derechohabientes el derecho de autorizar o prohibir el arrendamiento comercial al público de los originales o copias de sus obras amparadas por el derecho de autor. Se exceptuará a un Miembro de esa obligación con respecto a las obras cinematográficas a menos que el arrendamiento haya dado lugar a una realización muy extendida de copias de esas obras que menoscabe en medida importante

> el derecho exclusivo de reproducción conferido en dicho Miembro a los autores y sus derechohabientes. En lo referente a los programas de ordenador, esa obligación no se aplica a los arrendamientos cuyo objeto esencial no sea el programa en sí.

Existen varias modalidades de arrendamiento, tales como el licenciamiento, en cuyo caso el dueño de los derechos patrimoniales permite a un tercero el uso del software por un tiempo determinado, además de otros derechos también limitados; el caso de servicios en la nube, como el de software como un servicio (SaaS, por su nombre en inglés), es otra modalidad de arrendamiento.

Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos

Desde 1994, Costa Rica ha firmado más de doce tratados de libre comercio y un acuerdo de asociación (Ministerio de Comercio Exterior de Costa Rica, s. f.); algunos de ellos incluyen cláusulas sobre protección de la propiedad intelectual. Por ejemplo, en el primer tratado que se firmó, el de Costa Rica-México (Ley 7474 del 23 de diciembre de 1994), ambos países asumen el compromiso de reconocer a los nacionales del otro país los derechos de propiedad intelectual previamente adquiridos. Se reconoce a los autores sus derechos para "prohibir o autorizar la edición, reproducción y comunicación al público de las obras así como la importación de copias de la obra hechas sin autorización" (Programa Sociedad de la Información y el Conocimiento, 2006, p. 54); además, se establece el software como objeto de protección.

Sin embargo, el que más debate generó con respecto a la protección de propiedad intelectual es el Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos (Ley 8622 del 21 de noviembre de 2007, en vigencia desde el 1 de enero de 2009). El capítulo 15 de este tratado,

el cual se dedica íntegramente a los derechos de propiedad intelectual, es extenso y fortalece dichos derechos mediante disposiciones que superan las del Acuerdo sobre los ADPIC en algunos aspectos. Por tanto, este se considera un tratado ADPIC-*plus*.

Uno de los aspectos que motivó a Estados Unidos a firmar varios tratados de libre comercio fue justamente impulsar el fortalecimiento de los derechos de propiedad intelectual, en especial para proteger sus propias producciones como país (Díaz, 2008). Si bien en dichos tratados no se incorporaron cambios significativos en cuanto a derechos de autor, sí se integraron disposiciones para el resguardo legal de las medidas tecnológicas de protección (MTP).

En el caso particular del Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos, el artículo 15.5, titulado "Obligaciones Pertinentes a los Derechos de Autor y Derechos Conexos", inciso 7, apartado (a) define que cada país establecerá procedimientos y sanciones penales para quienes evadan las MTP y quienes fabriquen, distribuyan, importen y ofrezcan al público herramientas para evadirlas. Asimismo, en el apartado (d) se definen las excepciones que se aplicarán a bibliotecas, archivos, entidades educativas y organismos públicos de radiodifusión no comercial sin fines de lucro. Sin embargo, al incrementarse el control privado de las copias, se pone en riesgo el cumplimiento de las excepciones y limitaciones legales de los derechos de autor (Díaz, 2008).

Además, en este tratado se incluye que el Poder Ejecutivo de cada país utilizará únicamente software autorizado, por lo cual debe emitir la normativa necesaria para regular su adquisición y la forma de administrarlo.

En el caso de que un comprador adquiera una aplicación de software de un productor estadounidense o una licencia de uso, acepta un contrato de adhesión. Si hubiera un conflicto entre productor y comprador porque el segundo actuó de manera que violenta los derechos de autor del

primero, el productor puede determinar cuál ley será la aplicable, si la estadounidense o la costarricense. El conflicto podría surgir de una acción legal en el país del comprador que no es permitida en el del productor. Esta situación es contraria al principio de territorialidad, según el cual se aplica la ley del lugar en el cual se encuentra el software, y complica la defensa del comprador.

Como consecuencia del Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos, en Costa Rica surgió nueva normativa en relación con los derechos de propiedad intelectual, como se expondrá posteriormente.

Tratado de la OMPI sobre Derechos de Autor

Por medio de la Ley 7968 del 16 de diciembre de 1999, Costa Rica se suscribió al Tratado de la OMPI sobre Derechos de Autor. Este versa sobre "la protección de obras y los derechos de sus autores en el entorno digital" (Organización Mundial de la Propiedad Intelectual, 1996, párr. 1). En el artículo 2 se delimitan los derechos de autor a las expresiones, tal como se puede verificar a continuación:

> Artículo 2. La protección del derecho de autor abarcará las expresiones pero no las ideas, procedimientos, métodos de operación o conceptos matemáticos en sí.

En este tratado se indica que el software, en cualquiera de sus formas, está protegido como obra literaria y, por tanto, es objeto de protección mediante derechos de autor. En el caso del software, la expresión se refiere a los códigos fuente y objeto. Además, se conceden a los autores tres derechos adicionales a los previamente reconocidos por el Convenio de Berna para la Protección de Obras Literarias y

Artísticas: derecho de distribución, de alquiler y de comunicación al público.

El Tratado de la OMPI sobre Derechos de Autor obliga a los países firmantes a definir recursos jurídicos para evitar neutralizar las medidas tecnológicas de protección que establezcan los autores para ejercer sus derechos.

Ley 8039 de Procedimientos de Observancia de los Derechos de Propiedad Intelectual

La *Ley 8039 de Procedimientos de Observancia de los Derechos de Propiedad Intelectual,* la cual entró en vigencia en octubre del 2000, define las acciones administrativas que el titular de un derecho de propiedad intelectual en Costa Rica puede ejercer ante el Registro Nacional y las acciones judiciales, para el caso en que una persona u organización viole su derecho; también incluye el establecimiento de sanciones. Esta ley se promulgó con el objetivo de cumplir con lo estipulado en el Acuerdo sobre los ADPIC, en lo respectivo a la parte III, titulada "Observancia de los Derechos de Propiedad Intelectual", y en el Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos.

Para el tema que interesa en este capítulo, el software, son tres los artículos de esta ley que se destacan: el 62, el 62 bis y el 63. El artículo 62 fija las sanciones para las distintas acciones encaminadas a deshabilitar las medidas tecnológicas de protección (MTP) de los derechos de autor, lo cual incluye alterar, evadir, suprimir, modificar y deteriorar las MTP. La sanción por tales acciones puede ser una multa o la prisión. Se transcribe a continuación el artículo 62.

> Artículo 62. Alteración, evasión, supresión, modificación o deterioro de las medidas tecnológicas efectivas contra la reproducción, el acceso o la

puesta a disposición del público de obras, interpretaciones o ejecuciones, o fonogramas. Será sancionado con prisión de uno a cinco años o multa de cinco a quinientos salarios base, quien, de cualquier forma, altere, evada, suprima, modifique o deteriore medidas tecnológicas efectivas de cualquier naturaleza que controlen el acceso a obras, interpretaciones o fonogramas u otra materia objeto de protección.

No se impondrán sanciones penales en las conductas indicadas, cuando estas sean realizadas por funcionarios de bibliotecas, archivos, instituciones educativas u organismos públicos de radiodifusión no comerciales sin fines de lucro, en el ejercicio de sus funciones.

Cualquier acto descrito en el primer párrafo anterior constituirá una acción civil o un delito separado, independiente de cualquier violación que pudiera ocurrir según la Ley de derechos de autor y derechos conexos.

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

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

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

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

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

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

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

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

(Así reformado por el artículo 1° aparte e) de la ley N.° 8656 de 18 de julio de 2008).

Nótese que la ingeniería inversa, conocida también como ingeniería reversa, será sancionada, excepto cuando el objetivo de realizarla sea lograr que una aplicación opere conjuntamente con otras; esta es una excepción a las MTP.

El artículo 62 bis impone sanciones para quienes fabriquen, importen, distribuyan, ofrezcan o trafiquen con productos, componentes o servicios que sirvan para evadir medidas tecnológicas instaladas para la protección de los derechos de autor.

Según el artículo 62 bis, si se usa una copia legal, la ingeniería reversa no será sancionada si el objetivo es lograr que una aplicación de software opere conjuntamente con otras, o bien, identificar y analizar fallas y vulnerabilidades

de las tecnologías para codificar y decodificar la información.

El artículo 63 penaliza alterar o suprimir, sin autorización, la información electrónica colocada por los dueños de los derechos de autor para posibilitar la gestión de sus derechos patrimoniales y morales, de modo que estos puedan perjudicarse. El concepto de gestión de derechos patrimoniales se define en el inciso b) del artículo 2 bis de la ley. Seguidamente se transcriben los artículos 2 bis b) y 63.

> Artículo 2 bis. Definiciones. Para efectos de esta Ley, se entenderá por:
>
> b) Información sobre la gestión de derechos:
>
> i) Información que identifica a la obra, la interpretación o la ejecución, o el fonograma, al autor de la obra, al artista, al intérprete o el ejecutante de la interpretación o ejecución, o al productor del fonograma, o al titular de cualquier derecho sobre la obra, interpretación o ejecución, o fonograma.
>
> ii) Información sobre los términos y las condiciones de utilización de la obra, interpretación o ejecución, o fonograma.
>
> iii) Cualquier número o código que represente dicha información.
>
> Cuando cualquiera de estos elementos esté adjunto a un ejemplar de la obra, interpretación, ejecución o fonograma o figure en relación con la comunicación o puesta a disposición de la obra al público, interpretación o ejecución o fonograma.
>
> Artículo 63. Alteración, distribución, importación, transmisión o comunicación de información sobre gestión de derechos. Será sancionado con prisión de uno a cinco años o multa de cinco a quinientos salarios base, quien sin autorización:
>
> a) Suprima o altere cualquier información sobre gestión de derechos.
>
> b) Distribuya o importe, para su distribución, información sobre gestión de derechos, sabiendo que esa información ha sido suprimida o alterada sin autorización.

c) Distribuya, importe para su distribución, transmita, comunique o ponga a disposición del público, copias de obras, interpretaciones, ejecuciones o fonogramas, sabiendo que la información sobre gestión de derechos ha sido suprimida o alterada sin autorización.

En los artículos 62, 62 bis y 63 se define como sanción la pena de prisión de uno a cinco años o multas de cinco a quinientos salarios base, según el monto del perjuicio.

En el cuadro 1 se resumen las prácticas consideradas violaciones a los derechos de propiedad intelectual aplicables al software y que son sancionables, de conformidad con la *Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual*. En términos con los cuales los especialistas en computación e informática están familiarizados, son violaciones a los derechos de autor la copia ilegal de software, la distribución sin autorización del dueño de los derechos patrimoniales y el *hackeo*, es decir, alterar o modificar el código y las MTP usadas.

Cuadro N.º 1

Resumen de las violaciones al derecho de autor del software según la *Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual*

Artículo	Violación al derecho de autor del software
51	Representar de manera pública, comunicar o poner a disposición del público, sin autorización del titular de los derechos, obras literarias o artísticas.
53	Realizar la inscripción registral de derechos de autor ajenos.
54	Reproducir sin autorización obras literarias, artísticas o fonogramas.
57	Publicar como propias obras ajenas.
58	Adaptar, traducir, modificar y compendiar, sin autorización del titular de los derechos, obras literarias o artísticas.

60	Arrendar obras literarias, artísticas o fonogramas sin autorización del autor o representante.
62	Alterar, evadir, suprimir, modificar o deteriorar las medidas tecnológicas efectivas contra la reproducción, el acceso o la puesta a disposición del público de obras, interpretaciones, ejecuciones o fonogramas.
62 bis	Fabricar, importar, distribuir, ofrecer o traficar dispositivos, productos, componentes o servicios para evadir medidas tecnológicas efectivas contra la comunicación, la reproducción, el acceso, la puesta a disposición del público o la publicación de obras, interpretaciones, ejecuciones o fonogramas.
63	Alterar, distribuir, importar, transmitir o comunicar información sobre gestión de derechos.
Fuente: Elaboración propia.	

Decreto 37549-JP Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central

El primero de marzo de 2013 fue publicado en el diario oficial *La Gaceta* número 43 el *Decreto 37549-JP Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central.*

Este reglamento indica el deber de los ministerios e instituciones adscritas al Gobierno Central con respecto a usar exclusivamente software que cumpla con los derechos de autor. Cada institución deberá hacer una auditoría anual para determinar la ejecución de lo indicado en él, además de entregar un informe al Registro Nacional. Con este reglamento, el Gobierno de Costa Rica pretende ser un ejemplo para la empresa privada y para toda la sociedad. Su artículo 1 señala:

> Artículo 1. Se ordena que todo el Gobierno Central e Instituciones adscritas se propongan diligentemente prevenir y combatir el uso ilegal de programas de cómputo, con el fin de cumplir con las disposiciones sobre derechos de autor que establece la Ley N.° 6683 y sus reformas, y la

> Ley N.° 8039 y sus reformas, acatando las provisiones pertinentes de los acuerdos internacionales, incluyendo el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, y el Capítulo XV del Tratado de Libre Comercio entre Centroamérica-República Dominicana- Estados Unidos, además de las otras disposiciones de la normativa nacional vigente.

Si bien puede considerarse que lo indicado en el *Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central* solo incumbe a quienes laboran en la unidad de tecnología de información y en el departamento de proveeduría de estas instituciones, realmente esto es también muy importante para todas las personas físicas y jurídicas que son sus proveedoras de software. En efecto, el inciso f del artículo 10 señala lo siguiente:

> Artículo 10. Para los efectos de las adquisiciones y la utilización de programas de cómputo de acuerdo con las disposiciones de este Decreto, el experto en informática (Jefe Informática o quién [*sic*] este designe) de cada Ministerio o Institución adscrita al Gobierno Central deberá cumplir con las siguientes reglas:
>
> f. Exhortar a todos los contratistas y proveedores del Gobierno Central a cumplir con las normas sobre derechos de autor, a adquirir y utilizar programas de cómputo con sus respectivas licencias de uso.

El artículo 14 del reglamento autoriza la utilización de software de código abierto. Sin embargo, no es explícito sobre el software gratuito, como el *shareware* distribuido por los productores, el cual se puede adquirir legalmente. Pese a que, en este caso, no se irrespetan los derechos de propiedad intelectual, es conveniente reflejar la gratuidad del software en el informe de los resultados de la auditoría anual. El artículo 14 indica lo siguiente:

> Artículo 14. Los Ministerios e Instituciones adscritas al Gobierno Central, en los casos que sea posible, podrán utilizar software de código abierto en sus diferentes aplicaciones, como una alternativa útil; garantizando el respeto a los Derechos de la Propiedad Intelectual.

Registro de Propiedad Intelectual en Costa Rica

El Registro Nacional, dependencia del Ministerio de Justicia, tiene como propósito "registrar, en forma eficaz y eficiente, los documentos que se presenten ante el Registro Nacional, para su inscripción, así como garantizar y asegurar a los ciudadanos los derechos con respecto a terceros" (Registro Nacional, s. f., párr. 8). Por tanto, en esta entidad se inscriben las creaciones protegidas por derechos de propiedad intelectual. Existen dos registros: el de la propiedad industrial y el de derechos de autor y derechos conexos. En el primero, se inscriben, entre otros, las patentes de invención; en el segundo, el software.

Es muy importante destacar que, por la *Ley de Derechos de Autor y Derechos Conexos*, el Registro expide una certificación en la que se indica que una obra está registrada a nombre de una persona o entidad. Dicha certificación hace plena prueba, es decir, produce total certeza de la propiedad del derecho a un juez en caso de un proceso judicial, según lo indicado en el artículo 116 de dicha ley:

> Artículo 116. La certificación expedida por el Registrador hará plena prueba de que la obra está registrada a nombre de la persona que en ella se indique, salvo que, por decisión judicial inapelable, la inscripción sea declarada fraudulenta.

