RED ACADÉMICA INTERNACIONAL DE

PROTECCIÓN DE DATOS PERSONALES

Revista Internacional de Protección de Datos Personales

La Ley de Protección de Datos de Costa Rica. Luces en las sombras.

Alfredo Chirino Sánchez

Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia)
No. 1 Julio - Diciembre de 2012. ISSN: 2322-9705

La Ley de Protección de Datos de Costa Rica. Luces en las sombras

Alfredo Chirino Sánchez[1]

Abstract

The Data Protection Act 2011 is the recently enacted legislation which defines costarican law on the processing of data on identifiable living people. It is the main piece of legislation that governs the protection of personal data in Costa Rica. Although the Act itself does mention privacy and the right to information self-determination, it was enacted to bring costarican law into line with the modern tendencies to protect people's fundamental rights and freedoms and in particular their right to privacy with respect to the processing of personal data. In practice it provides a way for individuals to control information about themselves. Anyone holding personal data for other purposes is legally obliged to comply with this Act, subject to some exemptions. The Act defines eight data protection principles. It also requires companies and individuals to keep personal information to them-

Resumen

La Ley de Protección de Datos del 2011 es la legislación recientemente puesta en vigencia, que define las condiciones jurídicas del procesamiento de datos de personas identificadas o identificables. Es la parte principal del ordenamiento jurídico que gobierna la protección de datos en Costa Rica. Aun cuando la ley misma menciona el derecho a la privacidad y el derecho a la autodeterminación informativa, fue puesta en vigor para situar el derecho costarricense a tono con las modernas tendencias de protección de los derechos fundamentales de los ciudadanos y, en particular, el derecho a la privacidad con respecto al procesamiento de sus datos personales. En la práctica, provee una forma de controlar la información por parte de los mismos ciudadanos. Cualquier persona que esté en posesión de datos personales para otros propósitos estaría obligada a cumplir con

1 Abogado y notario. Licenciado en Derecho de la Universidad de Costa Rica. LL.M. y Doctor en Derecho de la Universidad Johann-Wolfgang Goethe, Frankfurt del Meno, República Federal de Alemania. Juez del Tribunal de Apelación de Sentencia Penal de San José. Catedrático de la Facultad de Derecho de la Universidad de Costa Rica. Correo electrónico: alfredochirino@gmail.com.

selves and to control whether their data banks comply with the standards set on this Act. This legislation introduces the Data Protection Agency (PRODHAH) and defines its competence and juridical liability.

Keywords: Costarican Data Protection Act, Privacy, Right to the information self-determination, Data Protection Agency, Sensible Data, Data Protection Principles, Consent of individuals, Hábeas Data.

esta ley, sujeta por supuesto a algunas excepciones. La ley define ocho principios de protección. También requiere que las compañías y los individuos mantengan la información personal para sí mismos y ayuden a controlar si los bancos de datos cumplen con los estándares establecidos en esta norma. La legislación crea la Agencia de Protección de Datos (PRODHAB) y define su competencia y personalidad jurídica.

Palabras clave: Ley costarricense de protección de datos personales, privacidad, derecho a la autodeterminación informativa, datos sensibles, principios de la protección de datos, consentimiento de los individuos, hábeas data.

Sumario

Introducción

Luego de un largo proceso legislativo de discusión y análisis, que se prolongó por casi veinte años, Costa Rica adoptó su primera legislación en materia de protección de datos personales.

Bajo el sugerente título de Ley de protección de la persona frente al tratamiento de sus datos personales[2], esta normativa se orienta hacia un reconocimiento del derecho a la autodeterminación informativa, como un complemento indispensable en el Estado de derecho. En su configuración original, este derecho, abordaba el control de quién, cuándo, dónde y bajo qué circunstancias entrar en contacto con datos personales de un individuo, tal y como lo incluyó el Tribunal Constitucional Federal Alemán en su famosa sentencia de 1983 sobre la Ley de Censos. Hoy, el legislador costarricense, decidió darle a esta apodíctica estructuración jurisprudencial una forma regulatoria, que permita alcanzar al ciudadano un estándar razonable de tutela frente a los retos que surgen del actual desarrollo del tratamiento de datos personales.

Como lo fue históricamente, y lo es hoy frente al influjo incontenible de las tecnologías de la información y la comunicación, se trata de un derecho de control del flujo de informaciones que tienen una conexión directa con el ejercicio de la democracia en la sociedad tecnológica y con la necesidad de proveer al individuo herramientas normativas y técnicas para que pueda ejercer sus derechos constitucionales en marcos de referencia cada vez más variados y afectados por su interacción en ambientes virtuales[3].

