

PODER LEGISLATIVO

LEYES

Nº 8354

LA ASAMBLEA LEGISLATIVA
DE LA REPÚBLICA DE COSTA RICA, DECRETA:

SEGREGACIÓN Y DONACIÓN DE UN INMUEBLE DEL CONSEJO
NACIONAL DE PRODUCCIÓN A LA FEDERACIÓN
COSTARRICENSE DE FÚTBOL

Artículo 1º—Autorízase al Consejo Nacional de Producción para que segregue un lote del inmueble inscrito en el Registro Público de la Propiedad, partido de Alajuela, bajo el Sistema de Folio Real matrícula Nº 122759-000. Según las especificaciones establecidas en el plano catastrado Nº A-821524-2002, del 15 de octubre del 2002, el inmueble se describe así: su naturaleza es de terreno de repasto; está situado en el distrito 8º, San Rafael; cantón uno, Alajuela; mide siete hectáreas dos mil doscientos ochenta y siete metros con cinco decímetros cuadrados y colinda al norte, con el río Burio; al sur, con el resto reservado; al este, en parte con Israel Delgado Herrera, el resto reservado y calle pública, con un frente de ciento veintiuno coma setenta y cinco metros lineales y al oeste, con el resto reservado y el río Burio.

Artículo 2º—Autorízase al Consejo Nacional de Producción para que done el inmueble por segregar a favor de la Federación Costarricense de Fútbol, cédula jurídica Nº 3-002-056141.

La Federación deberá limitar el destino del inmueble donado exclusivamente a la construcción de un complejo deportivo. Este proyecto deberá cumplir previamente todos los requisitos constructivos y ambientales fijados.

Artículo 3º—De incumplirse la limitación estipulada en el artículo anterior, de disolverse la Federación indicada o de transformarse en una persona jurídica con fines de lucro, la propiedad del inmueble donado se revertirá a favor del Consejo Nacional de Producción.

Para los efectos de lo dispuesto en este artículo, se considerará inculcación del hecho de que no estén finalizadas las obras del complejo deportivo en un plazo de cinco años.

Dichas obras deberán ser las siguientes:

- Canchas de fútbol con césped natural y artificial.
- Canchas para la práctica del fútbol playa.
- Áreas de calentamiento en césped natural y en concreto.
- Un gimnasio para la práctica del fútbol sala.
- Camerinos con piscina cubierta y temperada, consultorio médico, área de masajes y lavandería.
- Complejo habitacional consistente en habitaciones dobles con área de lavandería y área de esparcimiento.
- Área de comedor y cocina industrial.
- Edificio administrativo que albergará las oficinas de la Federación y de las ligas afiliadas a ésta y contará, además, con auditorios y salas de reuniones.
- Áreas verdes.
- Accesos pavimentados a cada una de las edificaciones descritas.
- Área de estacionamiento de vehículos.

Artículo 4º—En virtud del otorgamiento de este bien patrimonial del Estado a título gratuito, la Contraloría General de la República realizará la fiscalización referida en el artículo 5º de la Ley Orgánica de la Contraloría General de la República, Nº 7428, del 7 de setiembre de 1994, y anualmente informará a la Asamblea Legislativa de su fiscalización, la cual tendrá como objeto el estudio del cumplimiento de la construcción del complejo deportivo referido en esta Ley, fin para el que se autoriza esta donación.

Artículo 5º—En relación con el objeto de esta Ley, el Instituto Costarricense del Deporte y la Recreación tendrá las facultades que le señala el inciso n) del artículo 3º de la Ley Nº 7800, Creación del Instituto Costarricense del Deporte y la Recreación y del Régimen Jurídico de la Educación Física, el Deporte y la Recreación, del 30 de abril de 1998.

Rige a partir de su publicación.

Comunicase al Poder Ejecutivo

Asamblea Legislativa.—San José, a los treinta días del mes de abril del dos mil tres.—Rolando Laclé Castro, Presidente.—Ronaldo Alfaro García, Primer Secretario.—Lilliana Salas Salazar, Segunda Secretaria.