Dado que en este capítulo se hace énfasis en el software, a continuación se listan los requisitos que es necesario

presentar al solicitar la protección de derecho de autor para una aplicación de software. Estos son (Araya, 2004):

1. El código fuente del software en formato digital en un sobre lacrado (sellado) con su debida etiqueta, junto con un documento autenticado en el cual se dé fe del contenido del sobre.
2. Separadamente se entrega:
    a. Solicitud de inscripción.
    b. Declaración jurada de auditoría.
    c. Pago correspondiente por derechos de registro.
    d. Indicación explícita del deseo de proteger el software.
    e. Descripción del programa y de los módulos.
    f. Declaración del software utilizado para el desarrollo de la obra.
    g. Copia certificada de los certificados de licencia de uso o distribución, o bien, constancia del proveedor.
    h. Copia del diseño de pantallas, con la descripción de la navegación.
    i. Documentación técnica y manuales de uso.
    j. Todo lo demás que el solicitante considere conveniente.

Según la licenciada Eismey Álvarez, coordinadora de informática del Registro de Derechos de Autor y Conexos, el sobre lacrado permanece así, a no ser que se requiera su contenido como prueba en un proceso judicial (comunicación personal, 24 de julio de 2015). Si se diera este caso, el dueño del derecho de autor es quien abre el sobre, para no invalidar la prueba; este punto es garantía para el creador del software de que su código fuente se mantendrá en reserva.

Según el punto 2.g. de la lista de requisitos, quien solicita la protección de derecho de autor para su software debe estar en capacidad de demostrar dos aspectos: haber utilizado copias legales de las herramientas de desarrollo y tener permiso de usarlas.

La documentación técnica mencionada en el punto 2.i. incluye, al menos, el modelo de datos, el diccionario de datos, la definición de tablas y los tamaños de los campos.

El Registro de Derechos de Autor y Derechos Conexos es la entidad encargada de recibir y evaluar los informes anuales que entregue cada ministerio e institución adscrita al Gobierno Central, para cumplir con lo indicado en el *Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central.*

Aparte de esto, en el Registro de Propiedad Industrial, además de las patentes de invención, se inscriben marcas y otros signos distintivos –entre ellos, los nombres comerciales y emblemas–, dibujos y modelos industriales, indicaciones geográficas y denominaciones de origen –por ejemplo: queso de Turrialba–. Como se expondrá más adelante, también es posible proteger otros elementos del software, para los cuales se pueden utilizar los instrumentos que se inscriben en el Registro de Propiedad Industrial.

¿Se puede patentar software en Costa Rica?

En *La Gaceta*, diario oficial de Costa Rica, número 21 del 30 de enero de 2009 fue publicado el siguiente edicto:

> El señor Édgar Zurcher Gurdian, cédula N.º 1-532-390, mayor, divorciado, abogado, vecino de San José, en su condición de apoderado especial de Microsoft Corporation, de E.U.A., solicita la Patente de Invención denominada: DOCUMENTO PROCESADOR DE PALABRAS

> ALMACENADO EN UN SOLO ARCHIVO XML QUE PUEDE SER MANIPULADO POR APLICACIONES QUE CAPTAN XML. El presente invento tiene el fin de ofrecer un documento de procesamiento de palabras en un formato de archivo XMIL nativo que pueda ser comprendido por una aplicación que comprenda el lenguaje XML, o habilitar a una aplicación o servicio distinto para que logre crear un documento sustancioso en XMIL, de manera que la aplicación de procesamiento de palabras pueda abrirlo como si fuese uno de sus propios documentos. La memoria descriptiva, reivindicaciones, resumen y diseños quedan depositados, la Clasificación Internacional de Patentes Sexta Edición es G06F 17/22, cuyos inventores son Jones, Brian M., Bishop, Andrew K., Snyder, Daniel R., Sawicki, Marcin, Little, Rober A., Krueger, Anthony D. La solicitud correspondiente lleva el número 6980, y fue presentada a las 14:08:39 del 19 de mayo del 2003. Cualquier interesado podrá oponerse dentro de los tres meses siguientes a la tercera publicación de este aviso. Publíquese tres días consecutivos en el Diario Oficial La Gaceta y una vez en un periódico de circulación nacional.—San José, 12 de diciembre del 2008.—Lic. Hellen Marín Cabrera, Registradora. —(4630) (*La Gaceta,* 30 de enero de 2009, p. 12).

La publicación preocupó a los profesionales informáticos porque la empresa Microsoft solicitó patentar software aislado, ya que era la primera solicitud de este tipo en Costa Rica. Se planteó la solicitud el 19 de mayo de 2003 y se rechazó de plano en junio del mismo año; sin embargo, el solicitante insistió en su propósito por un tiempo, aunque finalmente desistió de su petición el 9 de mayo de 2012 y el Registro de Propiedad Industrial archivó la solicitud.

¿Se puede patentar software en Costa Rica? En el artículo 1, inciso 2 del capítulo I de la *Ley 6867 de Patentes de Invención, Dibujos y Modelos Industriales y Modelos de Utilidad* se indica que no puede patentarse el software aisladamente, tal como se lee a continuación:

> Artículo 1.
>
> 2. Para los efectos de esta ley no se considerarán invenciones:

> a) Los descubrimientos, las teorías científicas, los métodos matemáticos y *los programas de ordenador considerados aisladamente* [resaltado añadido].
>
> b) Las creaciones puramente estéticas, las obras literarias y artísticas.
>
> c) Los planes, principios o métodos económicos de publicidad o de negocios y los referidos a actividades puramente mentales, intelectuales o a materia de juego.
>
> d) La yuxtaposición de invenciones conocidas o mezclas de productos conocidos, su variación de forma o uso, dimensiones o materiales, salvo que se trate de una combinación o fusión tal que no puedan funcionar separadamente o que las cualidades o funciones características de ellas sean modificadas para obtener un resultado industrial no obvio para un técnico en la materia.

Al tomar en cuenta lo anterior, parece quedar abierta la posibilidad de que el software integrado a una invención, o empotrado, sí pueda patentarse, pues no está explícitamente excluido de la lista de aquello que no se considera invención. Sin embargo, si se consulta al respecto en el Registro de Propiedad Industrial, se obtendrá como respuesta que no son admitidas las solicitudes de patente para software; hasta la actualidad, no se ha aprobado ninguna. En el caso de que se presente una solicitud para proteger un dispositivo que tenga una aplicación de software integrada, la invención en su totalidad se podrá proteger con una patente o alguna otra forma de protección que sea pertinente, mientras que el software empotrado de forma aislada solo podrá ser protegido por medio de derechos de autor. Por tanto, el dueño de los derechos patrimoniales tendría que presentar otra solicitud, además de la de patente, en el Registro de Derechos de Autor si desea proteger de forma explícita el software.

Aparte de esto, se tiene que el artículo 2 de la *Ley 6867 de Patentes de Invención, Dibujos y Modelos Industriales y Modelos de Utilidad* indica cuáles invenciones son patentables. Se

transcriben a continuación los incisos 1, 3, 5 y 6 de este artículo, considerados los pertinentes para el tema que concierne a este apartado.

> Invenciones patentables
>
> Artículo 2.
>
> 1. Una invención es patentable si es nueva, si tienen nivel inventivo y si es susceptible de aplicación industrial.
>
> 3. Una invención es nueva cuando no existe previamente en el estado de la técnica. El estado de la técnica comprenderá todo lo divulgado o hecho accesible al público en cualquier lugar del mundo y por cualquier medio, antes de la fecha de presentación de la solicitud de patente en Costa Rica o, en su caso, antes de la fecha de prioridad aplicable.
>
> 5. Se considerará que una invención tiene nivel inventivo si para una persona de nivel medio versada en la materia correspondiente, la invención no resulta obvia ni se deriva de manera evidente del estado de la técnica pertinente.
>
> 6. Se considerará que una invención es susceptible de aplicación industrial cuando su objeto pueda ser producido o utilizado en la industria, entendida esta en su más amplio sentido, que abarque entre otros, la artesanía, la agricultura, la minería, la pesca y los servicios.

Debido a que este artículo no excluye la posibilidad de patentar software empotrado, las gestoras de innovación Lilliana Rojas y Yorleny Campos, de la unidad Proinnova de la Universidad de Costa Rica (comunicación personal, 5 de agosto de 2015), opinan que sí existe posibilidad de proteger software empotrado por medio de una patente. Si una persona o entidad crea una invención patentable, es decir, nueva, con nivel inventivo y susceptible de aplicarse industrialmente, la cual, además, incluye una aplicación de software empotrado, podrá patentarla y de esta forma quedará protegido también el software. Sin embargo, la protección de este último no será explícita ni de forma

aislada, pues se le otorgará una patente que cubra la invención como una unidad, lo cual en la *Ley de Patentes de Invención, Dibujos y Modelos Industriales y Modelos de Utilidad* se llama un único concepto inventivo general, tal como se indica en el artículo 7 de esta: "Artículo 7. La solicitud solo podrá referirse a una invención o a un grupo de invenciones relacionadas entre sí, de tal manera que conformen un único concepto inventivo general".

El creador de una invención patentada tendrá "el derecho a explotar, en forma exclusiva, la invención y conceder licencias a terceros para la explotación" (artículo 16 de la *Ley 6867 de Patentes de Invención, Dibujos y Modelos Industriales y Modelos de Utilidad).*

Software libre y software de código abierto

Aunque los conceptos de software libre y software de código abierto son, muchas veces, usados indistintamente, para Richard Stallman, uno de los fundadores del movimiento del primero, no son lo mismo (Stallman, s. f.). Todo el software libre es de código abierto, pero no viceversa. A continuación se describe el significado de cada uno.

El software libre, nombre que acuñó Richard Stallman, es aquel que los usuarios pueden usar, estudiar, modificar y compartir libremente; esto no significa que sea gratuito, aunque puede serlo. Para poder estudiar, modificar y distribuir el software se requiere de acceso al código fuente; existen licencias de software libre que imponen restricciones a quienes las usan.

Algunas aplicaciones han alcanzado un alto nivel de calidad y gran difusión. Por ejemplo, el *kernel* del sistema operativo Linux, desarrollado por muchos grupos y

personas, es uno de los proyectos más grandes y reconocidos del movimiento de software libre. Es ampliamente utilizado por empresas, por sus cualidades de robusto, eficiente y escalable y por poderse utilizar en una amplia variedad de plataformas de hardware (Corvet, 2008). También existe software para usuarios finales, por ejemplo, de ofimática –procesador de texto, hoja de cálculo y presentaciones–, aunque muchas veces las personas se quejan de los problemas de usabilidad de estas aplicaciones. Este es un defecto del software libre al cual es conveniente que los desarrolladores presten mayor atención.

El software de código abierto, por su lado, es una categoría que no se debe confundir con la anterior (Stallman, s. f.). En el caso del software de código abierto, el código fuente es puesto a disposición, bajo una licencia de código abierto con la cual quien ostenta los derechos de autor permite a otras personas estudiarlo, modificarlo y distribuirlo. Distintos tipos de licencia imponen algunas restricciones, tales como mantener en el código el nombre de los autores y redistribuir el software modificado bajo la misma licencia (Open Source Initiative, s. f.); algunas licencias permiten ver el código fuente, mas no ejecutar una versión distinta. Por esta razón, se considera que las licencias de código abierto son más restrictivas que las de software libre (Stallman, s. f.).

Al igual que para el software libre, algunas aplicaciones de código abierto han alcanzado un alto nivel de calidad. Por ejemplo, las creadas por la *Apache Software Foundation*, entre las cuales se encuentra un servidor web utilizado ampliamente por organizaciones, son muy robustas (The Apache Software Foundation, 2017).

Ante la pregunta de si en el futuro todo el software podría ser libre o de código abierto, no existe una única respuesta. Lo cierto es que el software propietario y las categorías anteriormente citadas han convivido por mucho tiempo. Con respecto a cuándo le conviene a una empresa dar

prioridad al uso de software libre y de código abierto y cuándo al software propietario, se debe tomar en cuenta que los primeros no son diferenciadores, por lo que no aportan una ventaja competitiva. El software propietario, en cambio, sí puede darla, si la empresa: 1) mejora sus procesos de negocio con la ayuda de las aplicaciones, 2) aprovecha el conocimiento acerca de sus clientes y 3) diseña una aplicación que saque partido de toda esta información. Por estas razones, es muy probable que continúe la coexistencia del software libre, el de código abierto y el propietario.

Los movimientos del software libre y el de código abierto han creado productos de gran uso y respeto. Se espera que un exceso de protección del software propietario no ponga en riesgo esta otra forma de desarrollo de aplicaciones.

Finalmente, quien desarrolle software tiene derecho a decidir cómo su producto será usado, transferido o copiado. Puede elegir el tipo de licencia bajo el cual desea distribuirlo; si escoge una de software libre o de código abierto, en principio lo respaldará la *Ley de Derechos de Autor y Derechos Conexos,* pues esta le da el derecho de autorizar a otros a reproducir, distribuir y darle uso a su obra.

Protección del software más allá del código

En las secciones anteriores se ha hablado sobre la protección del código, la parte no visible del software, pero se sabe que este es mucho más que código fuente y código objeto. Si bien nadie duda de la importancia de estos, existen elementos visibles muy relevantes, pues dan valor al software y forman parte de los activos intangibles de una organización. También es posible proteger algunos de estos elementos.

La apariencia y la facilidad de uso de una aplicación son primordiales para garantizar su éxito. Muchas horas se invierten en definir la interacción humano-computador (IHC) y la interfaz gráfica de una aplicación de software, con el objetivo de poder competir en un mercado globalizado, en el cual hay mayor cantidad de competidores y los usuarios son cada vez más exigentes en cuanto a usabilidad y accesibilidad.

Las organizaciones, incluso, definen una línea gráfica, la cual no solo permite a clientes y usuarios identificar quién es el fabricante de una aplicación, sino que también les facilita aprender a utilizar distintos productos del mismo desarrollador, por la consistencia mantenida entre ellos. La consistencia en el diseño de la IHC se refiere a crear la interfaz con elementos comunes a las distintas aplicaciones, es decir, utilizar los mismos términos e íconos, ordenar los elementos de un menú de forma semejante y colocar los íconos, botones y otros componentes de la interfaz en la misma posición.

Asimismo, se crean personajes, muchas veces con apariencia humana, los cuales interactúan con los usuarios en páginas web de comercio electrónico o de videojuegos. Todos estos elementos de la interfaz de una aplicación de software son también susceptibles de protección, tanto mediante derechos de autor, en la categoría de dibujos, como también en el Registro de Propiedad Industrial, en calidad de diseños industriales. Según la *Ley 6867 de Patentes de Invención, Dibujos y Modelos Industriales y Modelos de Utilidad,* los diseños industriales se dividen en dos categorías: dibujos industriales y modelos industriales.

Para que un diseño industrial sea protegible, debe ser nuevo, original e independiente, lo cual significa que el diseño debe ser suficientemente distinto de otros ya conocidos. Así se indica en los artículos 25 y 26 de la *Ley de Patentes de Invención, Dibujos y Modelos Industriales y Modelos de Utilidad* los cuales se transcriben a continuación:

Artículo 25.

1. Para los efectos de la presente ley, se considerará dibujo industrial toda reunión de líneas o de colores, modelo industrial toda forma plástica, asociada o no a líneas o colores, siempre que esa reunión o esa forma de [*sic*] una apariencia especial a un producto industrial o de artesanía y pueda servir de tipo para su fabricación. Se considerará modelo de utilidad toda nueva disposición o forma obtenida o introducida en herramientas, instrumentos de trabajo o utensilios conocidos, que permitan una mejor función o una función especial para su uso.

Artículo 26.

1. Los dibujos y modelos industriales nuevos y originales obtenidos independientemente, serán protegidos por esta ley.

Asimismo, es posible que una familia de aplicaciones de software creada por un desarrollador se distinga de la de otro por medio de una marca, un nombre que identifica a su creador. Las marcas han sido usadas por mucho tiempo para dar valor a un bien o servicio y transmitir una idea o emoción. Una marca es un activo intangible, parte del capital intelectual de una empresa; toma tiempo fijarla en la mente de las personas, pero una vez logrado esto, es un elemento diferenciador muy fuerte.