La persona debe poder decidir cuándo y dentro de cuáles límites sus asuntos de carácter personal pueden ser dispuestos públicamente, y esta posibilidad debe estar garantizada por las normas. Sin embargo, los cambios revolucionarios en las formas de comunicación, la creciente movilidad entre un mundo "virtual" y un mundo "físico" que pierde sus contornos y fronteras, la disponibilidad cada vez mayor de información y datos para la toma de decisiones, así como otras innovaciones en el contexto de la información, conducen a que ese poder de decisión se haga cada vez más difícil.

Junto a lo anterior, en el derecho comparado, este derecho ha sido concebido de tal manera que se requiera siempre un fundamento legal para establecerle límites. Las regulaciones legales que sean creadas deben concretar el uso de los datos personales y su procesamiento a determinados propósitos, de tal manera que las recopilaciones de datos hechas con fines inespecíficos o simplemente "a beneficio de inventario" deban ser prohibidas.

2 Ley de protección de la persona frente al tratamiento de sus datos personales, Ley No. 8968, publicada en *La Gaceta* No. 170 de 05 de septiembre de 2011. A continuación se citará como LPPTDP.

3 La búsqueda de la tutela del ciudadano en esos ámbitos es fundamental como requisito para su autodeterminación como persona en la sociedad de la información y la comunicación. Hará falta, por supuesto, reducir la brecha digital, demostrar voluntad política para impulsar un acceso igualitario a las tecnologías y promover competencias para el uso de estas en el desarrollo económico y social. Tal parece ser, al menos, el enfoque de la Unión Europea acerca de las ventajas de la sociedad de la información: promover infraestructuras de comunicación de costes razonables, ciudadanos con competencias necesarias para vivir y trabajar en la sociedad de la información y garantía de acceso al aprendizaje permanente como componente esencial del modelo europeo. Cfr. Rossi Carleo, L., "La sociedad de la información: el ciudadano frente al poder de decisión ajeno", en Llácer Matacás, María Rosa (Coordinadora), *Protección de datos personales en la sociedad de la información y vigilancia,* Madrid, La Ley, primera edición, 2011, p. 28.

Otras limitaciones se refieren a la búsqueda de fines públicos de gran calado, como los alusivos a la seguridad ciudadana, la toma de decisiones por parte de la administración estatal, y el desarrollo del crédito público, entre otros objetivos de trascendencia social.

La ley costarricense apunta hacia estas direcciones, no obstante, con medidas que en algunos casos resultan contradictorias, en otros, poco claras, y las más de las veces, inciertas en cuanto a sus alcances y compromisos. Un análisis de estos aspectos implicaría un estudio que excede las posibilidades de este artículo, cuya intención es difundir los objetivos más importantes que esta nueva legislación procura, y la forma en que se instauró el régimen de protección. Quedará para más adelante un análisis más profundo de las "sombras" que se ciernen sobre algunos de los problemas que existen en el país y en la región respecto el tema de la protección de datos personales y su régimen jurídico.

I. EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA Y SU APRECIACIÓN NORMATIVA

Es en virtud de esta vocación de solidaridad, y de la necesidad de preservar la intimidad y la privacidad del individuo para garantizarle un *status civitatis* en una sociedad tecnológica, que ha resultado indispensable construir un nuevo derecho, desde las bases mismas de la tradicional tutela de la intimidad, pero con una orientación superior: facultar la realización de la persona en un mundo complejo de aislamientos y aspiraciones individuales pero también de relaciones comunicacionales de primer orden.

Es así que surge, de la mano de la jurisprudencia del Tribunal Constitucional Federal Alemán, pero con contribuciones previas de la doctrina civil y constitucional alemana, la figura jurídica del derecho a la autodeterminación informativa, en la importante sentencia sobre la Ley de Censos de 1982. En este fallo se sostiene que en las condiciones actuales de desarrollo del tratamiento de datos personales resulta indispensable la protección del individuo frente a la recolección, almacenamiento, utilización y difusión ilimitada de sus datos personales. Esta protección quedaba englobada, según el decir de la sentencia, en el artículo 2, párrafo primero, de la Ley Fundamental de Bonn de 1949. De esta forma se reconoce un derecho ciudadano a la autodeterminación informativa frente a la difusión y utilización de sus datos.

El Tribunal Constitucional Alemán destacó este derecho como una garantía a saber "quién, cuándo, dónde y bajo qué circunstancias ha tenido acceso a sus datos personales". Se trata de un derecho a controlar el flujo de las informaciones y datos personales. No obstante, no lo visualiza como una garantía absoluta. Como todo derecho tiene límites, los cuales pueden ser fijados por razones de interés general superior y necesitan, para ser asumidos, un fundamento legal basado en la Constitución, el cual, a su vez, debe responder a la necesidad de normas claras y precisas, que es una garantía adicional en el Estado de derecho[4].

4 Tribunal Constitucional Federal Alemán, Sentencia 65, 1, publicada en español en Schwabe, J., (Compilador), Cincuenta años de jurisprudencia...