Dado en la Presidencia de la República.—San José, a los siete días del mes de mayo de dos mil tres.

Ejécútese y publíquese

ABEL PACHECO DE LA ESPRIELLA.—El Ministro de Cultura, Juventud y Deportes, Guido Sáenz González.—1 vez.—(O. C. Nº 3196).—C-23505.—(L8354-34889).

PROYECTOS

Nº 15.178

LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO
DE SUS DATOS PERSONALES

Asamblea Legislativa:

1. Los riesgos para los derechos fundamentales en la sociedad de la información.

Hoy más que nunca, las informaciones adquieren un enorme valor económico. Esto es particularmente cierto en el caso de las transacciones bancarias y financieras en general, pero sobre todo en aquellos ámbitos en donde es posible construir una imagen de los ciudadanos a partir de su interacción con la sociedad y con los medios tecnológicos dispuestos para garantizar el acceso a los datos e informaciones que requiere para realizar su plan de vida y los objetivos que se haya planteado. Estos datos, adecuadamente tratados y transmitidos con herramientas tecnológicas cada vez más poderosas, han determinado que el verdadero signo de la sociedad de la última década del siglo XX esté caracterizado por el uso intensivo de informaciones.

Las tecnologías de la información y de la comunicación han hecho posible que las personas puedan garantizarse condiciones excelentes para interactuar en una gran cantidad de escenarios sociales, pero también para que puedan acceder a un mundo de datos e informaciones que ha transformado profundamente la forma en que la humanidad crea y distribuye sus conocimientos.

Hemos sido testigos de la llegada de una verdadera sociedad de la información, en donde las condiciones para el intercambio de ideas y opiniones se han mejorado a tal punto que es posible pensar en un futuro cercano donde la participación de las personas en los asuntos públicos pueda promocionarse y lograrse por medio de las herramientas e instrumentos dispuestos por la tecnología.

En la actualidad, es de cita común el mencionar la importancia de la Internet para las relaciones comerciales del mundo, y es que en realidad la red de redes se ha convertido en una verdadera autopista que refleja todas las maravillas y las perversiones de la sociedad que la ha concebido. El acceso inmediato a datos e informaciones de la más variada índole, así como a mecanismos para enviar mensajes, imágenes y sonidos a cualquier rincón del mundo, sin las ataduras de distancia y tiempo, han hecho de Internet la esencia básica de esa sociedad de la información.

A pesar de que todos estos avances garantizan mejores condiciones de vida para los seres humanos, así como medios para incentivar el intercambio y producción de conocimiento, es un hecho que el tráfico con informaciones personales, de datos sensibles de las personas, se ha convertido en un verdadero riesgo vital en una sociedad profundamente marcada por la necesidad de intercambiar datos e informaciones.

Tanto los viajeros de Internet, como los ciudadanos que realizan transacciones de la más variada índole, van dejando una huella indeleble que puede ser utilizada para los más diversos objetivos, algunos de ellos lícitos, pero muchos de ellos ilícitos, causando gravísimos perjuicios económicos y sociales a los afectados. Algunos autores han indicado, correctamente, que nos encontramos viviendo una época donde los ciudadanos tienen una presencia virtual, donde todas sus aspiraciones, gustos, apetencias, y más ocultas inclinaciones están disponibles para aquel que desee rastrearlas, perfilarlas, catalogarlas y utilizarlas con los más diversos fines y objetivos de control.

Este peligro de control sin límites, y sin conocimiento del afectado, merece ser tomado en cuenta en la coyuntura que vive actualmente el país.

Costa Rica, al igual que otros países del mundo, debe dotar a sus ciudadanos de un estatus jurídico con el fin de que puedan realizar, en la práctica de la sociedad de la información, su derecho al libre desarrollo de su personalidad y su autodeterminación, sin temor a que el ejercicio de estas y otras libertades esté ensombrecida por el temor a ser observado y detalladamente controlado cuando busca ejercer sus derechos.