Algunas marcas de software son muy reconocidas e influyen en las personas cuando toman decisiones sobre adquirir o no una aplicación. Cualquier creador de software puede definir su marca, lo cual le ayudará, con el paso del tiempo y el uso de publicidad y redes sociales, a que los clientes identifiquen sus productos fácilmente y estos sean aceptados en el mercado. Las marcas se pueden proteger y registrar en el Registro de Propiedad Industrial, tal como lo garantiza la *Ley 7978 de Marcas y Otros Signos Distintivos.* En el artículo 3 de esta se describen las características de una marca:

> Artículo 3. Signos que pueden constituir una marca. Las marcas se refieren, en especial, a cualquier signo o combinación de signos capaz de distinguir los bienes o servicios; especialmente las palabras o los conjuntos de palabras -incluidos los nombres de personas-, las letras, los números, los elementos figurativos, las cifras, los monogramas, los retratos, las etiquetas, los escudos, los estampados, las viñetas, las orlas, las líneas o franjas, las combinaciones y disposiciones de colores, así como los sonidos. Asimismo, pueden consistir en la forma, la presentación o el acondicionamiento de los productos, sus envases o envolturas o de los medios o locales de expendio de los productos o servicios correspondientes. (Así reformado por la Ley 8632)
>
> Sin perjuicio de las disposiciones relativas a las indicaciones geográficas contenidas en esta ley, las marcas podrán referirse a nombres geográficos, nacionales o extranjeros, siempre que resulten suficientemente distintivos y su empleo no sea susceptible de crear confusión respecto del origen, la procedencia y las cualidades o características de los productos o servicios para los cuales se usen o apliquen tales marcas.
>
> La naturaleza del producto o servicio al cual ha de aplicarse la marca, en ningún caso será obstáculo para registrarla.

Por tanto, esta es otra forma de protección del software que no debe menospreciarse, pues así se evitará que un tercero lucre con una marca consolidada y con buena reputación. Esto se indica en el artículo 25 de la *Ley 7978 de Marcas y Otros Signos Distintivos:*

> Artículo 25. Derechos conferidos por el registro. El titular de una marca de fábrica o de comercio ya registrada gozará del derecho exclusivo de impedir que, sin su consentimiento, terceros utilicen en el curso de operaciones comerciales, signos idénticos o similares, incluso indicaciones geográficas y denominaciones de origen, para bienes o servicios iguales o parecidos a los registrados para la marca, cuando el uso dé lugar a la probabilidad de confusión. En el caso del uso de un signo idéntico, incluidas indicaciones geográficas y denominaciones de origen, para bienes o servicios idénticos, se presumirá la probabilidad de confusión.

Las organizaciones que desarrollan tecnologías de información deben establecer la política de protección de la propiedad intelectual, en la cual se definan las formas de proteger el software que desarrollan. Las que adquieren software también deben tener una estrategia acorde con la ley, para así evitar situaciones que pongan en riesgo su reputación e incluso su continuidad; esta estrategia debe contar con el apoyo de quienes toman decisiones en la organización.

Reflexión

¿Creó usted una aplicación de software con un socio y la comercializan juntos? ¿Confía usted plenamente en su socio? No importa que la respuesta a esta segunda pregunta sea positiva; a veces quien antes era su amigable socio se convierte en su peor pesadilla, al dejarlo a usted sin siquiera el derecho moral de afirmar que usted es uno de los creadores. Asegúrese de que usted es parte de quienes deciden cómo compartirán su aplicación con el mundo. Antes de empezar a distribuirla o comercializarla, proteja su software; después será muy tarde.

CAPÍTULO IV
DISCAPACIDAD

Las personas con discapacidad debemos lidiar, en nuestras vidas, con muchas adversidades.

Adrián Mena
Profesor de inglés, no vidente

Resumen

Actualmente, la discapacidad es vista como el resultado de la interacción con un contexto que impone a las personas barreras limitantes para sus posibilidades de actuar. Por tanto, eliminar dichas barreras es fundamental para permitir a las personas con discapacidad integrarse a nivel social. En Costa Rica, más del 10 por ciento de los habitantes tiene alguna discapacidad. Se han creado leyes contra la discriminación de estas personas y para establecer sus derechos. Una de las más conocidas es la *Ley de Igualdad de Oportunidades para las Personas con Discapacidad*; en esta se garantiza el derecho de acceso a la información, en el cual las aplicaciones de software y otras tecnologías de información y comunicación juegan un papel fundamental. Cumplir con la normativa legal no es difícil ni caro si se toma en cuenta el aspecto de la accesibilidad de una tecnología desde su diseño. Organismos internacionales han definido guías de accesibilidad que reúnen reglas fáciles de aplicar para cumplir con el mandato de la ley. El desarrollo de aplicaciones de software accesibles no debe hacerse únicamente para respetar la legislación, sino también como un compromiso de todo profesional en computación e informática con sus congéneres.

Introducción

Los datos sobre discapacidad en el mundo son alarmantes. En diciembre del 2014 se reportaron las siguientes cifras (Organización Mundial de la Salud, 2014):

1. Más de mil millones de personas, es decir, 15 por ciento de la población mundial, tenía alguna discapacidad.
2. Entre 110 millones y 190 millones de personas mayores de 15 años tenían dificultades considerables para funcionar, es decir, tenían deficiencias o limitaciones que les impedían actuar y participar.
3. El envejecimiento y las enfermedades crónicas, entre otras, causan el aumento continuo de las tasas de discapacidad.

Las personas con discapacidad fueron por mucho tiempo apartadas del resto de la sociedad. Se ha dado un gran avance en el mundo, en general, y en Costa Rica en particular, en los derechos de las personas con discapacidad; la discriminación de la cual han sido objeto por largo tiempo actualmente es inaceptable. Se han promulgado leyes para crear instituciones rectoras de políticas acerca de este tema y para definir los derechos de las personas con discapacidad, pero no es posible aún hablar de una sociedad totalmente inclusiva, en la cual estas personas estén totalmente libres de obstáculos. Para alcanzarlo, es imprescindible hablar de accesibilidad, es decir, del diseño de productos, servicios y ambientes que ofrezcan tecnología de asistencia (por ejemplo, lectores de pantalla). Falta prestar interés a este tema en Costa Rica, especialmente cuando se trata de software y otras tecnologías de información y comunicación. La tecnología debe ayudar a crear oportunidades y mejores condiciones para las personas con discapacidad.

En este capítulo se repasa el concepto de discapacidad, se presentan estadísticas en Costa Rica y se revisan las leyes

sobre este tema relacionadas con tecnologías de información y comunicación. Además, se dan ejemplos de las acciones legales posibles cuando no se cumple la normativa y, finalmente, se brinda una guía de accesibilidad para las personas que participan en el desarrollo de software y otras tecnologías de información y comunicación. En este grupo se incluyen, entre otros, profesionales en computación e informática, diseño gráfico, psicología, sociología y comunicación.

¿Qué es la discapacidad?

Por mucho tiempo, la presencia de una persona con discapacidad fue motivo de vergüenza para sus familiares y de compasión para otros. Se hablaba en el pasado de personas inválidas, incapacitadas o minusválidas, lo cual le restaba valor a estos seres humanos. La sociedad es ahora más madura y ha entendido que estas personas deben integrarse a ella; asimismo, el concepto de discapacidad ha cambiado a lo largo del tiempo. La OMS, en su clasificación internacional del funcionamiento y la discapacidad, define esta como "un término que engloba deficiencias, limitaciones de la actividad y restricciones a la participación" (Organización Mundial de la Salud, 2011, p. xxiii).

La OMS ve la discapacidad como el resultado de la interacción entre dos partes: 1) la persona que padece alguna enfermedad o tiene una limitación física o mental y 2) los factores personales y ambientales. Entre estos últimos se incluyen el rechazo y la infraestructura inaccesible (Organización Mundial de la Salud, 2014).

El artículo 1 de la *Convención Interamericana de la Eliminación de todas las Formas de Discriminación contra las Personas con Discapacidad* de la Organización de Estados Americanos (OEA) define la discapacidad como:

> Una deficiencia física, mental o sensorial, ya sea de naturaleza permanente o temporal, que limita la capacidad de ejercer una o más actividades esenciales de la vida diaria, que puede ser causada o agravada por el entorno económico y social (Organización de Estados Americanos, 1999, p. 2).

En esta definición también se hace referencia al entorno, el cual no solo puede agravar la condición de discapacidad, sino causarla. En Costa Rica, el Consejo Nacional de Rehabilitación y Educación Especial (CNREE) es la institución rectora de las políticas públicas acerca del tema de discapacidad. El artículo 4 del *Reglamento para el Otorgamiento de Subsidios para Personas con Discapacidad en Condición de Pobreza y Abandono* del CNREE define la discapacidad así:

> Artículo 4
>
> Discapacidad: es el resultado de la interacción de una persona que experimenta algún grado de limitación funcional y el contexto que no le ofrece los apoyos y servicios accesibles, oportunos y efectivos, por lo cual se ve limitada en la realización de sus actividades y restringida en la participación en situaciones esenciales de la vida.

Nótese que en las visiones de la OMS, la OEA y el CNREE hay un factor común: la discapacidad es resultado de la interacción entre una persona con alguna limitación y un entorno que no se adapta a sus necesidades especiales. Por tanto, un cambio en el entorno podría ayudar a la persona con discapacidad a conseguir autonomía e independencia.

La autoestima de las personas se fortalece cuando pueden realizar sus tareas y alcanzar sus metas de forma independiente, pues así sienten que realmente se integran a la sociedad. Las computadoras y tecnologías de información y comunicación pueden ayudar en este propósito; sin embargo, quienes las diseñan y programan no siempre consideran este aspecto cuando realizan su trabajo. Por ejemplo, si se piensa en un ascensor, uno de los medios de transporte que más personas moviliza diariamente en el mundo, se sabe que, además de las partes físicas, es un sistema controlado por una

aplicación de software que se ejecuta en una computadora. Suponga que usted es no vidente y espera el ascensor en el cuarto piso de un edificio para bajar al primero. La cabina del ascensor llega al cuarto piso y se abre la puerta. Sin una señal sonora que lo indique, la persona no podrá saber si el ascensor se dirige hacia la dirección deseada; deberá recurrir a alguien para preguntárselo o arriesgarse a entrar en la cabina y subir hasta el último piso del edificio. Para poder movilizarse con independencia y seguridad, otra señal sonora que indique a la persona a cuál piso llegó será necesaria para saber si ha arribado a su destino. Todas estas señales son controladas por el software.

Existen estándares internacionales sobre cómo debe funcionar un ascensor, pero en Costa Rica los vendedores de estos dispositivos no siempre se apegan a ellos. También existen leyes que definen los derechos de las personas con discapacidad; sin embargo, muchas veces no se cumplen.

Discapacidad en Costa Rica

Según los resultados del X Censo Nacional de Población y VI de Vivienda del Instituto Nacional de Estadística y Censos (INEC), en el año 2011 vivían en Costa Rica 452 849 personas con discapacidad, lo que representa el 10,53 por ciento de los habilitantes del país (Instituto Nacional de Estadística y Censos, 2012). Los tipos de discapacidad más comunes son la visual aun cuando se utilicen anteojos –el 55,53 por ciento de los habitantes con discapacidad la tiene–, la imposibilidad para caminar o subir gradas –el 31 por ciento– y la auditiva –el 15,61 por ciento–; las discapacidades sensoriales y las de movimiento son las más frecuentes.

En el cuadro 2 se muestra la distribución de la población total de Costa Rica por tipo de discapacidad, según la clasificación que hace el INEC. Es notable que el porcentaje de personas con discapacidad aumenta significativamente con la edad; como lo menciona la OMS, la incidencia de

enfermedades crónicas es una de las principales causas de esto (Organización Mundial de la Salud, 2014). Es importante destacar que la población costarricense está en un proceso de envejecimiento demográfico desde hace varias décadas. En 1984, el 4,5 por ciento de los habitantes tenía 65 años de edad o más, mientras que en el 2000 y 2011 este grupo etario había alcanzado el 5,6 por ciento y el 7,2 por ciento, respectivamente (Instituto Nacional de Estadística y Censos, 2012).

Las proyecciones del INEC muestran que el envejecimiento demográfico de la sociedad costarricense continuará si se mantiene la esperanza de vida alta y el descenso en la fecundidad. Además, aumenta constantemente la incidencia de enfermedades cardiovasculares y diabetes a una edad más temprana, debido a los hábitos de alimentación y el sedentarismo. Por esto, las autoridades de salud del país insisten en la importancia de seguir un modo de vida sano que ayude a llegar a una vejez saludable.

Es importante destacar que en el cuadro 2 se incluyen solamente quienes tienen una discapacidad severa. Sin embargo, entre las personas consideradas *normales*, es decir, que no sobrepasan un cierto límite arbitrario, se presentan discapacidades en distintos grados, las cuales, si bien no les imposibilitan realizar las tareas diarias, sí les causan cierto grado de dificultad, incomodidad e, incluso, peligro. Por ejemplo, quienes no distinguen un color, al vestirse pueden combinar colores de ropa que no se vean bien; aunque esto no es un problema para su seguridad, sí puede ser motivo de burla para otras personas. Existen otras situaciones que pueden generar peligro. En las aplicaciones de software, se utilizan estándares de colores para indicar al usuario que está cerca de realizar una transacción irreversible, por ejemplo, eliminar datos. Sin embargo, quien no se percate de esto podría ejecutar el comando y perder información importante.

Cuadro N.º 2

Distribución de la población por tipo de discapacidad en Costa Rica

Población con discapacidad en Costa Rica 1/									
Grupos de edad	Población total	Para ver aun con anteojos	Para oír	Para hablar	Para caminar o subir gradas	Para utilizar brazos o manos	De tipo intelectual	De tipo mental	Porcentaje de personas con discapacidad
Todas las edades	4 301 712	5,85%	1,64%	0,68%	3,26%	1,14%	0,82%	0,63%	10,53%
De 0 a 14	1 067 830	1,36%	0,31%	0,69%	0,44%	0,21%	0,90%	0,25%	3,37%
De 15 a 29	1 194 080	2,57%	0,42%	0,40%	0,70%	0,33%	0,95%	0,42%	4,85%
De 30 a 59	1 590 466	7,39%	1,30%	0,53%	3,08%	1,23%	0,68%	0,71%	12,22%
De 60 a 64	137 624	16,26%	3,93%	0,88%	10,02%	3,46%	0,56%	1,04%	27,04%
De 65 a 74	181 582	18,77%	7,08%	1,36%	14,71%	4,52%	0,66%	1,36%	33,65%
De 75 a 89	117 955	24,05%	16,33%	3,50%	27,32%	7,28%	1,13%	2,98%	49,13%
De 90 o más	12 175	32,79%	34,65%	9,10%	46,33%	13,17%	2,32%	5,86%	68,17%

1/ Algunas personas tienen más de una discapacidad, por lo que caen en más de una categoría.

Fuente: Elaboración propia con base en datos del X Censo Nacional de Población y VI de Vivienda del Instituto Nacional de Estadística y Censos (2012).

Ver Cuadro 2 en línea

Fijarse en los porcentajes es importante, pero lo es más comprender que las cifras sobre discapacidad revelan la gran cantidad de personas que se enfrentan diariamente con obstáculos para realizar sus tareas. Además, cualquier persona puede tener un accidente o encontrarse en una situación que le cause una discapacidad temporal; esto no se representa en las estadísticas del cuadro 2. Por ejemplo, cuando una persona se quiebra una extremidad o cuando se encuentra en un medio con poca luz o mucho ruido, esta condición temporal puede ser un impedimento para realizar una tarea. De una u otra forma, todas las personas tienen algún grado de discapacidad, la cual puede ser congénita, por un accidente o pérdida paulatina de las capacidades, ya sea por enfermedad, hábitos alimenticios, desgaste, exposición constante a ruido o exceso de luz, falta de actividad física, malas posturas, deporte o ejercicio físico mal realizado, violencia o envejecimiento. Por lo tanto, todo esfuerzo que se realice para eliminar las barreras sociales, económicas y físicas agravantes de la situación de las personas con discapacidad puede beneficiar a otras en algún momento de su vida.

Legislación sobre discapacidad

Muchas aplicaciones de software son rígidas, es decir, no permiten excepciones. Estas pueden impedir a alguien ejercer un derecho garantizado por la Constitución Política de Costa Rica, por ejemplo, el derecho al trabajo. Por tanto, al hablar de legislación sobre discapacidad, se debe tener presente que, ante todo, el software y cualquier otra tecnología de información y comunicación no deben impedir a una persona disfrutar de sus derechos.

En Costa Rica, la lista de la legislación específica sobre discapacidad es amplia, pues se empezó a crear desde mediados del siglo XX. En 1957 se aprobó la *Ley 2171 sobre el Patronato Nacional de Ciegos*. La Ley 5347 de 1973 creó el Consejo Nacional de Rehabilitación y Educación Especial, entidad rectora de las políticas públicas acerca del tema de discapacidad en Costa Rica. Las funciones de esta institución se definen en el artículo 2 de la Ley 5347, el cual se transcribe enseguida.