Los objetivos de la autodeterminación informativa[5] pueden resumirse en dos: por una parte, convertirse en salvaguarda de la persona frente al creciente uso de las tecnologías para el tratamiento de datos personales y, en un segundo plano, crear posibilidades reales y efectivas de evitar la construcción de personalidades de cristal, transparentes a cualquier uso y abuso, sin el conocimiento ni la voluntad del afectado o sin atender a algún interés general preponderante.

El legislador costarricense, en el artículo 4, con el epígrafe "Autodeterminación Informativa", establece que esta garantía abarca el "conjunto de principios y garantías relativas al legítimo tratamiento de sus datos personales reconocidos en esta sección". Pero en el párrafo dos, luego de vincular la autodeterminación informativa al tratamiento de datos personales, indica que este derecho tiene como fin "controlar el flujo de informaciones que conciernen a cada persona, derivado del derecho a la privacidad, evitando que se propicien acciones discriminatorias".

Lo cierto es que, a pesar de la circunscripción del derecho a la autodeterminación informativa a la privacidad, que es, de suyo, una limitación innecesaria, es claro que se trata de una garantía de carácter esencial para evitar lesiones a otros derechos fundamentales como el derecho al ejercicio de derechos cívicos, al honor, a la imagen, a construir un plan de vida, al respeto a su dignidad, a la libre escogencia de ideologías y credos, etcétera[6]. En otras palabras, el derecho a la autodeterminación informativa promueve condiciones en las cuales pueden desarrollarse y ejercerse otros derechos fundamentales de gran importancia para el Estado democrático y social de derecho.

Este derecho ostenta diversas características que lo distinguen: es garantizador y facilitador; no busca obstaculizar o interrumpir el libre flujo de informaciones que hoy identifica a las sociedades democráticas, sino preservar la protección de la persona frente a intromisiones no conocidas o no queridas en su ámbito de privacidad; es una garantía que busca, en suma, a través de principios reguladores, supeditar el tratamiento de datos personales a estándares de calidad, de transparencia, de sometimiento al fin para el que fueron recabados y a fundar su uso y manejo en el consentimiento informado del afectado. Adicionalmente a ello, se ha reconocido la necesidad de una tutela institucional que ayude a prevenir daños a la esfera de derechos de la persona mucho antes de que un tratamiento de datos específicos o una transferencia electrónica de datos transfronteras pueda generar un daño o afectación al derecho de la persona a la autodeterminación informativa.

Hablamos, entonces, de un derecho basado en principios que garantizan el libre flujo de informaciones, la creación de bancos de datos y de

cia del Tribunal Constitucional Federal Alemán, Medellín, Colombia, Konrad Adenauer Stiftung, Ediciones Jurídicas Gustavo Ibáñez, 2003, pp. 36 a 44.

5 Un panorama sobre este derecho puede encontrarse en Limberger, T., *O Direito à Intimidade na Era da Informática. A necessidade de proteção dos dados pessoais*, Porto Alegre, Brasil, Livraria do Advogado, 2007, pp. 103-116.

6 La tecnología ha hecho posible crear cuadros muy exactos de nuestros movimientos, de nuestras comunicaciones, de la forma en que interactuamos con nuestros semejantes, de nuestras costumbres y apetencias, del uso de nuestro tiempo libre, de lo que leemos y pensamos, de las participaciones que hacemos en asuntos públicos y privados, y, en general, de nuestra cotidianeidad.

actividades en el marco tecnológico, pero preservando y garantizando la tutela de la persona en sus derechos fundamentales.

Es indudable que habrá limitaciones a este derecho y que estas se producirán por intereses públicos preponderantes como lo es la investigación de los delitos, pero estas restricciones deben contemplarse en la ley y someterse a un control constitucional de la proporcionalidad de estas intervenciones estatales en las esferas de derechos del ciudadano.

En su moderna configuración, el derecho a la autodeterminación informativa concede al ciudadano la facultad para estar informado del procesamiento de los datos y de los fines que con él se pretende alcanzar, junto con el derecho de acceso, corrección o eliminación en caso de que se le cause un perjuicio ilegítimo[7].

1. Límites al derecho a la autodeterminación informativa

La Ley de protección de la persona frente al tratamiento de sus datos personales, en su artículo 8, establece las excepciones al derecho a la protección de datos personales:

> ARTÍCULO 8.- Excepciones a la autodeterminación informativa del Ciudadano.
>
> Los principios, los derechos y las garantías aquí establecidos podrán ser limitados de manera justa, razonable y acorde con el principio de transparencia administrativa, cuando se persigan los siguientes fines:
>
> a) La seguridad del Estado.
>
> b) La seguridad y el ejercicio de la autoridad pública.
>
> c) La prevención, persecución, investigación, detención y represión de las infracciones penales, o de las infracciones de la deontología en las profesiones.
>
> d) El funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica, cuando no exista riesgo de que las personas sean identificadas.
>
> e) La adecuada prestación de servicios públicos.
>
> f) La eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.

Como puede observarse, el legislador pretendía dejar en claro que el derecho a la autodeterminación informativa no iba a imperar sin límites, y definió que la seguridad del Estado, la prevención y persecución de los delitos serían objetivos que no podrían limitarse con el argumento de proteger esta garantía. No obstante, tales excepciones deberían pasar por el tamiz de principios tales como el de justicia, razonabilidad y transparencia administrativa, a los que habría que agregar el de proporcionalidad.

Es evidente que el principio de proporcionalidad, sobre todo el de proporcionalidad en sentido estricto, entra en discusión directamente cuando se plantean limitaciones al derecho a la autodeterminación informativa. No sería po-

7 Cfr. Sala Constitucional de la Corte Suprema de Justicia, Costa Rica, Voto 1434-2003 de las 10:56 hrs. del 21 de febrero de 2003. Sobre el fondo, apartado V.

sible pensar ninguna limitación de este derecho si no se ha realizado un análisis de su necesidad, adecuación e idoneidad para cumplir el fin público del que se trate. Aun después de este análisis, habría que preguntarse si la limitación es "soportable" individualmente para el sujeto que la sufre en razón de esos fines públicos que se plantea realizar.

2. Autodeterminación informativa vs. hábeas data

En el contexto latinoamericano la formulación de un derecho de la persona frente al tratamiento de datos personales suele evocar la necesidad de proteger el hábeas data, considerándolo al mismo tiempo como la garantía de acceso a la jurisdicción así como también el derecho a proteger[8].

Este acercamiento al tema ha provocado que el desarrollo normativo de los países haya comenzado con prever garantías a la tutela jurisdiccional antes que un verdadero reconocimiento del derecho fundamental a la autodeterminación informativa.

El hábeas data tiende a ser, en la discusión latinoamericana, el sinónimo al derecho de acceso, revisión, corrección y rectificación de información y datos personales, y por allí toda la tarea del legislador se ha concentrado en crear los medios para que esta vía jurisdiccional quede preservada y garantizada. Tal es el caso de la Ley de control constitucional del Ecuador que habilitó el hábeas data a ciudadanos y extranjeros, entidades públicas y privadas, que desean tener acceso a documentos, bancos de datos y otros ficheros que contengan información acerca de sí mismos o de las propiedades que poseen. El propósito del hábeas data ecuatoriano es asegurar que el controlador de los datos los entregue de manera clara, completa y verdadera; que corrija, borre o no entregue información a terceros; y que el afectado obtenga garantías de que el controlador de los datos ha rectificado, eliminado o no ha entregado la información[9].

El hábeas data no es, entonces, sino una garantía o mecanismo jurídico procesal que permite la defensa, la realización de derechos fundamentales, en este caso, el derecho a la intimidad, a la autodeterminación informativa contra el uso indebido por parte de terceras personas.

8 Esta interesante dualidad es planteada problemáticamente por la Sentencia del Tribunal Constitucional de Perú en el expediente EXP. N° 1797-2002-HD/TC que sostiene:

> Este Tribunal ha expresado en la sentencia recaída en el Exp. N°. 666-1996-HD/TC que la protección del derecho a la autodeterminación informativa a través del hábeas data comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona. Tal acceso puede tener por objeto que se permita conocer qué es lo que se encuentra registrado, para qué y para quién se realizó el registro de información así como la (o las) persona(s) que recabaron dicha información. En segundo lugar, el hábeas data puede tener la finalidad de agregar datos al registro que se tenga, ya sea por la necesidad de que se actualicen los que se encuentran registrados, o bien con el fin de que se incluyan aquellos no registrados, pero que son necesarios para que se tenga una cabal referencia sobre la imagen e identidad de la persona afectada. Asimismo, con el derecho en referencia, y en defecto de él, mediante el hábeas data, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados.

Sentencia disponible en: http://www.tc.gob.pe/jurisprudencia/2003/01797-2002-HD.html

9 Cfr. Artículo 34 de la Ley de Control Constitucional, disponible en: http://www.uc3m.es/uc3m/inst/MPG/JCI/02-ecuador-leycontrolconstitucionalidad.htm#II.II

Se trata de una tutela jurisdiccional y en modo alguno del derecho en juego.

Las tendencias jurisprudenciales se orientan a convertir el recurso o acción de amparo en una forma de "hábeas data" que permite rectificar, cambiar o eliminar datos que contengan información imprecisa, incorrecta, desactualizada o falsa de los ciudadanos.

Esta tendencia ha sido recogida también en las recientes constituciones políticas regionales y en legislación[10].