> Artículo 2. El Consejo Nacional de Rehabilitación y Educación Especial, tendrá las siguientes funciones:
>
> a) Servir de instrumento coordinador y asesor entre las organizaciones públicas y privadas que se ocupen de la Rehabilitación y la Educación Especial.
>
> b) Coordinar un Plan Nacional de Rehabilitación y Educación Especial que integre sus programas y servicios con los Planes específicos de Salud, Educación y Trabajo, evitando duplicaciones y utilizando los recursos económicos y humanos disponibles.
>
> c) Promover la formación de profesionales especialistas en rehabilitación y educación especial, en conexión con las Universidades y entidades que tengan a su cargo la preparación de personal profesional, técnico y administrativo.
>
> d) Fomentar medidas que aseguren las máximas oportunidades de empleo para los disminuidos físicos y mentales.

e) Organizar el Registro Estadístico Nacional de los Disminuidos Físicos o Mentales para su identificación, clasificación y selección.

f) Motivar, sensibilizar e informar acerca de los problemas, necesidades y tratamiento de la población que requiere de Rehabilitación y Educación Especial.

g) Gestionar en coordinación con los Ministerios respectivos la provisión anual de los fondos necesarios para la atención debida de los programas de Rehabilitación y Educación Especial asegurando su utilización para los fines establecidos.

h) Coordinar con los Ministerios y Organismos Nacionales e Internacionales la canalización por medio del Consejo Nacional de Rehabilitación y Educación Especial; y, además estimular la superación del personal solicitando becas adicionales.

La más conocida de las leyes sobre discapacidad es la *Ley 7600 de Igualdad de Oportunidades para las Personas con Discapacidad*, de 1996 y reformada el año 2014. En esta ley se definieron los derechos de las personas con discapacidad y se reforzó el papel del CNREE. En 1999, con la Ley 7948, Costa Rica se adhirió a la *Convención Interamericana para la Eliminación de todas las Formas de Discriminación contra las Personas con Discapacidad*. Posteriormente, en el 2008, por medio de la Ley 8661, otro tratado internacional, la *Convención sobre los Derechos de las Personas con Discapacidad y su Protocolo*, entró en vigencia. En esta sección se hace énfasis en estas tres leyes, pues se les considera las más pertinentes en cuanto a discapacidad y tecnologías de información y comunicación.

Ley 7600 de Igualdad de Oportunidades para las Personas con Discapacidad

La *Ley 7600 de Igualdad de Oportunidades para las Personas con Discapacidad* y su reglamento consagra los derechos de las personas con discapacidad: acceso al sistema educativo, el trabajo, los servicios de salud, el espacio físico, los medios de

transporte, la información y la comunicación, la cultura, el deporte y las actividades recreativas.

Para los profesionales en computación e informática u otros campos que se relacionen con el diseño y el desarrollo de software, el capítulo VI –titulado "Acceso a la información y la comunicación"–, contiene los artículos más relevantes para su ejercicio laboral en cuanto a discapacidad. Los artículos 50 y 51 de esta ley garantizan el derecho de acceso a la información, el cual es también reconocido internacionalmente (Lobo, s. f.). Los artículos señalan:

> Artículo 50. Información accesible. Las instituciones públicas y privadas deberán garantizar que la información dirigida al público sea accesible a todas las personas, según sus necesidades particulares.
>
> Artículo 51. Programas informativos. Los programas informativos transmitidos por los canales de televisión, públicos o privados, deberán contar con los servicios de apoyo, inclusive intérpretes o mensajes escritos en las pantallas de televisión, para garantizarles a las personas con deficiencias auditivas el ejercicio de su derecho de informarse.

El artículo 177 del *Reglamento de la Ley de Igualdad de Oportunidades para las Personas con Discapacidad* refuerza lo establecido en la ley y menciona explícitamente los sistemas de información y comunicación, entre los cuales se incluyen aplicaciones de software, tal como se lee en la siguiente cita:

> Artículo 177. Sistemas informativos. Todas las instituciones públicas y privadas que brinden servicios al público adaptarán, a las necesidades de las personas con discapacidad y sus familias, *todos los sistemas de información y comunicación* [resaltado añadido], materiales divulgativos, así como los medios tecnológicos utilizados para esos fines, entre ellas el uso del Braille y el Lenguaje de Señas Costarricense.

Para los profesionales en computación e informática, el artículo 50 de la Ley 7600 debe estar siempre presente en el momento de desarrollar aplicaciones de software u otros productos. En la actualidad, muchas instituciones, empresas

privadas y organizaciones publican por medios digitales información dirigida al público. Internet se ha convertido en la fuente de información más consultada; catálogos de productos y servicios, material sobre salud, libros, cursos en línea, comercio electrónico y acceso a consultas sobre trámites en instituciones públicas son solo algunos ejemplos de lo que la gente busca. No tener acceso a Internet significa estar en desventaja.

Asimismo, con la adopción masiva de teléfonos inteligentes y dispositivos móviles en general, han surgido nuevos obstáculos. Por una parte, muchas páginas *web* diseñadas para computadoras de escritorio y portátiles no se aprecian bien en las pantallas pequeñas de estos dispositivos, por lo cual se dificulta usarlas. Las aplicaciones de software creadas especialmente para dispositivos móviles ofrecen a las personas usuarias acceso a información y servicios muy variados, pero no todas se han diseñado pensando en las personas con discapacidad. Costa Rica es un país con un alto uso de la telefonía celular. Actualmente, existen más líneas telefónicas que personas; por esta razón, es muy importante considerar el tema de la accesibilidad cuando se desarrollan aplicaciones para dispositivos móviles.

El artículo 53 de la Ley 7600 establece las facilidades que deben brindar las bibliotecas de acceso público a todos sus usuarios:

> Artículo 53. Bibliotecas. Las bibliotecas públicas o privadas de acceso público, deberán contar con servicios de apoyo, incluyendo el personal, el equipo y el mobiliario apropiados, para permitir que puedan ser efectivamente usadas por todas las personas.

El artículo 53 hace referencia al equipo apropiado, el cual puede incluir la posibilidad de contar con aplicaciones de software que lean el contenido de una pantalla, reciban instrucciones por medio de la voz humana, emitan señales sonoras para alertar al usuario de un riesgo, generen e impriman texto en el sistema de escritura y lectura táctil

braille o agranden la imagen de la pantalla. Quienes laboran en el departamento de proveeduría de una empresa y los profesionales en computación e informática responsables de gestionar o autorizar la adquisición de equipos computacionales para bibliotecas deben tener presente este artículo de la ley, con el fin de facilitar el acceso a todas las personas.

El artículo 44 de la Ley 7600 y los 150, 151 y 152 de su reglamento se refieren al tema de los ascensores. Dichos artículos se transcriben a continuación.

> Artículo 44. Ascensores. Los ascensores deberán contar con facilidades de acceso, manejo, señalización visual, auditiva y táctil, y con mecanismos de emergencia, de manera que puedan ser utilizados por todas las personas.
>
> Artículo 150. Entradas a edificios. Del total de las entradas utilizadas por el público en cualquier edificio, al menos una de ellas estará a nivel o el cambio de nivel será salvado por ascensor o rampa, con la pendiente indicada en el artículo 124 de este Reglamento.
>
> Artículo 151. Características de los ascensores. Los ascensores deberán presentar una abertura máxima de 0.02 mts. entre el carro y el piso. Exactitud en la parada: 0.02 mts. máximo entre el piso del edificio y el piso del ascensor. Ancho mínimo de puerta: 0.90 mts. Las dimensiones interiores mínimas de 1.10 mts. de ancho por 1.40 mts. de profundidad y deberán contar con señalización en Braille y auditiva.
>
> La puerta será preferiblemente telescópica. Altura máxima de botones de servicio (exterior e interior): 1.20 mts. La velocidad de cierre de las puertas del ascensor, debe permitir el ingreso y egreso sin riesgo para el usuario.
>
> Artículo 152. Parada de ascensores. En el caso de edificios con elevadores o ascensores, éstos [*sic*] tendrán parada en todos los pisos, incluyendo mezanines y sótanos.

Se mencionan estos artículos aquí, pues un computador oculto para los usuarios controla un sistema de ascensores. El software es el encargado de activar las puertas y la señalización; por tanto, estos aspectos son programables. El profesional en computación e informática, ingeniero o

técnico que tenga a su cargo la responsabilidad de instalar un sistema de ascensores, ya sea por la parte proveedora o por la parte cliente, debe tener presente los requisitos que deben cumplir los ascensores, con el fin de apegarse a la ley, pero especialmente, para facilitar a todas las personas el uso de este medio de transporte. Una fuente valiosa para informarse al respecto es la Organización Internacional para Estandarización, más conocida como ISO, la cual ha publicado estándares para ascensores.

Ley 7948 Convención Interamericana para la Eliminación de todas las Formas de Discriminación contra las Personas con Discapacidad

La *Ley 7948 Convención Interamericana para la Eliminación de todas las Formas de Discriminación contra las Personas con Discapacidad* es un compromiso adquirido por los países que la han adoptado. Si bien no hay en ella referencia directa a las computadoras y las tecnologías de información y comunicación, es importante el artículo 4, el cual indica:

> Artículo IV. Para lograr los objetivos de esta Convención, los Estados parte se comprometen a:
>
> 1. Cooperar entre sí para contribuir a prevenir y eliminar la discriminación contra las personas con discapacidad.
>
> 2. Colaborar de manera efectiva en:
>
> a) La investigación científica y tecnológica relacionada con la prevención de las discapacidades, el tratamiento, la rehabilitación e integración a la sociedad de las personas con discapacidad; y
>
> b) *El desarrollo de medios y recursos diseñados para facilitar o promover la vida independiente, autosuficiencia e integración total, en condiciones de igualdad, a la sociedad de las personas con discapacidad* [resaltado añadido].

El inciso 2, apartado b) del artículo 4 se refiere al desarrollo de medios y recursos, entre los cuales se podrían incluir el software y otras tecnologías de información y comunicación, tales como exoesqueletos y casas inteligentes. Las personas profesionales en computación e informática deben procurar que los productos y servicios que crean faciliten y promuevan la vida independiente, la autosuficiencia y la integración total de todas las personas, especialmente de las personas con discapacidad.

Ley 8661 Convención sobre los Derechos de las Personas con Discapacidad

La *Ley 8661 Convención sobre los Derechos de las Personas con Discapacidad* es la más reciente de las tres consideradas en este capítulo. Fue aprobada por todos los países miembros de las Naciones Unidas en el año 2006; en ella se plantea la discapacidad como resultado de la interacción de la persona con barreras existentes en el entorno o por causa de la actitud de otras. En esta ley se consideran, a muy alto nivel, las acciones que en Costa Rica se deben emprender para eliminar dichas barreras.

Es necesario destacar dos puntos en los apartados f) y g) del inciso 1 del artículo 4 de la convención, en los cuales se habla de bienes, servicios y equipo de diseño universal, y se menciona la necesidad de dar mayor prioridad a las tecnologías de un precio asequible para las personas con discapacidad. En primer lugar, por diseño universal se refiere a que el producto pueda ser utilizado fácilmente por personas con el más amplio rango de habilidades posible. En segundo lugar, el tema del precio asequible es muy importante, porque discapacidad y pobreza están muchas veces correlacionadas, debido al rezago en educación de las personas con esta condición, con la consecuente dificultad para conseguir trabajo y, más aún, que este sea bien remunerado (Programa Sociedad de la Información y el Conocimiento, 2011). Ante estas circunstancias, el artículo 27 del *Reglamento de la Ley de*

Igualdad de Oportunidades para las Personas con Discapacidad contempla la ayuda técnica y económica a familias en riesgo social en los casos en que uno o más miembros tengan una discapacidad. El inciso 1 del artículo 4 de la convención indica lo siguiente:

> Artículo 4. Obligaciones generales
>
> 1. Los Estados Partes se comprometen a asegurar y promover el pleno ejercicio de todos los derechos humanos y las libertades fundamentales de las personas con discapacidad sin discriminación alguna por motivos de discapacidad. A tal fin, los Estados Partes se comprometen a:
>
> f) Emprender o promover la investigación y el desarrollo de bienes, servicios, equipo e instalaciones de diseño universal, con arreglo a la definición del artículo 2 de la presente Convención, que requieran la menor adaptación posible y el menor costo para satisfacer las necesidades específicas de las personas con discapacidad, promover su disponibilidad y uso, y promover el diseño universal en la elaboración de normas y directrices;
>
> g) Emprender o promover la investigación y el desarrollo, y promover la disponibilidad y el uso de nuevas tecnologías, incluidas las tecnologías de la información y las comunicaciones, ayudas para la movilidad, dispositivos técnicos y tecnologías de apoyo adecuadas para las personas con discapacidad, *dando prioridad a las de precio asequible* [resaltado añadido].

Se quiere destacar que crear software y tecnologías de información y comunicación accesibles no debería conllevar un aumento significativo en el costo de producirlos ni en su precio de venta, pues si ocurriera, esto imposibilitaría el acceso a las personas con discapacidad. La brecha económica y la brecha digital se pueden retroalimentar mutuamente, y formar así un círculo vicioso.

El artículo 9 de la Ley 8661, titulado “Accesibilidad”, resalta la importancia del acceso a los servicios de información y las comunicaciones, incluidos los sistemas y las tecnologías de la información y comunicación, y establece las medidas necesarias para garantizar a las personas con discapacidad el

acceso a la información. Entre ellas, se sugiere que el tema de accesibilidad sea tomado en cuenta desde las primeras etapas de diseño de los nuevos productos. Esto tiene sentido porque se sabe que realizar cambios en las etapas finales siempre es mucho más caro que introducir desde el principio los elementos necesarios para alcanzar los objetivos de accesibilidad. El artículo 9 indica:

> Artículo 9. Accesibilidad
>
> 1. A fin de que las personas con discapacidad puedan vivir en forma independiente y participar plenamente en todos los aspectos de la vida, los Estados Partes adoptarán medidas pertinentes para asegurar el acceso de las personas con discapacidad, en igualdad de condiciones con las demás, al entorno físico, el transporte, la información y las comunicaciones, incluidos los sistemas y las tecnologías de la información y las comunicaciones, y a otros servicios e instalaciones abiertos al público o de uso público, tanto en zonas urbanas como rurales. Estas medidas, que incluirán la identificación y eliminación de obstáculos y barreras de acceso, se aplicarán, entre otras cosas, a:
>
> b) Los servicios de información, comunicaciones y de otro tipo, incluidos los servicios electrónicos y de emergencia.
>
> 2. Los Estados Partes también adoptarán las medidas pertinentes para:
>
> g) Promover el acceso de las personas con discapacidad a los nuevos sistemas y tecnologías de la información y las comunicaciones, incluida Internet;
>
> h) *Promover el diseño, el desarrollo, la producción y la distribución de sistemas y tecnologías de la información y las comunicaciones accesibles en una etapa temprana* [resaltado añadido], a fin de que estos sistemas y tecnologías sean accesibles al menor costo.

El artículo 21 de la Ley 8661, el cual trata sobre libertad de expresión y de opinión y acceso a la información, en los incisos a), c) y d), destaca el uso de formatos accesibles para las personas con discapacidad, con el fin de que tengan acceso en las mismas condiciones que las demás. Esto sugiere el uso de distintos canales para brindar información, tales como la asistencia personal, la voz sintetizada, la mensajería de texto,

páginas web y el uso de subtítulos y lengua de señas en videos. El artículo 21 se transcribe seguidamente.

> Artículo 21. Libertad de expresión y de opinión y acceso a la información. Los Estados Partes adoptarán todas las medidas pertinentes para que las personas con discapacidad puedan ejercer el derecho a la libertad de expresión y opinión, incluida la libertad de recabar, recibir y facilitar información e ideas en igualdad de condiciones con las demás y mediante cualquier forma de comunicación que elijan con arreglo a la definición del artículo 2 de la presente Convención, entre ellas:
>
> a) Facilitar a las personas con discapacidad información dirigida al público en general, de manera oportuna y sin costo adicional, *en formatos accesibles y con las tecnologías adecuadas a los diferentes tipos de discapacidad* [resaltado añadido];
>
> c) Alentar a las entidades privadas que presten servicios al público en general, incluso mediante Internet, a que proporcionen información y servicios en formatos que las personas con discapacidad puedan utilizar y a los que tengan acceso;
>
> d) Alentar a los medios de comunicación, incluidos los que suministran información a través de Internet, a que hagan que sus servicios sean accesibles para las personas con discapacidad;

Claramente, existe legislación que, de forma explícita o implícita, define requerimientos de accesibilidad obligatorios en los bienes y servicios producidos por profesionales en computación e informática.