Con o sin ley que considere este recurso, existe una predisposición para que la jurisdicción constitucional dé acceso, por la vía de amparo, a la tutela de ciertos aspectos del derecho a la protección de datos personales. Sin embargo, un amparo de esta índole opera cuando ya la lesión ha sido ocasionada, cuando el ciudadano no ha recibido un préstamo o no fue contratado o ha perdido alguna oportunidad de empleo o de interacción social. En tal caso no funciona con vocación preventiva sino reivindicatoria y en cierta forma indemnizatoria.

El derecho a la autodeterminación informativa es, pues, el derecho protegido dentro de una perspectiva jurisdiccional de amparo. No obstante, hace falta reconocer legislativamente otra faz trascendente de este derecho: sus perspectivas de control y organización del tratamiento de los datos personales.

Una regulación normativa del derecho a la autodeterminación informativa, en los términos de la Constitución Política, no puede quedar constreñida a garantizar el acceso a la jurisdicción, aun si resulta indispensable para atender a los estándares internacionales en la materia, así como ofrecer medios para garantizar que el procesamiento de datos personales sigue una serie de lineamientos de calidad y de control contra los abusos y el ejercicio abusivo de prerrogativas de vigilancia y perfilado de las personas en la sociedad moderna.

Es por lo anterior que la tercera generación de leyes de protección de datos personales[11] se orienta en el modelo institucional, donde, por medio de un órgano creado al efecto, se vela constantemente por tomar directrices y políticas que garanticen las condiciones de este tipo de

10 Entre otras, pueden mencionarse los siguientes ejemplos de incorporación del hábeas data en fecha reciente: Colombia lo incluyó en la Constitución desde 1991 y la Corte Constitucional tiene ya más de 140 precedentes que le han dado forma al hábeas data colombiano, así como a las condiciones en que debe realizarse el tratamiento de datos. La Constitución paraguaya de 1992, en su artículo 135 lo institucionaliza, garantizando de esa manera a los ciudadanos el acceso a sus datos, tanto en bancos de datos públicos o privados, y a requerir información acerca de la forma en que se está haciendo uso de los mismos. La Constitución de Perú en su artículo 2.6 contempla el derecho al acceso a la propia información, el cual es definido como derecho a la autodeterminación informativa como también el derecho de acceso a la información pública. El Parlamento uruguayo promulgó la Ley número 17.838 sobre protección de datos personales que regula la tutela de información bancaria y financiera e instituye la figura del hábeas data.

11 Las leyes de la primera generación serían, según este autor, las que se concentraban en una autorización previa de los bancos de datos, lo que tenía sentido ya que estas leyes surgieron cuando el procesamiento de datos era centralizado, los equipos voluminosos y fácilmente localizables. Luego surgieron las "leyes de la segunda generación" las cuales pusieron el énfasis en los datos sensibles, a fin de evitar daños a la privacidad y ofrecer alguna garantía frente a posibles prácticas discriminatorias que pudieran tener su origen en el uso de esos datos "sensibles". Luego vendrían las leyes de la tercera generación, interesadas en el "uso" y "funcionalidad" de las informaciones. Aquí ubica Pérez Luño, por ejemplo, a la LORTAD española. Cfr. PÉREZ LUÑO, A., "La tutela de la libertad informática", en *Agencia de protección de datos* (Edit.). *Jornadas sobre el derecho español de la protección de datos personales*, Madrid, De Arellano S.L., 1996, pp. 97-98.

tratamiento de datos en forma coherente con las expectativas de protección en el actual ambiente de desarrollo de la sociedad[12].

Las leyes de cuarta generación hacen una apuesta más fuerte por un control autorregulatorio, con más opciones para el tratamiento de datos personales y para una cooperación a nivel transnacional entre las autoridades de control. En esta línea se orienta la presente legislación.

3. Carácter complementario del régimen jurídico de la ley y el hábeas data desarrollado jurisprudencialmente

El legislador se ha decantado, entonces, por una tutela doble. El recurso de amparo especial denominado "hábeas data" ha sido desarrollado por la Sala Constitucional de la Corte Suprema de Justicia de una manera fuerte y vigorosa, por ello se ha convertido en una importante herramienta para obtener acceso a los bancos de datos públicos y privados, para averiguar qué información existe sobre el ciudadano y hacer las correcciones del caso. No obstante, es un derecho de carácter "reactivo", esto es, se ejerce cuando ya es demasiado tarde y el derecho fundamental a la autodeterminación informativa ha sido lesionado.

Por lo anterior, resultaba necesario completar la tutela ya existente con el hábeas data, con una ley que proveyera protección preventiva; con un órgano de vigilancia que pudiera establecer límites, controles de calidad y ejercer una supervisión del cumplimiento de los principios de la protección de datos personales que forman parte del núcleo de tutela del derecho a la autodeterminación informativa.

Es así que todo el capítulo IV de la Ley está dirigido a crear las condiciones para el funcionamiento de la así denominada Agencia de Protección de Datos de los Habitantes (PRODHAB).

Hubo una fuerte discusión en la Asamblea Legislativa costarricense, en primer lugar, sobre cuál debería ser el régimen jurídico de este órgano y, en segundo lugar, a cuál ministerio o entidad pública debería adscribirse. Por algún tiempo se mantuvo el proyecto con la indicación que sería la Defensoría de los Habitantes la que debería asumir a la PRODHAB, dotarla de financiamiento y de personal adecuado, y crear condiciones para su funcionamiento. No obstante, no solo la resistencia de la propia Defensoría, sino también de algunos juristas nacionales, provocó que el legislador meditara mejor su decisión y se diera cuenta, al mismo tiempo, que las características de la Defensoría de los Habitantes no satisfacían las expectativas sociales de un órgano que tenía como deber garantizar el acceso a la información de los ciudadanos, así como proveer una adecuada tutela preventiva con acciones en el campo de la protección de datos, mediante visitas técnicas, revisión de estándares, dictado de directivas pero, al mismo tiempo, mediante el juzgamiento y sanción administrativas de las desviaciones al régimen legal establecido por esta Ley.

12 Un panorama amplio de estas generaciones de leyes puede ser consultado en CHIRINO SÁNCHEZ, A. y Marvin CARVAJAL PÉREZ, "El camino hacia la regulación normativa del tratamiento de datos personales en Costa Rica", en CANALES GIL, Á.; BLANCO ANTÓN, M. J.; ORTUÑO SIERRA, M. (coordinadores), *Protección de datos de carácter personal en Iberoamérica*. II Encuentro Iberoamericano de Protección de Datos. La Antigua, Guatemala, 2-6 de junio de 2003, Valencia, Tirant Lo Blanch, 2005, pp. 211 y ss.

Luego de algunos retrasos en la toma de una decisión sobre cuál sería el ente u órgano que asumiría la responsabilidad de echar adelante esta institución, se terminó por crear una adscripción al Ministerio de Justicia y Paz, con personalidad jurídica instrumental, lo que le permite tener las competencias administrativas de fiscalización y sanción, pero también la capacidad de manejar sus presupuestos y recursos[13]. Se garantizó, igualmente, su independencia de criterio, aspecto que sin duda debe entenderse en el marco de sus competencias, aun dentro de los problemas que pudieran surgir en la aplicación de este marco legal al interior del propio Ministerio de Justicia y Paz, el cual, en Costa Rica, también administra el sistema penitenciario y los registros públicos de propiedad mueble e inmueble, de indudable incidencia en el ámbito del tratamiento de datos personales.

El artículo 16 incluye las atribuciones de la PRODHAB, que son las que suelen estar previstas en las legislaciones que contemplan este tipo de garantías institucionales de protección del derecho a la autodeterminación informativa: facultad de control del cumplimiento de la normativa; requerimiento de informaciones a los encargados del tratamiento, acceso a los bancos de datos propiamente dichos; instalación, administración y puesta en funcionamiento de un registro de bancos de datos personales; ordenar los cambios solicitados por los ciudadanos, así como imponer las sanciones previstas en la ley.

Dentro de su función institucional se agrega, adicionalmente, su papel de líder en la construcción de directivas en materia de protección de datos en Costa Rica, promoviendo cambios en el manejo y administración de bancos de datos, diseñando legislación y reglamentación en el campo. El legislador hizo un énfasis especial en establecer como tarea de la PRODHAB la de difundir una cultura de sensibilidad por la protección de datos[14].

La agencia tendrá un director o directora, con conocimientos en este campo, acompañado de un personal adecuado para proveer los servicios previstos[15].

Las condiciones anotadas deberían estar listas en un plazo de seis meses a partir de la vigencia de la ley[16]. Dicho plazo habrá transcurrido para la fecha de la publicación de este ensayo, y no se avizora que vayan a darse en corto tiempo.

II. PRINCIPIOS ORIENTADORES DE LA REGULACIÓN DE PROTECCIÓN DE DATOS PERSONALES

El tratamiento de datos personales es hoy una forma de obtener enormes beneficios en los más diversos campos de la actividad humana,

13 Cfr. Artículo 15 de la lpptdp.

14 Cultura que es esencial para crear condiciones para que los ciudadanos busquen la realización del derecho a la autodeterminación informativa e impulsen cambios correspondientes en la legislación y en la práctica de las instituciones públicas y las empresas del sector privado que realizan tratamiento de datos personales.

15 El artículo 19 contiene una serie de prohibiciones que buscan garantizar el cumplimiento de deberes éticos del personal de la PRODHAB, entre ellos el deber de sigilo, la prohibición de actuar en casos donde pueda haber conflicto de intereses, y de trabajar de cualquier forma con las empresas e instituciones que realizan algún tipo de tratamiento de datos personales.