¿Qué pasa si no se cumple la legislación sobre discapacidad?

Dado que las tres leyes sobre discapacidad analizadas anteriormente no imponen sanciones por su incumplimiento, cuando las personas sienten que sus derechos no son respetados, interponen un recurso de amparo en la Sala Constitucional de la Corte Suprema de Justicia. Si la Sala lo

acoge y lo declara con lugar, la persona u organización recurrida está obligada a hacer los cambios necesarios para respetar los derechos de quien planteó el recurso, también llamado el recurrente. Las sentencias de la Sala Constitucional son importantes para los profesionales en computación e informática, pues representan jurisprudencia guía para saber cómo actuar con el fin de evitar recursos de amparo.

Algunos ejemplos de recursos de amparo resueltos recientemente se resumen y comentan a continuación:

1. **Se ordena prorrogar licencia de conducir por un año. Se afirma que los sistemas informáticos deben adaptarse a los derechos fundamentales de las personas**
   Sentencia 18295-2014

   En este caso, el recurrente padecía de distrofia muscular. Por esta razón, el Colegio de Médicos y Cirujanos podía extender un dictamen médico, requisito para solicitar licencia de conducir, solo por el plazo de un año. El Departamento de Acreditación de Conductores del Ministerio de Obras Públicas y Transportes (MOPT) negó al recurrente la renovación de la licencia, pues no era posible otorgársela por menos de seis años. El recurrente alegó trabajar como chofer, por lo que se le estaba negando el derecho a trabajar libre y dignamente. El recurrido adujo, entre otras, limitaciones informáticas para extender la licencia por un periodo menor a seis años. La Sala Constitucional declaró con lugar el recurso contra el MOPT y afirmó que las limitaciones informáticas no son una razón aceptable. Los sistemas informáticos deben permitir respetar los derechos fundamentales de las personas. Este es un ejemplo en el cual el recurrente no interactúa de forma directa con el software; sin embargo, la rigidez de este impedía hacer efectivo el derecho al trabajo de todo costarricense.

2. **Se ordena al Ministerio de Hacienda crear programas para que las declaraciones y la página web sean accesibles a personas con discapacidad visual**
   Sentencia 11851-2014

   Este recurso fue interpuesto contra el Ministerio de Hacienda. Fue declarado con lugar y se obligó al Ministerio a realizar las acciones pertinentes con el fin de crear programas para los distintos tipos de declaraciones de impuesto, los cuales sean accesibles para personas con discapacidad visual (usuarios de lectores de pantalla). Asimismo, el Ministerio debe proveer una versión de la página web accesible para personas con discapacidad visual, es decir, en la cual se pueda tener acceso a toda la información mediante un lector de pantalla.

3. **Cambios en el cobro de recibos del servicio de agua**
   Sentencia 3567-2014

El recurrente planteó un recurso contra el Instituto Costarricense de Acueductos y Alcantarillados (AyA) porque consideró que se lesionaban sus derechos fundamentales por los cambios futuros con respecto a la forma de consultar el monto de los recibos de agua. Dichos cambios consisten en dejar de entregar el recibo de papel y que el monto se puede consultar en la página web del AyA. El recurrente alegó la existencia de gente que no sabe leer ni escribir y de personas con alguna discapacidad que viven solas, entre otras, que no cuentan con herramientas tecnológicas para acceder a consultar el recibo en estas condiciones. La Sala Constitucional declaró sin lugar el recurso, pues además del acceso por medios tecnológicos, también se cuenta con otras opciones, tales como: a) la línea gratuita 800-REPORTE, b) servicio de mensajería de texto, c) agentes recaudadores, con el número de localización (NIS), d) solicitud de duplicado de factura y e) solicitud de envío de facturas mediante correo electrónico. Este caso es interesante, pues si bien personas con ciertas discapacidades no pueden acceder a un recurso

tecnológico en particular, sí pueden hacerlo por otros medios. Esto es congruente con el artículo 21 de la *Ley 8661 Convención sobre los Derechos de las Personas con Discapacidad.* Por lo tanto, la lección que esta sentencia deja es que las organizaciones deben procurar ofrecer a sus usuarios varios canales de acceso; de esta forma, un posible recurso de amparo no procedería. Sin embargo, esto no exonera a las organizaciones de crear medios tecnológicos accesibles.

Tecnologías de información y comunicación accesibles

En muchas ocasiones es notorio que las organizaciones se preocupan por crear un entorno físico accesible. Elementos como rampas, ascensores, señales en braille, pisos antideslizantes, servicios sanitarios más amplios o lavatorios alcanzables para personas en silla de ruedas son algunos de los encontrados más comúnmente en sitios públicos. Sin embargo, pocas veces se brinda la atención necesaria al software, pese a estar presente en todos los campos de la actividad humana.

¿Por qué se brinda poca importancia a la accesibilidad del software y de otras tecnologías de información y comunicación? No hay una respuesta única. Probablemente se debe a varias razones combinadas, tales como el desconocimiento del porcentaje de personas con discapacidad, la predominancia de desarrolladores de software muy jóvenes sin discapacidad, la falta de formación en el campo, la creencia de que crear tecnología accesible es costoso y la falta de sensibilidad.

¿Qué se requiere para construir software y otras tecnologías de información y comunicación accesibles? Lo primero y más importante es la conciencia de la importancia de crear tecnologías accesibles y de conocer las necesidades y limitaciones de los posibles usuarios. Otro factor es la

participación de personas con discapacidad en el proceso de desarrollo, con el fin de identificar las características requeridas en la interfaz y la forma de interacción para hacer accesibles las tecnologías.

La participación de personas con discapacidad es muy conveniente, pues son ellas quienes pueden brindar su punto de vista para definir requerimientos y verificar las tecnologías creadas. Por ejemplo, en Costa Rica se creó un buscador en línea para personas no videntes, llamado CR Texter (Vargas, 2015). En su desarrollo participaron personas con esta condición. Un detalle interesante es que el software evita la infección de la computadora del usuario con software malicioso, pues el resultado recibido por quien hace la búsqueda es un archivo de texto que CR Texter genera, el cual contiene los enlaces y el contenido de las páginas encontradas. Si bien la preocupación por la seguridad es común a todos los usuarios de Internet, las personas no videntes están en desventaja, pues podrían no darse cuenta de que empieza a ejecutarse de forma no deseada un programa; por tanto, estas personas son más vulnerables. Esto genera un requerimiento de seguridad en el cual comúnmente no se pensaría si no se conocieran sus necesidades especiales. Pese a sus ventajas, la participación de personas con discapacidad en el proceso de desarrollar software todavía es una práctica poco común en Costa Rica.

Son aún muchos los obstáculos que las personas con discapacidad enfrentan al utilizar una computadora. Por ejemplo, muchos videos no son traducidos a lengua de señas ni muestran subtítulos, lo cual es una gran limitación para personas con discapacidad auditiva. El desarrollo de algoritmos para solucionar de forma automática estos obstáculos es una labor que requiere un gran esfuerzo humano y muchos recursos materiales, por lo cual muy probablemente solo grandes empresas transnacionales puedan invertir en un proyecto de esta naturaleza. Por ejemplo, Youtube tiene en ejecución un proyecto con el objetivo de generar subtítulos con muy alta calidad de los videos presentes en su plataforma (Vargas, 2017).

Si bien las empresas costarricenses no cuentan con el capital para emprender un proyecto de esta magnitud, sí pueden definir una política de accesibilidad y guías para el diseño y el desarrollo de tecnologías de información accesibles. Para esto se debe contar con el apoyo de quienes toman decisiones en las organizaciones y con un plan para concientizar y capacitar todo el personal participante en el proceso de diseño y desarrollo.

¿En cuál etapa del ciclo de desarrollo de un producto se introduce el tema de la accesibilidad? Debe hacerse desde la primera etapa, pues esto tendrá varios beneficios encadenados, como evitar rehacer el trabajo, lo cual redundará en menos tiempo de desarrollo y menores costos para el productor y, finalmente, menor precio para el usuario. Así, se creará tecnología accesible y asequible.

Desarrollar aplicaciones de software accesibles no debe consistir únicamente en apegarse a la ley, sino también en un compromiso de todo profesional en computación e informática con sus congéneres. Cumplir con lo indicado en la ley y aún transcenderlo no es difícil. Ya existen guías para crear tecnologías accesibles que permitan cumplir con el mandato de las leyes. El campo de la interacción humano-computador ha dado un gran aporte en este sentido. Las siguientes tres subsecciones presentan guías de accesibilidad para software y otras tecnologías de información y comunicación.

Debido a que en el desarrollo de la interfaz entre el ser humano y la tecnología participan no solo profesionales en computación e informática, sino también diseñadores gráficos, comunicadores, especialistas en multimedios, sociólogos y psicólogos, entre otros, la información presentada en las siguientes subsecciones puede ser de gran utilidad para todos.

Guías de accesibilidad generales

Idealmente, durante el diseño de un proyecto se debe seguir un proceso con el fin de que un producto:

1. Sea usable para las personas con el mayor rango de habilidades posible.
2. Funcione en el rango más amplio de situaciones.
3. Sea comercialmente viable.

Cuando estas tres características se cumplen, se habla de diseño universal. Son varios los principios que, de seguirse, sirven para producir un producto que cualquier persona pueda usar sin necesidad de adaptaciones posteriores. Estos principios, todos aplicables al software, son los siguientes:

1. El producto ha de ser usable y asequible a un precio razonable para cualquier persona. Si se piensa en accesibilidad desde que se empieza a diseñar el producto, el costo no será significativamente más alto.
2. El producto se debe acomodar a personas con distintas habilidades y gustos. Por ejemplo, las aplicaciones ofrecen sistemas de ayuda para los usuarios novatos, aunque muy probablemente los expertos nunca los usen.
3. El diseño del producto debe ser fácil de entender, independientemente de la experiencia de los usuarios, de sus habilidades de lenguaje y su capacidad de concentración. Por ejemplo, las personas con discapacidad auditiva manejan un léxico muy reducido en comparación con quienes no la tienen; por tanto, es conveniente usar palabras sencillas y emplear consistentemente la misma palabra en lugar de sinónimos.
4. El producto debe mostrar la información que el usuario necesita saber, con independencia del ambiente y de cómo este afecte las habilidades sensoriales de la persona. Por ejemplo, cuando se vaya a realizar una

transacción irreversible, como una transferencia bancaria de una cuenta a otra, es importante que la persona reciba la advertencia a través de un texto que pueda leer y, a la vez, por medios que perciba por otros sentidos.

5. El producto debe ser tolerante al error, para permitir la recuperación cuando el usuario se equivoque mientras use el sistema. Por ejemplo, la posibilidad de revertir el efecto de haber presionado un botón (*undo*) es un caso en el cual el usuario puede recuperarse de un error o una acción involuntaria. Esto le da confianza a la persona y lo anima a experimentar y buscar la opción o comando que necesita en un menú o un conjunto de botones.
6. El producto ha de ser usado con el esfuerzo físico y mental mínimo. Por ejemplo, no se debe obligar al usuario a recordar qué hizo o digitó en la pantalla anterior, pues esto le impondrá una carga cognitiva muy pesada, la cual lo obligará a intentar recordar, retroceder para fijarse en lo anterior o cometer un error. Se debe favorecer el reconocimiento antes que el recuerdo. Se debe tener en cuenta que una persona con discapacidad se puede fatigar más rápidamente.
7. El producto debe ser de un tamaño que permita a una persona utilizarlo. Por ejemplo, cuando las opciones no estén suficientemente separadas o sean muy pequeñas, un usuario con discapacidad motora no podrá seleccionar la opción correcta. Por tanto, además de equivocarse, podrá sentirse frustrado.

De forma más específica, según el tipo de discapacidad, se deben tomar en cuenta los siguientes aspectos:

1. Para las personas que no pueden distinguir colores se debe:
    a. Evitar codificar información importante únicamente por medio de colores. Por ejemplo: en

una página web, un enlace (*link*) a otra página se escribe en color celeste (codificado mediante colores), pero también se nota que el cursor adquiere forma de mano al pasar por encima. Se usa, entonces, doble codificación.

b. Utilizar colores distinguibles aún cuando una persona no pueda percibir uno o más colores. Algunos sitios web permiten a un desarrollador o un diseñador gráfico comprobar que dos colores son distinguibles, independientemente de la deficiencia que tenga el usuario (no distingue el rojo, el verde o el azul, o bien dos o tres colores).
c. Comprobar cómo se ve la pantalla bajo distintas condiciones de luz.

2. Para las personas con visión reducida, se recomienda:
   a. Usar fuentes de letras de ancho variable y combinación de mayúsculas y minúsculas, para dar la máxima diferenciación posible entre las letras y ayudar a distinguir el texto. Ello facilita encontrar una palabra buscada. Nótese la diferencia entre los dos ejemplos siguientes:
      - **Este es un ejemplo en el cual se usa una fuente de ancho variable y se combinan mayúsculas y minúsculas para aumentar la legibilidad.**
      - ESTE ES UN EJEMPLO EN EL CUAL SE USA UNA FUENTE DE ANCHO FIJO Y NO SE COMBINAN MAYÚSCULAS Y MINÚSCULAS Y POR ELLO BAJA LA LEGIBILIDAD.
   b. Evitar alinear el texto a la derecha, más conocido como justificarlo, pues el espacio insertado entre las palabras dificulta la lectura. La práctica de justificar el texto está muy extendida por estética; si se insiste en seguirla, puede recurrirse a un procesador de texto que permita la separación automática de palabras, con el fin de no generar espacio.
   c. Utilizar **en pantalla** tipos de letra sin terminaciones, más conocidas como *sans serif*, tal como Arial o

Verdana, y **en documentos impresos**, los tipos *serif*, como Times New Roman, pues así se facilita la lectura.

3. Para las personas no videntes se recomienda:
    a. Utilizar un canal distinto al visual. Por ejemplo, para dar instrucciones al computador, la persona puede usar su voz o un teclado braille. Para recibir la respuesta, es posible recurrir a la voz sintetizada.
    b. Proveer la opción de lectores de pantalla.
    c. Permitir el acceso a todas las opciones del software mediante teclado, en el caso de contar con uno.
4. En el caso de las personas con discapacidad auditiva, incluidos sordos, se requiere que los mensajes de riesgo y de alerta no sean codificados únicamente con sonido. Es necesario incluir un mensaje visual. Si se usa un video, se debe proveer la traducción a la lengua de señas costarricense (LESCO) o subtítulos.
5. Las personas sordas manejan un léxico reducido; por lo tanto, se recomienda evitar el uso de lenguaje innecesariamente complejo y de sinónimos; aunque vean una palabra o se les deletree, no sabrán su significado pues no serán capaces de reconocerla. Para ilustrar esta realidad, se tiene que en el más reciente diccionario de LESCO, del año 2013, se incluyen tan solo poco más de 1 100 entradas, que incluyen palabras y expresiones (Centro Nacional de Recursos para Educación Inclusiva, s. f.; Oviedo y Ramírez, 2013).
6. En el caso de las personas con movilidad reducida, es importante tener presente que se les puede dificultar el uso de un dispositivo apuntador, como el ratón, y de un teclado. Por esta razón, se recomienda usar un canal distinto para el ingreso de datos, como la voz, el rastreo ocular o movimientos del cuerpo.
7. Para las personas con discapacidad motora o cognitiva, se debe tomar en cuenta que pueden cansarse más

rápidamente. Por tanto, se recomienda crear software sencillo y fácil de usar, con el fin de evitar la fatiga.

Páginas web

Internet es una plataforma de oportunidades para las personas y las organizaciones; les permite socializar, adquirir bienes y servicios, trabajar a distancia e informarse, entre otros. No tener acceso a Internet significa estar en desventaja; por esa razón, es importante proveer accesibilidad a las páginas web.