16 Cfr. Transitorio II de la LPPTDP.

tanto de los sectores públicos como privados. Desde la toma de decisiones en el ámbito de la política pública (salud, educación, prevención y represión del delito, política económica, etc.), pasando por la forma de organizar la sociedad acorde con los cambiantes paisajes del desarrollo de expectativas, hasta llegar a la definición de políticas de trabajo, aseguramiento médico, campañas publicitarias y avituallamiento de supermercados y tiendas, el tratamiento de datos personales de ciudadanos consumidores de servicios es esencial para garantizar el funcionamiento de la economía y de la sociedad.

Sin embargo, tales fines, de indudable valor e impacto en el momento actual, no están alejados de riesgos y peligros de que se produzca un uso arbitrario, indiscriminado e ilegal de los datos personales.

El abuso de las facultades de control y vigilancia de casi todos los aspectos de la vida privada de los ciudadanos puede llevar no solo a una conquista del mundo de la vida por la vía de la utilización de las tecnologías, sino también a una destrucción de los ámbitos privados, dejando la vida social sin posibilidad de espacios para el impulso de un plan individual, libremente escogido y garantizado.

El riesgo de un retraimiento de la persona en el ejercicio de sus derechos, ante el temor de la vigilancia y control desmedidos no solo por parte del Estado sino también de los particulares, opera en la base misma de la reflexión sobre las condiciones para el desarrollo de una tutela jurídica de este derecho.

En virtud de lo anterior, se han venido desarrollando doctrinal y legislativamente algunos principios rectores de la protección de datos personales; estos principios orientan la forma en que debe darse su tratamiento.

Legislaciones como la española, que sigue los estándares establecidos por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, relativa a la protección de las personas físicas en relación con el tratamiento de datos personales y a la libre circulación de estos, incluyen principios tales como el de calidad, que obliga a que los datos que sean tratados han de ser ciertos, verdaderos y no excesivos. Igualmente exige que sean actualizados.

De la misma forma, se incluye el principio de pertinencia, el cual obliga a valorar los datos acorde con el ámbito y la finalidad para los que se obtuvieron.

Como casi todas las legislaciones modernas de Europa, el tratamiento de datos personales se hace depender del consentimiento inequívoco de la persona titular.

De igual forma, y casi desde el propio inicio de la historia del derecho a la protección de datos personales, se exige que el tratamiento de datos se someta a la criba constitucional del principio de proporcionalidad, tanto cuantitativa como cualitativamente. Esto involucra no solo una valoración de la necesidad e idoneidad del tratamiento para alcanzar los fines legales, sino también la atención a los compromisos del principio de proporcionalidad en sentido estricto

(prohibición de exceso) y el análisis de si son soportables, individualmente, las consecuencias de ese tipo concreto de tratamiento para realizar el manejo que se ha considerado necesario e idóneo para alcanzar los fines establecidos previamente en la ley, por medio de disposiciones claras y expresas.

En concordancia con los principios anteriores, el procesamiento de datos debe sujetarse a los fines para los cuales fue autorizado (principio de sujeción al fin) y, además, ser transparente, de modo que el ciudadano pueda controlar no solo la existencia de los registros donde se conservan y se tratan sus datos (electrónica o manualmente), sino los fines del banco de datos, como también del responsable de los mismos.

Igualmente han de garantizarse arreglos institucionales para asegurar el sigilo en el tratamiento y los mecanismos de seguridad que garanticen la integridad de los datos y su preservación.

En concordancia con estas aspiraciones principialistas del derecho a la autodeterminación informativa, el legislador costarricense incorporó, en primer lugar, el principio de consentimiento informado (artículo 5), que se subdivide, a su vez, en la obligación de informar al afectado de la existencia del banco de datos y de la forma en que dicha información será administrada y manejada. De la misma manera se establece una regulación sobre cómo otorgar este consentimiento informado (párrafo 2 del artículo 5).

De igual forma, el principio de calidad de la información se encuentra incorporado en el artículo 6 de la Ley, desgajando sus elementos en actualidad, veracidad, exactitud y adecuación en sus distintos párrafos.

El artículo 7 describe los derechos que le asisten a la persona frente al tratamiento electrónico de sus datos personales. Establece, en primer lugar, el derecho al acceso en su más amplio sentido, obligando a que este sea realizado de manera gratuita y con respuesta rápida al interesado (cinco días a partir de la solicitud de información). El legislador prestó especial atención a las medidas de seguridad para la conservación de los datos, y a la obligación del centro de procesamiento de informar acerca de la existencia de estos en sus acervos, la finalidad para la que fueron recopilados, así como sobre los registros en su integralidad que se conservan de esta. Es claro que dichos informes deben ser entregados sin complejidades o lenguajes que hagan imposible su comprensión al ciudadano medio, y con una explicación de los términos técnicos que pudieran incorporar.