Diseñar páginas web accesibles tiene ventajas para sus dueños. Es una forma de atraer más visitantes; no se puede olvidar que actualmente los competidores están en todo el mundo y las personas escogerán aquellas aplicaciones carentes de barreras. Además, no se necesitará corregir las páginas para adaptarlas a las necesidades de las personas con discapacidad, por lo cual bajarán los costos de mantenimiento.

En la actualidad existen guías muy completas sobre cómo hacer accesible una página web. El *World Wide Web Consortium* (W3C), comunidad internacional que desarrolla estándares para la web, creó la Iniciativa de accesibilidad web, más conocida como WAI por su nombre en inglés; el propósito de la WAI es crear estrategias, guías y recursos para lograr una web más accesible (World Wide Web Consortium, s. f.). La WAI ha desarrollado las muy reconocidas guías de accesibilidad, llamadas *Web Content Accessibility Guidelines* (WCAG) 2.0 (W3C, 2008). Dichas guías tienen como propósito hacer que una página web sea perceptible, operable, entendible y robusta. Por perceptible se entiende que quienes usen la página puedan percibir, por medio de alguno de los sentidos, la información y los componentes de la interfaz de usuario; por operable se refiere a que la persona que usa la página pueda navegar y utilizar los elementos de la interfaz; por entendible se refiere a que las personas puedan comprender los elementos mostrados y la forma en que

funciona la interfaz; finalmente, por robusta se entiende que el contenido de la página pueda ser interpretado por la tecnología que utilice la persona, ya sea un buscador (*browser*) de los comúnmente usados o una tecnología de asistencia (por ejemplo, software lector de pantalla). Algunas de las guías WCAG se listan a continuación (W3C, 2008).

1. La página web tiene un título para identificar su propósito.
2. Para el contenido que no sea texto (por ejemplo: gráficos y fotos), se usa el texto alternativo (atributo "alt") para indicar la función o describir dicho contenido.
3. Para videos con audio, se provee interpretación con lengua de señas.
4. Se utilizan varios medios para desplegar datos o mensajes de alerta, indicar una acción, pedir una respuesta o distinguir un elemento visual. Dichos medios pueden ser sonidos, colores e íconos, entre otros.
5. El tamaño del texto se puede ampliar hasta un 200 por ciento sin ser necesaria la tecnología de asistencia.
6. En video pregrabado, se evita el uso de sonido de fondo (por ejemplo: música) o se utiliza a muy bajo volumen para que no impida escuchar el mensaje.
7. Toda la funcionalidad de la página es operable desde una interfaz de teclado.
8. La página web no presenta elementos intermitentes (los cuales aparecen y desaparecen de la pantalla) más de tres veces por segundo.
9. La persona puede determinar el propósito de un enlace (*link*) con solo el texto de este.
10. El usuario debe saber su localización dentro de un conjunto de páginas.

Además, se puede comprobar el grado de cumplimiento de las guías de la WAI con la ayuda de herramientas de software. Incluso, es posible conseguir una certificación de accesibilidad para una página web, la cual indica el nivel de cumplimiento de las guías WCAG 2.0 en una fecha particular.

Existen otras guías de evaluación, tales como la norma española UNE 139801 Aplicaciones informáticas para personas con discapacidad. Requisitos de accesibilidad al ordenador. Hardware (Asociación Española de Normalización y Certificación, 2003).

Dispositivos móviles

En un principio, los teléfonos móviles eran simplemente teléfonos; en la actualidad, son verdaderas computadoras, al igual que lo son otros dispositivos, como las tabletas. Constituyen una herramienta para comunicarse, mantenerse informado, realizar transacciones bancarias y comerciales, jugar y decidir dónde almorzar, entre muchas otras posibilidades. Miles de aplicaciones están disponibles, en muchos casos gratuitamente, para que las personas las descarguen.

Existen tres tipos de aplicaciones móviles: web, nativas e híbridas. En el caso de una aplicación web, en el dispositivo móvil se despliega la misma página que se vería en un computador de escritorio; no siempre se ajusta al tamaño de la pantalla del dispositivo y los elementos de la interfaz pueden ser muy pequeños. Las aplicaciones nativas son creadas para un sistema operativo, por lo que aprovechan las características del hardware del dispositivo móvil; por lo general, su interfaz se ajusta al tamaño del dispositivo y los elementos en ella se distinguen bien. Las aplicaciones híbridas son una mezcla de aplicación web y nativa, pues son creadas con tecnología web (HTML), pero se incrustan en una ventana de navegador nativa; pueden funcionar en distintas plataformas (por ejemplo, IOS y Android), pero no sacan provecho de todas las características del dispositivo; tienen la

ventaja de que la interfaz se ajusta al tamaño de la pantalla como si fueran nativas. Independientemente del tipo de aplicación, es importante tener en mente el uso masivo de los dispositivos móviles y que es probable que muchas personas, con discapacidad o sin ella, los usen.

En cuanto a accesibilidad en dispositivos móviles, se trata de un tema más reciente, por lo cual no ha alcanzado tanta madurez como para las páginas web. La WAI ha presentado sus guías de accesibilidad para móviles, titulado *Mobile Accessibility: How WCAG 2.0 and Other W3C/WAI Guidelines Apply to Mobile* (W3C, 2015). En estas guías, se propone lo necesario para hacer una aplicación móvil perceptible, operable, entendible y robusta. Seguidamente se listan algunas de las recomendaciones de la WAI con respecto a cómo conseguir accesibilidad en dispositivos móviles (W3C, 2015):

1. La cantidad de información desplegada debe limitarse debido al tamaño reducido de la pantalla.
2. El tamaño de las letras y de los controles táctiles debe ser apropiado para que no sea necesario el uso de ampliadores de pantalla.
3. Las etiquetas se deben colocar arriba de los campos de ingreso de texto en lugar de al lado, para no hacer necesario desplazarse horizontalmente (*scroll*) en la pantalla.
4. El contraste debe poder ajustarse a las necesidades del usuario y a las condiciones del entorno, pues los dispositivos móviles se utilizan en una gran variedad de ambientes.
5. Los elementos de información más importantes se deben colocar en la parte superior de la pantalla, de modo que no haya necesidad de desplazarse verticalmente (*scroll*).
6. Los elementos tocables en la pantalla deben medir, al menos, 9 milímetros por 9 milímetros. Si el tamaño de

un elemento es muy cercano al tamaño mínimo sugerido, un espacio inactivo debe rodearlo.

7. El software debe funcionar independientemente de la posición en que el usuario coloque el dispositivo móvil, es decir, tanto en orientación vertical o retrato (*portrait*) como horizontal o paisaje (*landscape*).
8. En la aplicación se debe reducir el ingreso de texto. En lugar de esto, se deben utilizar menús, controles como los botones de opción o de radio (*radio buttons*) o las cajas de chequeo (*check boxes*), y el ingreso automático de datos conocidos.

Reflexión

¿Por qué deben los profesionales en computación e informática dar importancia al tema de la discapacidad? No se trata solo de cumplir la ley para evitar una sanción. Es necesario estar conscientes de que las personas con discapacidad tienen derecho a utilizar la tecnología fácilmente y de que la tecnología de información y comunicación debe ayudar a mejorar su calidad de vida. El costo de desarrollar herramientas tecnológicas accesibles no es tan alto cuando se considera el tema desde las etapas tempranas, pero sus beneficios sociales sí serán muchos: una sociedad sin discriminación que integra a todos sus habitantes es una sociedad más justa.

CAPÍTULO V
REDES SOCIALES

El sabio no dice nunca todo lo que piensa, pero siempre piensa todo lo que dice.

Aristóteles
Filósofo griego

Resumen

Las redes sociales, tal como se conocen actualmente, dan la posibilidad de publicar a un costo muy bajo, pero lo publicado en ellas no está exento de cumplir la normativa legal nacional. La libertad de expresión es un derecho constitucional que mucha gente hace efectivo especialmente mediante las redes sociales, usadas como medio de desahogo, crítica, burla y denuncia. Los comentarios negativos contra el empleador pueden tener consecuencias para quien los publica, algunas leves, como una sanción oral, y otras graves, como el despido. Es deber de todo trabajador mantener confidencialidad sobre el proceso productivo y administrativo del lugar en el cual labora. Las redes sociales deben administrarse con especial cuidado, para evitar que afecten la vida laboral.

Introducción

¿Ha sabido de una fotografía que le tomaron y publicaron en las redes sociales sin darse usted cuenta? ¿Recuerda los casos que han aparecido en la prensa sobre personas despedidas de su trabajo por publicar una fotografía en su

página de Facebook en la cual están vestidas con una determinada indumentaria?, ¿y el de la joven que habló mal de su jefe y que también fue despedida?, ¿o el estudiante de medicina que desató molestia en las redes sociales por desear, en su perfil, un mal al centro hospitalario en el cual realizaba su internado? Las publicaciones en redes sociales tienen consecuencias, especialmente en el contexto laboral.

El concepto de redes sociales no es nuevo. Desde hace varias décadas, en las escuelas de negocios se destacaba la importancia de crear la red social propia que le facilitara a una persona alcanzar sus objetivos en el ámbito laboral; sin embargo, las redes sociales con ayuda de tecnología de información son un fenómeno del siglo XXI. Estas han cambiado la forma de comunicarse y relacionarse, no solo de las personas, sino también de las organizaciones. A nivel personal, las redes sociales podrían considerarse un tema poco preocupante para los profesionales en computación e informática y también para los de otros campos. Sin embargo, tanto en el ámbito personal como de trabajo existen aspectos de interés para los profesionales.

Internet y, en particular, las redes sociales tal como se las concibe actualmente son una plataforma para expresarse utilizada con múltiples propósitos. Son una herramienta de divulgación de muy bajo costo. Grandes movimientos se han orquestado por medio de redes sociales. Cada vez más gente se une a ellas. Algunas redes se dirigen a un público meta con un cierto perfil, como profesionales o investigadores, mientras otras son abiertas a todo público.

Asimismo, hay quienes organizan redes para cometer actos ilícitos, para lo que se valen de la ingenuidad de los demás. Así, por ejemplo, se sabe de enormes redes de pederastia, las cuales operan a nivel mundial y reclutan a sus víctimas mediante redes sociales y otras herramientas TIC.

Las redes sociales conectan a la gente. Algunas personas logran crear redes sociales que pueden estar formadas por

cientos e incluso miles de contactos, a los cuales posiblemente no conozcan personalmente. Muchas utilizan las redes sociales para informar a los demás sobre sus actividades, expresar sus sentimientos y frustraciones, criticar, difamar o buscar reconocimiento.

En las organizaciones, el personal encargado de reclutar y seleccionar personas revisa lo que los candidatos publican para conocer más sobre ellos y finalmente decidir si los contratan o no. Sin embargo, esto transciende el momento en el cual las personas son contratadas. Se sabe de casos publicados en los medios de comunicación en los cuales una persona fue despedida porque reveló algo sobre su lugar de trabajo o publicó una imagen contraria a los valores de su empleador.

Los mensajes que una persona publica surten efectos sobre otras, pero ella no los ve; por esta razón, la gente se atreve a escribir lo que probablemente nunca tendría valor de decir en persona. Bajo pretexto de ejercer su derecho a la libertad de expresión, se publica contenido ofensivo para otros. Además, al enterarse tanta gente, el daño moral provocado a la víctima es todavía mayor y, en muchos casos, irreparable. Las personas parecen creer que existe impunidad en el ciberespacio; sin embargo, como se expondrá en este capítulo, no es así. Existe normativa para limitar el derecho a la libertad de expresión.

En este capítulo se da cobertura al tema de las redes sociales y la libertad de expresión en el lugar de trabajo. Por esto, primero se presenta la base jurídica de este derecho y sus límites, y posteriormente se tratan los aspectos legales de los comentarios negativos sobre el trabajo en las redes sociales y la obligación de la confidencialidad. Pese a no haber leyes creadas de forma específica para las redes sociales, la normativa legal nacional sí respalda las acciones a seguir cuando alguien sienta que sus derechos han sido afectados por una publicación.

El derecho de libertad de expresión y sus limitaciones

Los artículos 28 y 29 de la Constitución Política de Costa Rica garantizan el derecho de libertad de expresión, tal como se puede leer enseguida:

> Artículo 28. Nadie puede ser inquietado ni perseguido por la manifestación de sus opiniones ni por acto alguno que no infrinja la ley.
>
> Las acciones privadas que no dañen la moral o el orden público, o que no perjudiquen a tercero, están fuera de la acción de la ley. No se podrá, sin embargo, hacer en forma alguna propaganda política por clérigos o seglares invocando motivos de religión o valiéndose, como medio, de creencias religiosas.
>
> Artículo 29. Todos pueden comunicar sus pensamientos de palabra o por escrito, y publicarlos sin previa censura; pero *serán responsables de los abusos que cometan en el ejercicio de este derecho, en los casos y del modo que la ley establezca* [resaltado añadido].

Según el artículo 29, es claro que no existe la libertad de expresión absoluta, pues quien abuse de su derecho puede ser denunciado si alguien se siente ofendido. Al respecto, el *Código Penal* de Costa Rica contempla, en el libro II, título II, artículos 145 a 155, una serie de delitos contra el honor, los cuales incluyen injuria, calumnia y difamación. En estos artículos se establecen las penas para los casos en los cuales se haya abusado del derecho de libertad de expresión. Así, por ejemplo, el artículo 145 señala:

> Injurias
>
> Artículo 145. Será reprimido con diez a cincuenta días multa el que ofendiere de palabra o de hecho en su dignidad o decoro a una persona, sea en su presencia, sea por medio de una comunicación dirigida a ella.

> La pena será de quince a setenta y cinco días multa si la ofensa fuere inferida en público.

Además, 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.

El *Código Penal* también contempla el delito de suplantación de identidad, tanto de personas físicas como jurídicas y de marcas comerciales. Es relativamente muy fácil cometer este delito por medio de redes sociales; basta con crear un perfil falso de una persona o violentar la clave de su perfil legítimo. Ya esto se ha dado en Costa Rica, por ejemplo, los jóvenes que crean cuentas en redes sociales a nombre de compañeros de clase para acosarlos (*bullying*). Sobre suplantación de identidad, el artículo 230 del *Código Penal* indica:

> Artículo 230. Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información.

Aparte de esto, el libro I (“De las personas”), título II (“Derechos de la personalidad y nombre de las personas”) del *Código Civil* de Costa Rica introduce el concepto de derechos de la personalidad; estos son inherentes a la persona (Ochoa, 2006). Dichos derechos incluyen la

imagen, el nombre, la vida, las partes separadas de cuerpo y cadáver, el honor, la libertad, la intimidad y el derecho moral de autor (Bou y Pérez, 1977; Ochoa, 2006).

Mediante una publicación en redes sociales, ya sea texto o fotografía, se puede causar daño al honor de una persona. El artículo 47 del *Código Civil* limita el derecho a la libertad de expresión con respecto a la publicación de fotografías o imágenes de una tercera persona, tal como se lee enseguida:

> Artículo 47. La fotografía o la imagen de una persona no puede ser publicada, reproducida, expuesta ni vendida en forma alguna si no es con su consentimiento, a menos que la reproducción esté justificada por la notoriedad de aquélla *[sic]*, la función pública que desempeñe, las necesidades de justicia o de policía, o cuando tal reproducción se relacione con hechos, acontecimientos o ceremonias de interés público o que tengan lugar en público. Las imágenes y fotografías con roles estereotipados que refuercen actitudes discriminantes hacia sectores sociales no pueden ser publicadas, reproducidas, expuestas ni vendidas en forma alguna.

Nótese que hay excepciones en las cuales se permite la publicación de una foto sin consentimiento de la persona. Por ejemplo, en la sentencia 11715-2014 de la Sala Constitucional, en la cual una empresa periodística fue recurrida por publicar fotografías que mostraban las heridas de un privado de libertad muerto durante un intento de fuga, se expresa que el derecho a la propia imagen está limitado por otros derechos, tales como el de la comunicación de información y las libertades de expresión y creación artística. En este caso, la Sala Constitucional declaró sin lugar el recurso, pues los actos de violencia de los policías penitenciarios durante el intento de fuga se consideraron de interés público. Este es un ejemplo de una de las excepciones mencionadas en el artículo 47 del *Código Civil*.

Pese a lo establecido en el artículo 47, miles de fotografías son publicadas en redes sociales sin el consentimiento de quienes aparecen en ellas. El artículo 48 del *Código Civil* establece que un juez puede solicitar suspender la reproducción no justificada, según el artículo 47, de la imagen o fotografía de una persona. El artículo 48 indica:

> Artículo 48. Si la imagen o fotografía de una persona se publica sin su consentimiento y no se encuentra dentro de alguno de los casos de excepción previstos en el artículo anterior, aquella puede solicitarle al Juez como medida cautelar sin recursos, suspender la publicación, exposición o venta de las fotografías o de las imágenes, sin perjuicio de lo que resuelva en definitiva. Igual medida podrán solicitar la persona directamente afectada, sus representantes o grupos de interés acreditados, en el caso de imagen o fotografías que estereotipen actitudes discriminantes.

Una vez que alguien ha publicado un texto o una fotografía en Internet, otras personas pueden crear una copia y publicarla, por lo que es prácticamente imposible asegurar que su publicación se suspende. Por tanto, el posible daño moral a una persona puede prolongarse en el tiempo. A esto se une el hecho de que mucha gente podría haber visto lo publicado, debido al efecto viral conseguido con las redes sociales y otras tecnologías de información y comunicación.

La ley costarricense contempla el derecho a que la víctima sea indemnizada cuando sienta que la lesión a sus derechos de la personalidad ha causado un daño moral, tal como lo menciona el artículo 59 del *Código Civil*. Esta indemnización es adicional a la posible pena impuesta por la vía penal para el acto delictivo correspondiente. Suplantar una identidad, lo cual pena el artículo 230 del *Código Penal* con prisión de uno a tres años, puede lesionar los derechos de la personalidad; por lo tanto, podría también implicar una indemnización para la víctima.

Comentarios negativos sobre el trabajo en redes sociales

Son varios los casos que han trascendido a los medios de comunicación en los cuales a una persona se le abre un procedimiento administrativo o, incluso, es despedida por algo que publicó en su red social. A veces, los valores presentes en la publicación son contrarios a los de la organización en la cual labora o los de la sociedad, pero, en otras, se expresa desacuerdo con lo que el patrono hizo o dijo; al enterarse, el empleador reacciona. Sin embargo, las acciones del patrono en contra de sus empleados, como consecuencia de sus publicaciones, algunas veces son inconstitucionales.

La Sala Constitucional es la encargada de resolver los recursos de amparo puestos por los trabajadores que consideran su derecho a la libertad de expresión lesionado. Cada caso es único, por lo cual la Sala Constitucional emite un criterio con base en las circunstancias particulares. Seguidamente se muestran resúmenes de tres sentencias de casos relacionados con este tema. La sentencia 7500-2015 trata sobre un procedimiento administrativo contra un funcionario por las publicaciones en su red social; la sentencia 11855-2014, acercade las normas de una institución respecto a la difusión de comentarios que la afecten o desprestigien; y la sentencia 1806-2015, sobre un despido por declaraciones publicadas. Con estas, se pueden ilustrar los límites de la libertad de expresión en el contexto laboral.

1. **Procedimiento administrativo contra un funcionario por comentarios en red social**
   Sentencia 7500-2015

   Recurso de amparo contra una municipalidad. El recurrente alegó haber publicado en la red social

Facebook, una serie de comentarios negativos sobre la calidad de los jefes del Gobierno local y por esa razón se le abrió un procedimiento administrativo, pese a que de sus comentarios no se concluyó un ataque personal hacia los recurridos; el recurrente estimó que los hechos acusados violentaban sus derechos fundamentales. Se declaró con lugar el recurso, por vulnerar los artículos 28 y 29 de la Constitución Política. En consecuencia, se anuló el procedimiento administrativo tramitado en contra del recurrente por causa de las manifestaciones hechas en su perfil de Facebook el 26 de marzo de 2015.

2. **Libertad de expresión de funcionarios públicos**
   Sentencia 11855-2014

Recurso de amparo contra la Decanatura del Colegio Universitario de Cartago, puesto por docentes en propiedad en el Colegio Universitario de Cartago (CUC). Los recurrentes señalaron que, por medio del comunicado DEC-569-2014 del 27 de junio de 2014, la Decanatura del CUC indicó que "aquellos funcionarios docentes o administrativos, así como estudiantes, usuarios y particulares que realicen acciones o manifestaciones públicas en forma oral, escritas o por Internet de las redes sociales, que desprestigien o afecten públicamente la fama, buen nombre o la imagen del Colegio Universitario de Cartago, con sus declaraciones pueden ser denunciados ante las autoridades del CUC y la Institución realizará contra los sujetos infractores las acciones judiciales para que se sienten las responsabilidades por los daños y perjuicios generados, en protección del buen nombre y prestigio del CUC". Los recurrentes señalaron en dicho comunicado la finalidad de amenazar con represalias y censurar de forma previa. Alegan que de esta forma se lesionan sus derechos a la libertad de expresión, de cátedra, a la información,

petición y de estabilidad laboral, entre otros, al pretender callar e intimidar a los funcionarios para que no denunciaran actos corruptos. Se declaró sin lugar el recurso.

3. **Despido de embajadora por declaraciones en Facebook**
   Sentencia 1806-2015

Recurso de amparo contra el Presidente de la República de Costa Rica. La recurrente manifestó que fue despedida de su puesto de embajadora de Bolivia por las declaraciones publicadas en su cuenta de Facebook que se relacionaban con la Procuradora de la República. La Sala Constitucional consideró que el nombramiento y la remoción de los miembros del Servicio Exterior de la República de Costa Rica están regulados especialmente en el *Estatuto del Servicio Exterior de la República.* Por tanto, este Tribunal no encontró violación a derecho constitucional alguno. Es razonable que los embajadores y miembros del servicio exterior, en la medida que cumplen la función de mantener buenas relaciones con los Gobiernos ante los cuales se encuentran acreditadas las misiones diplomáticas, estén obligados a expresarse con la prudencia debida conforme a los criterios del Poder Ejecutivo. El motivo del despido no fue un padecimiento de salud ni una incapacidad, sino, como lo admitió la misma recurrente, sus declaraciones en su página de Facebook, no compartidas por el Poder Ejecutivo; este consideró que lo publicado afectaba las relaciones con el Estado Plurinacional de Bolivia. La funcionaria ostentaba un puesto de confianza, por lo cual es de libre nombramiento y remoción. La causa del despido no radicó en la incapacidad de la recurrente ni aludió a una enfermedad específica, por lo que no se advirtió lesión a derecho

constitucional alguno y, por consiguiente, se rechazó el recurso.

Confidencialidad en el trabajo

Muchas veces, la frustración o el enojo hace que las personas busquen el desahogo en las redes sociales, sin pensar si violan su compromiso de confidencialidad para con el patrono ni si alguien en el círculo laboral puede acceder a sus publicaciones. En los contratos de trabajo que firman los profesionales en computación e informática, es común encontrar una cláusula de confidencialidad. Sin embargo, no es necesaria su existencia para que un empleado tenga esta obligación, pues los artículos 71 y 81 del *Código de Trabajo* de Costa Rica la contemplan de forma previa. A continuación, se transcriben el artículo 71, inciso g, y el artículo 81, inciso e de esta ley.

> Artículo 71. Fuera de las contenidas en otros artículos de este Código en sus reglamentos y en sus Leyes supletorias o conexas, son obligaciones de los trabajadores
>
> g) Guardar rigurosamente los secretos técnicos, comerciales o de fabricación de los productos a cuya elaboración concurran directa o indirectamente, o de los cuales tengan conocimiento en razón del trabajo que ejecuten; así como de los asuntos administrativos reservados, cuya divulgación pueda causar perjuicios al patrono;
>
> Artículo 81. Son causas justas que facultan al patrono para dar por terminado el contrato de trabajo:
>
> e) Cuando el trabajador revele los secretos a que alude el inciso g) del artículo 71.

Nótese entonces que por divulgar información en redes sociales u otros medios, un profesional puede perder su

trabajo sin responsabilidad patronal, es decir, sin recibir prestaciones ni auxilio de cesantía.

Adicionalmente, la *Ley 7975 de Información No Divulgada* norma la confidencialidad en las relaciones laborales y comerciales. Esta ley se relaciona con secretos comerciales e industriales; estos son materia de derechos de propiedad intelectual. El artículo 7 de dicha ley señala:

> Artículo 7. Confidencialidad en las relaciones laborales o comerciales. Toda persona que con motivo de su trabajo, empleo, cargo, desempeño de su profesión o relación de negocios, tenga acceso a información no divulgada en los términos señalados en el primer párrafo del artículo 2 de esta ley y sobre cuya confidencialidad se le haya prevenido en forma expresa, deberá abstenerse de usarla o divulgarla sin consentimiento del titular, aun cuando su relación laboral, el desempeño de su profesión o la relación de negocios haya cesado.
>
> En los contratos por los que se transmiten conocimientos técnicos especializados, asistencia técnica, provisión de ingeniería básica o tecnologías, podrán establecerse cláusulas de confidencialidad para proteger la información no divulgada que reúnan las condiciones referidas en el primer párrafo del artículo 2 de la presente ley.
>
> Una ley posterior regulará las responsabilidades dispuestas en el presente artículo.

Por último, en cuanto a la confidencialidad de lo sucedido en el trabajo, el artículo 11 de la *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales* establece la exigencia del secreto profesional a todas las personas participantes en el proceso de tratamiento de los datos. Por tanto, la confidencialidad es fundamental para los profesionales en computación e informática que participan en este proceso. El artículo 11 indica:

> Artículo 11. Deber de confidencialidad. La persona responsable y quienes intervengan en cualquier fase del tratamiento de datos personales están

> obligadas al secreto profesional o funcional, aun después de finalizada su relación con la base de datos. La persona obligada podrá ser relevado [*sic*] del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce.

Lo más conveniente para una persona es mantener toda información sobre su trabajo fuera de las redes sociales.

A pesar de la existencia de normativa legal que limita la libertad de expresión de una persona respecto a lo acontecido en su trabajo, es conveniente para toda organización definir y difundir su política de confidencialidad.

Reflexión

Una de las virtudes obligatorias para todo profesional es pensar antes de expresarse. Aunque la tentación de publicar los pensamientos en la red social personal puede ser muy fuerte, no se debe olvidar que parte del profesionalismo es mantener la confidencialidad sobre lo visto, oído y hecho en el lugar de trabajo. Sin embargo, nunca se debe olvidar la responsabilidad de un profesional para con la sociedad. Si se ha de denunciar algo, existen otras vías, probablemente más indicadas para hacerlo que las redes sociales.

Conclusiones

La justicia es la constante y perpetua voluntad de dar a cada uno su derecho.

Domicio Ulpiano
Jurista romano de origen fenicio

El campo de la computación e informática se ejerce dentro de un marco jurídico que tiene por objetivo proteger los derechos de las personas usuarias de software y otras tecnologías de información y comunicación. La existencia de normativa no garantiza el respeto de los derechos; las razones para ello son varias. Por ejemplo, aunque en Costa Rica no se puede alegar desconocimiento de la ley, puede ocurrir que quienes tengan el deber de hacerla cumplir ni siquiera sepan de su existencia. Aunque no fuera este el caso, hace falta la voluntad de cumplirla.

No siempre se es consciente de la importancia de los derechos que la Constitución Política de Costa Rica y otra normativa otorgan a las personas. Además de muy extensa, diversa e intrincada, la legislación es difícil de comprender e interpretar por la complejidad de los temas en sí y por el lenguaje en el cual está escrita. Por esta razón, no es fácil identificar aquellas secciones de la ley pertinentes en un determinado caso. Aunado a esto, la normativa relacionada con el ejercicio profesional de la computación e informática es difícil de hacer cumplir. Por ejemplo, no es tarea fácil demostrar que se ha cometido un delito informático.

A pesar de todo lo anterior, para que el marco jurídico en el cual se desenvuelven los profesionales en computación e informática se cumpla, es necesario, en primer lugar, darlo a conocer en palabras comprensibles. Con esta obra se ha intentado alcanzar este propósito.

Los temas elegidos para este libro no son los únicos que atañen a los profesionales en computación e informática, pero son comunes a prácticamente todo el gremio. En cuanto a cada uno de ellos, es posible afirmar lo siguiente:

1. La privacidad, derecho fundamental, está seriamente amenazada por el uso extensivo de tecnologías de información y comunicación. El valor de los datos personales es tan alto para las organizaciones, que estas utilizan todos los recursos disponibles para obtenerla. En Costa Rica se han dado los primeros pasos para dar la debida importancia a la protección de datos, pero todavía queda un largo camino por recorrer. La legislación define el derecho a la autodeterminación informativa, es decir, que una persona pueda ejercer un control sustancial de sus datos personales y el uso que se les da. Lo más notable de la normativa existente es que eleva la autodeterminación informativa a la categoría de derecho fundamental. Sin embargo, derechos tan importantes como el de prohibir la interconexión de archivos y el de impugnar valoraciones basadas solo en datos procesados automáticamente aún no se incluyen en la *Ley 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales.* Es importante considerar integrar estos dos derechos en la normativa legal.

   Aunado a esto, los artículos de la ley de delitos informáticos relativos a violaciones a la privacidad establecen penas más altas para los profesionales en computación e informática que tengan a cargo la administración o el apoyo técnico de los sistemas o redes informáticas. Ellos difícilmente podrían alegar desconocimiento de sus actos y sus implicaciones.
2. La seguridad está relacionada de forma estrecha con la privacidad; prácticamente se puede afirmar que no

es posible la privacidad sin seguridad, aunque un exceso de la segunda puede ir en detrimento de la primera. La seguridad es responsabilidad tanto de usuarios como de profesionales en computación e informática. Sin embargo, la jurisprudencia costarricense ha dejado clara la responsabilidad de las organizaciones si existe un riesgo intrínseco al negocio, es decir, son responsables aún sin tener la culpa de un delito. Esto representa un incentivo para mejorar la seguridad en todas las organizaciones que custodian bienes de terceros.

En la ley de delitos informáticos se utilizan muchos verbos técnicos en un solo artículo, lo cual significa que muchas acciones distintas se agrupan en un solo tipo penal. No todas estas acciones requieren del mismo conocimiento, causan el mismo impacto ni ofrecen el mismo grado de dificultad. Si se toma en cuenta el estado actual de la legislación, corresponde a un juez comprender el impacto y la dificultad de una posible acción informática delictiva para determinar la pena. Por tanto, es conveniente realizar un análisis del grado de conocimiento, complejidad y daño posible de cada acción delictiva y una diferenciación de las penas de acuerdo con estos aspectos, con el objetivo de facilitar la aplicación de la ley.

Asimismo, la aprobación de parte de la Asamblea Legislativa de convenios internacionales sobre ciberseguridad es una tarea pendiente; la posibilidad de cooperación internacional y asistencia mutua en caso de ocurrir un delito informático y de ser necesario obtener pruebas en el extranjero es muy importante para Costa Rica.

3. En cuanto a la propiedad intelectual del software, tema complejo por sus características, lo más importante es la existencia de un marco jurídico muy

amplio; este debe ser respetado, aun si mucha gente no está de acuerdo. Lo relevante es que quienes crean software cuentan con instrumentos para protegerlo y determinar cómo quieren compartirlo con los demás; este es un derecho que se debe respetar.

En Costa Rica, el código del software se protege mediante derechos de autor, pero existen otros mecanismos de protección para otros elementos, tales como los diseños de la interfaz gráfica y la marca, los cuales son importantes para la usabilidad y la comercialización. Sin embargo, proteger software aislado por medio de patentes no está permitido en Costa Rica.

Aparte de esto, quienes adquieren software deben conocer las limitaciones que les imponen los mecanismos y las medidas tecnológicas de protección establecidas por los productores, para evitar cometer un delito que ponga en riesgo su continuidad y afecte su imagen pública.

El Tratado de Libre Comercio República Dominicana-Centroamérica-Estados Unidos es el mecanismo por medio del cual Estados Unidos introdujo su normativa legal sobre propiedad intelectual en la de otros países. Por causa del énfasis de aquella en el resguardo de las medidas de protección tecnológica, en la actualidad los usuarios de software corren el riesgo de que no se respeten las excepciones que no constituyen violaciones a los derechos de autor.