En segundo lugar se establece, en el párrafo segundo del artículo 7 de la Ley, el derecho a la rectificación de datos e informaciones incompletas o inexactas o cuando hayan sido obtenidos con infracción a las reglas establecidas normativamente. El derecho de rectificación involucra, igualmente, el derecho a la actualización y a la cancelación y eliminación de aquellos datos que causen o puedan causar perjuicio a la persona.

El ejercicio del derecho a la autodeterminación informativa le presta una especial importancia al consentimiento. El artículo 5 de la ley contiene el principio del consentimiento informado. La idea es que siempre que se vayan a recoger datos de

carácter personal debe informarse a la persona titular, de forma clara, tanto verbal o mediante una advertencia por escrito, sobre todo cuando se pida información en cuestionarios.

La idea es que la persona sepa quién, por qué, para qué fines y quiénes son los destinatarios de la información, así como quiénes van a consultar los datos. Debe informarse también sobre la forma del tratamiento que se dará a la información, la identidad del responsable de la recolección de datos y la posibilidad de ejercer derechos.

En las páginas web el derecho de consentimiento suele dejarse a la modalidad "*opt in*" "*opt out*" que tiene como propósito que cuando la persona haga un clic en alguna opción que implica tratamiento de datos personales sepa si está de acuerdo con dicho tratamiento, y pueda siempre renunciar si ha dado el consentimiento.

III. CONCLUSIONES

El ordenamiento jurídico costarricense se ha completado con la entrada en vigencia de esta ley de protección de datos. Su vocación tanto técnica como jurídica la ubica en las modernas tendencias de legislación de cuarta generación, y procura establecer un nivel adecuado de tutela de la persona frente a los peligros de un uso abusivo de sus datos personales.

No obstante, algunos problemas de definición y énfasis innecesarios podrían llevar a una difícil puesta en vigor de la ley, y a problemas de implementación, en especial, a cuanto se refiere a las facultades de control y vigilancia del procesamiento de datos personales en el país. Es posible que el reglamento que habrá de dictarse pronto pueda paliar algunos de los vacíos de precisión y aclarar algunos de sus puntos oscuros, con el objetivo de brindar un buen arranque a esta nueva etapa de la protección de datos en Costa Rica.

El sistema convivirá, a no dudarlo, con la ya preexistente jurisprudencia de hábeas data de la Sala Constitucional, que ya había dado los pasos más importantes conducentes a crear las condiciones para el desarrollo normativo de esta legislación. Es clave para el avance futuro que esta relación se mantenga fuerte y firme, de tal manera que los ciudadanos puedan confiar no solo en la autotutela de su derecho a la protección de datos, sino también en una protección preventiva vía la PRODHAB.

La vigencia de legislación en esta materia en América Latina, así como la experiencia acumulada de los encargados de protección en diversas latitudes, será un marco de referencia que jugará un papel trascendente en la realización de los principios de protección que esta ley incorpora.

El futuro de la protección de datos en Costa Rica luce interesante, aun cuando algunas sombras se asoman en el horizonte, por lo que el buen trabajo de la PRODHAB será clave para desterrar algunos temores que se escuchan en relación con la validez puramente formal de esta legislación.

Bibliografía

Chirino Sánchez, A. y Marvin Carvajal Pérez, "El Camino hacia la Regulación normativa del Tratamiento de Datos Personales en Costa Rica", en: Álvaro Canales Gil; María José Blanco Antón; Mercedes Ortuño Sierra (coordinadores), *Protección de datos de carácter personal en Iberoamérica* (II Encuentro Iberoamericano de Protección de Datos, La Antigua, Guatemala, 2-6 de junio de 2003, Valencia, Tirant Lo Blanch, 2005.

Limberger, T., *O Direito à Intimidade na Era da Informática. A necessidade de proteção dos dados pessoais*, Porto Alegre, Brasil, Livraria do Advogado, 2007.

Llácer Matacás, María Rosa (Coordinadora), *Protección de datos personales en la sociedad de la información y vigilancia*, Madrid, La Ley, primera edición, 2011.

Pérez Luño, A., "La tutela de la libertad informática", en *Agencia de Protección de Datos (Edit.), Jornadas sobre el derecho español de la protección de datos personales*, Madrid, De Arellano S.L., 1996.

Rossi Carleo, L., "La sociedad de la información: el ciudadano frente al poder de decisión ajeno", en María Rosa Llácer Matacás (Coordinadora), *Protección de datos personales en la sociedad de la información y vigilancia*, Madrid, La Ley, primera edición, 2011.

Schwabe, J. (Compilador), *Cincuenta años de jurisprudencia del Tribunal Constitucional Federal Alemán*, Medellín, Colombia, Konrad Adenauer Stiftung, Ediciones Jurídicas Gustavo Ibáñez, 2003, pp. 36 a 44.