4. La discapacidad, vista actualmente como el resultado de la interacción con un contexto que impone a las personas barreras limitantes para sus posibilidades de actuar, atañe a los profesionales en computación e informática y a todas las demás personas participantes en el proceso de diseño y desarrollo de tecnologías de información y comunicación; estos

tienen en sus manos la posibilidad de crear tecnologías que abran oportunidades a quienes no las tendrían de otra forma. De esta manera, se le garantiza el cumplimiento de sus derechos como, por ejemplo, el de acceso a la información o al trabajo, a un grupo de personas mayor al 10 por ciento de los habitantes de Costa Rica, el cual crecerá conforme avance el envejecimiento demográfico.

Aunque la legislación sobre discapacidad no impone multas ni penas por su incumplimiento, quienes consideren lesionados sus derechos pueden recurrir a la Sala Constitucional para hacerlos valer. Las sentencias de esta Sala son vinculantes.

La accesibilidad de los productos se debe tomar en cuenta desde la primera etapa de desarrollo, para lograr que sean tanto accesibles como asequibles. La participación de personas con discapacidad es una práctica poco común en Costa Rica pero muy conveniente, pues se pueden conocer sus necesidades de primera mano e incorporar requerimientos específicos para ellas. No se trata solo de cumplir con la normativa legal sobre este tema, sino de ser solidario con un grupo de personas del cual se puede pasar a formar parte en cualquier momento.

5. En cuanto a redes sociales y libertad de expresión, si bien no hay leyes específicas, sí existe suficiente normativa que limita lo que se puede publicar en general y sobre el ámbito de trabajo. Las organizaciones pueden limitar los comentarios que publican sus trabajadores; además, la violación de la confidencialidad puede ser causa de despido. En particular, todas las personas participantes en un proceso de tratamiento de datos deben mantener el secreto profesional. La prudencia debe predominar en el momento de publicar opiniones.

Sin lugar a dudas, la legislación existente en Costa Rica constituye un gran paso. Sin embargo, es necesario actualizarla y ampliarla de manera ágil, pues la tecnología avanza a pasos gigantescos y son cada vez más los ámbitos de las actividades humanas en los cuales se introduce. Esto da lugar a nuevas condiciones, tanto positivas como negativas, que están fuera del ámbito de la legislación actual.

A lo largo de esta obra, se ha mencionado la necesidad de contar con estrategias y políticas en cada uno de los temas tratados en las organizaciones que diseñan y desarrollan tecnologías de información y en las que las adquieren y usan. La capacidad de convencimiento de los profesionales en computación e informática es necesaria para lograr establecerlas, pues esto requiere de esfuerzo y recursos financieros y materiales. Por lo tanto, el convencimiento y el apoyo de quienes toman decisiones en las organizaciones son fundamentales. No basta con saber qué se debe hacer y cómo; además se necesita la voluntad política para lograrlo.

Los profesionales en computación e informática han estudiado poco el tema del marco jurídico de la profesión informática en Costa Rica. Deben existir más esfuerzos para lograr que campos multidisciplinarios, como el derecho informático, sean de interés para los creadores de tecnologías de información y comunicación.

Para terminar, este es el mensaje final para todas las personas profesionales en computación e informática: tienen en sus manos la posibilidad de garantizar el cumplimiento de los derechos de los demás, pero no lo hagan solo porque la ley lo indica, sino por el sentimiento de responsabilidad y solidaridad propio del ser humano.

Bibliografía

Agencia de Protección de Datos de los Habitantes. (2014). *Preguntas frecuentes de empresa*. Recuperado de http://www.prodhab.go.cr//preguntas-frecuentes/?empresas

Anderson, R. (2001). Why information security is hard – An Economic Perspective. En *Proceedings of the 17th Annual Computer Security Applications Conference* (pp. 358-365). Washington D.C., Estados Unidos: IEEE Computer Society.

Araya, A. (16 de abril del 2004). *Circular RDADC-04-2004*. Recuperado de http://www.registronacional.go.cr/derechos_autor/Documentos/DA_Normativa/DA_Circulares_Criterios/DA_Circulares_2004.pdf

Asamblea Legislativa. (30 de junio del 2014). Expediente Legislativo: Código Procesal Civil. *Alcance Digital No. 32, La Gaceta.* Recuperado de https://www.imprentanacional.go.cr/pub/2014/06/30/ALCA32_30_06_2014.pdf

Asociación Española de Normalización y Certificación. (2003). *Norma UNE 139801:2003. Aplicaciones informáticas para personas con discapacidad. Requisitos de accesibilidad al ordenador. Hardware.* Recuperado de http://www.aenor.es/DOCUMENTOS/NORMALIZACION/NORMASNACIONALES/EXTRACTOS/(EX)UNE_139801=2003.pdf

Ávalos, A. (4 de octubre del 2015). Director de la Agencia de Protección de Datos: ´Protección de datos en Costa Rica está en fase embrionaria´. *La Nación*, p. 8A.

Avižienis, A.; Laprie, J. C. y Randell, B. (2001). *Fundamental concepts of dependability*. Newcastle upon Tyne: University

of Newcastle upon Tyne.

Baase, S. (2012). *A gift of fire: social, legal, and ethical issues for computing technology.* Boston, Estados Unidos: Prentice Hall.

Badilla, A. E. (2007). Derechos fundamentales y derechos humanos en Costa Rica. Alcances particulares en relación con los derechos de las personas con VIH. *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades,* 9 (17), 151-165.

Bou, Z. y Pérez, V. (1977). *Los valores fundamentales de la personalidad y sus medios de tutela.* San José: Editorial Universidad de Costa Rica.

Business Software Alliance. (s. f.). *Acerca de BSA*. Recuperado de http://www.bsa.org/about-bsa/careers

Centro de Información Jurídica en Línea. (s. f.). *Responsabilidad objetiva de los bancos por delitos informáticos.* Recuperado de http://www.asamblea.go.cr/Centro_de_informacion/biblioteca/Centro_Dudas/Lists/Formule%20su%20pregunta/Attachments/392/1398-RESPONSABILIDAD_OBJETIVA_DE_LOS_BANCOS_POR_DELITOS_INFORMATICOS_(4-08)[1].pdf **vínculo removido del servidor**

Centro Nacional de Recursos para la Educación Inclusiva. (2011). *Lengua de Señas Costarricense (LESCO).* Recuperado de http://cenarec-lesco.org/DiccionarioLESCO.php

Chen, S. (2010). "Privacidad y protección de datos: un análisis de legislación comparada". *Diálogos Revista Electrónica de Historia,* 11 (1). Recuperado de http://www.redalyc.org/pdf/439/43915696004.pdf.

Chirino, A. y Carvajal, M. (s. f.). *El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica.* Recuperado de http://www.ocw.uned.ac.cr/eduCommons/s.e.p/tecnologia

-y-trabajo/tutorias/tutoria-segunda/el-camino-hacia-la-regulacion-normativa-del-tratamiento-de-datos-personales-en-costa-rica-alfredo-chirino. **vínculo removido del servidor**

Clarke, R. (2006). *What's 'privacy'?* Recuperado de http://www.rogerclarke.com/DV/Privacy.html

Corvet, J. (2008). *How to participate in the Linux community. A guide to the kernel development process.* Recuperado de https://www.linux.com.

Díaz, A. (2008). *América Latina y el Caribe: la propiedad intelectual después de los tratados de libre comercio.* Santiago, Chile: Comisión Económica para América Latina y el Caribe.

Escoto, C. M. (s. f.). *Procedimientos de observancia en materia de derechos de propiedad intelectual y de comercio en Costa Rica.* Recuperado de http://www.wipo.int/edocs/mdocs/enforcement/es/wipo_ace_2/wipo_ace_2_www_33725.pdf

Finn, R. L.; Wright, D. y Friedewald, M. (2013). Seven types of privacy. En S. Gutwirth, R. Leenes, P. de Hert y Y. Poullet (Eds.), *European Data Protection: Coming of Age* (pp. 3-32). Dordrecht: Springer Science+Business Media.

Hess, C. (2004). *La dimensión jurídica del software: naturaleza, tutela jurídica, contratos y responsabilidad.* Recuperado de https://dl.dropboxusercontent.com/u/3863866/dimension.pdf **vínculo removido del servidor.**

Hess, C. (2015). *Normativa de Derecho informático.* Recuperado de http://hess-cr.blogspot.com/p/normativa-de-derecho-informatico.html **vínculo removido del servidor.**

Instituto Nacional de Estadística y Censos. (2012). *X Censo Nacional de Población y VI de Vivienda: Resultados Generales Censo 2011.* San José, Costa Rica.

Karyda, M.; Gritzalis, S. y Park, J. (2007). A critical approach to privacy research in ubiquitous environments – Issues and underlying assumptions. En M. K. Denko, *et al.* (Eds.), *Emerging Directions in Embedded and Ubiquitous Computing* (pp. 12-21). Heidelberg: Springer.

Lemaitre, R. (2011). *Manual sobre delitos informáticos.* San José, Costa Rica: Investigaciones Jurídicas, S.A.

Lobo, L. D. (s. f.). *Cooperación internacional para el cumplimiento de los derechos de las personas con discapacidad. Acercamiento al informe país acerca del cumplimiento de la Convención Internacional de los derechos de las personas con discapacidad.* Recuperado de http://issuu.com/cn7600/docs/cooperacion-internacional-para-cumplimiento-dhpcd

Ministerio de Comercio Exterior de Costa Rica. (s. f.). *Tratados vigentes.* Recuperado de http://www.comex.go.cr/tratados/index.aspx **vínculo removido del servidor**

Miró, F. (2011). La Oportunidad Criminal en el Ciberespacio, Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología,* 13(07). Recuperado de http://criminet.ugr.es/recpc/13/recpc13-07.pdf

Mora, T. y Guzmán, J. A. (2008). *Análisis de las Deficiencias de la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, sus Implicaciones en el Código Notarial y una propuesta de reforma para su implementación* (Tesis de Licenciatura en Derecho). Universidad de Costa Rica, San José.

Ochoa, O. (2006). *Personas: Derecho Civil I.* Caracas: Universidad Católica Andrés Bello.

Organización de Estados Americanos. (1999). *Convención Interamericana de la Eliminación de todas las Formas de*

Discriminación contra las Personas con Discapacidad. Recuperado de http://www.dgri.sep.gob.mx/formatos/4_oea_11.pdf **vínculo removido del servidor**

Organización Mundial del Comercio. (s. f.). *Entender la OMC: los acuerdos. Propiedad intelectual: protección y observancia.* Recuperado de https://www.wto.org/spanish/thewto_s/whatis_s/tif_s/agrm7_s.htm

Organización Mundial de la Propiedad Intelectual. (1978). *Guía del Convenio de Berna para la protección de obras literarias y artísticas.* Ginebra, Suiza.

Organización Mundial de la Propiedad Intelectual. (1996). *Reseña del Tratado de la OMPI sobre Derecho de Autor.* Recuperado de http://www.wipo.int/treaties/es/ip/wct/summary_wct.html

Organización Mundial de la Propiedad Intelectual. (s. f.). *What is intellectual property?* Recuperado de http://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf

Organización Mundial de la Salud. (2001). *CIF Clasificación internacional del funcionamiento, la discapacidad y la salud.* Recuperado de http://conadis.gob.mx/doc/CIF_OMS.pdf **vínculo removido del servidor.**

Organización Mundial de la Salud. (2014). *Discapacidad y salud. Nota descriptiva N° 352.* Recuperado de http://www.who.int/mediacentre/factsheets/fs352/es/

Oviedo, A. y Ramírez, C. (2013). Das Projekt LESCO. Entstehung und Durchführung eines Forschungsprojekts für eine erste Beschreibung der Costa-ricanischen Gebärdensprache (2011-2013). *Das Zeichen,* 27(95), 358-364.

París, A. y Zamora J. I. (2015). *Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Comentada y*

anotada. San José, Costa Rica: Editorial Jurídica Continental.

Programa Sociedad de la Información y el Conocimiento. (2006). Marco regulatorio de la sociedad de la información y el conocimiento en Costa Rica. En *Informe 2006 Hacia la Sociedad de la Información y el Conocimiento* (pp. 43-86). Recuperado de http://www.prosic.ucr.ac.cr/informe-2006

Programa Sociedad de la Información y el Conocimiento. (2008). Comercio electrónico en Costa Rica. En *Informe 2008 Hacia la Sociedad de la Información y el Conocimiento* (pp. 185-216). Recuperado de http://www.prosic.ucr.ac.cr/informe-2008

Programa Sociedad de la Información y el Conocimiento. (2011). TIC y personas con discapacidad en Costa Rica. En *Informe 2011 Hacia la Sociedad de la Información y el Conocimiento* (pp. 295-329). Recuperado de http://www.prosic.ucr.ac.cr/informe-2011

Quesada, L. (29 de setiembre del 2008). *Oficio N° 09650-2008-DHR Informe especial. Fraudes electrónicos: la responsabilidad de los bancos del Estado*. San José, Defensoría de los Habitantes.

Registro Nacional. (s. f.). *Historia Institucional*. Recuperado de http://www.registronacional.go.cr/Institucion/index.htm

Reig, D. (2012). *Socionomía ¿Vas a perderte la revolución social?* Bilbao, España: Ediciones Deusto.

Shapiro, C. y Varian, R. (1999). *Information rules. A strategic guide to the network economy*. Boston, Massachusetts: Harvard Business School Press.

Sistema Nacional de Certificación Digital. (s. f.). *Firma digital*. Recuperado de http://www.firmadigital.go.cr

Tapscott, D. y Williams, A. D. (2006). *Wikinomics: how mass colaboration changes everything*. Nueva York: Penguin

Group.

The Apache Software Foundation. (2017). *Apache HTTP Server 2.4.27 Released.* Recuperado de https://www.apache.org/dist/httpd/Announcement2.4.html

Unión Internacional de las Telecomunicaciones. (2007). *Guía de ciberseguridad para los países en desarrollo.* Recuperado de http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-s.pdf

Vargas, M. (14 de octubre del 2015). CR Texter facilita búsquedas en línea para personas ciegas. *La Nación,* p. 15A.

Vargas, M. (12 de marzo del 2017). Costarricense contribuye a elevar calidad de los subtítulos de videos en Youtube. *La Nación,* p. 15A.

Viega, M. J. y Rodríguez, B. (2005). *Documento electrónico y firma digital: cuestiones de seguridad en las nuevas formas documentales.* Montevideo: Vega & Asoc.

Wiederhold, G. (2014). *Valuing intellectual capital: multinationals and taxhavens.* Dordrecht: Springer Science+Business Media.

World Wide Web Consortium. (2008). *Web content accessibility guidelines (WCAG) 2.0.* Recuperado de http://www.w3.org/TR/WCAG20/

World Wide Web Consortium. (2015). *Mobile accessibility: how WCAG 2.0 and other W3C/WAI guidelines apply to mobile. W3C First Public Working Draft.* Recuperado de http://www.w3.org/TR/mobile-accessibility-mapping/

World Wide Web Consortium. (s. f.). *Getting started with web accessibility.* Recuperado de http://www.w3.org/WAI/gettingstarted/Overview.html

Índice de cuadros

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.

Notas

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

Ficha catalográfica y créditos

343.728.609.99
Cl46m
Calderón Campos, Marta Eunice, 1965-
Marco jurídico de la profesión informática en Costa Rica /
Marta Eunice Calderón Campos. – 1. edición – [San José, Costa Rica]: Editorial UCR, 2019
1 recurso en línea (xiv, 183 páginas): digital, archivo de texto, ePub; 593 KB

ISBN 978-9968-46-792-6

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/3407
CC/SIBDI.UCR

Edición aprobada por la Comisión Editorial de la Universidad de Costa Rica.
Primera edición impresa: 2018.
Primera edición digital (ePub): 2019

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 de la versión impresa: *Raquel Fernández C. y Grettel Calderón A.* • Diseño de portada: *Priscila Coto M.* • Realización de ePub: *Hazel Aguilar B.* • Control de calidad de la versión digital: *Elisa Giacomin V.*

Edición digital de la Editorial Universidad de Costa Rica. Fecha de creación: setiembre, 2019.

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

Valoramos su opinión. Por favor comente esta obra

Licencia de tipografías

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and

open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives,however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

DEFINITIONS

“Font Software” refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

“Reserved Font Name” refers to any names specified as such after the copyright statement(s).

“Original Version” refers to the collection of Font Software components as distributed by the Copyright Holder(s).

“Modified Version” refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

“Author” refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.

2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.

3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding

Copyright Holder. This restriction only applies to the primary font name as presented to the users.

4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The

requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.