El moderno tratamiento de las informaciones tiene, por supuesto, un sinnúmero de ventajas para los ciudadanos que viven en sociedad, sin embargo, sus peligros son mucho más serios porque su carácter es incruento, sutil, carente de violencia. La observación de los datos personales que circulan por las redes de información se hace, normalmente, sin que los afectados tomen conocimiento de tal circunstancia, amparados, en general, en su convencimiento de que si no tienen algo que ocultar, por qué tendrían que preocuparse por velar por su intimidad y por el ejercicio de su libertad.

Esta no es, por supuesto, la situación en otras latitudes, donde existe una profunda sensibilidad por los riesgos representados por el uso indiscriminado de datos personales, sobre todo en manos de particulares.

En los Estados Unidos de Norteamérica, así como en los países de la Unión Europea existe, desde hace muchos años, legislación de tutela para el ciudadano frente al tratamiento electrónico de sus datos personales. La legislación europea se remonta a la década de los años setenta, donde ya comenzaba a desarrollarse un intenso movimiento social tendente a construir herramientas que garantizaran la posibilidad de desarrollarse como persona en una sociedad que centralizaba peligrosamente todas las informaciones y datos sobre los ciudadanos.

Hoy en día, el gran riesgo no lo representa, directamente, el procesamiento centralizado de datos, ni el tratamiento de información que realiza el Estado a través de sus administraciones. Quizá el riesgo mayor está representado por el creciente desarrollo de la informatización de los particulares, los cuales utilizan los cada vez más rápidos, poderosos y pequeños equipos que ofrece la tecnología de la información. Este apertrechamiento tecnológico ubica al procesamiento de datos en manos de los particulares en un papel trascendental en la sociedad de mercado, pero también en la mira de la reflexión sobre los peligros que este tratamiento indiscriminado de datos implica para los ciudadanos, así como para las oportunidades de garantizar la libertad en una sociedad cada vez con menos posibilidades para la soledad y la reserva.

Las investigaciones de crédito y financieras han sido declaradas por la Sala Constitucional de interés público, y nadie duda que son indispensables en los trámites que se realizan cotidianamente en las instituciones bancarias. Sin embargo, ha quedado demostrado en informaciones recientemente difundidas por los medios de comunicación que los ciudadanos se encuentran indefensos ante cada vez más graves y profundas invasiones en sus ámbitos de intimidad, sin tener tales invasiones el correlato de una efectiva tutela contra abusos, contra informaciones imprecisas, inexactas o exageradas o desproporcionadas frente a los intereses y objetivos lícitos que estas empresas persiguen.

Esta laguna normativa no sólo genera un grave peligro para la vigencia real de los derechos constitucionales a la dignidad, la intimidad y al libre desarrollo de la personalidad, sino también representa para el país una grave desigualdad frente a la tutela que se ofrece en otros países de la región latinoamericana que ya han ido comprendiendo la importancia de alcanzar estándares en este campo. Alcanzar estos estándares significa además, una importante condición para participar en las negociaciones comerciales con importantes mercados como los de la Unión Europea, cuyas directivas y normativas exigen que los países con los cuales se tengan relaciones de este tipo demuestren que tienen estándares similares de protección a los ofrecidos en los países miembros. En momentos en que el país (en conjunto con las otras naciones centroamericanas) se encuentra negociando un tratado de libre comercio con los Estados Unidos y con el posible lanzamiento del ALCA a mediano plazo, la necesidad de establecer un adecuado y moderno estatuto jurídico de la privacidad resulta a todas luces indispensable. De lo contrario, podría Costa Rica adquirir, al cabo de algunos años, la muy poco deseable etiqueta de paraíso del tráfico de datos personales, con insospechables consecuencias en nuestras pretensiones de ser parte del mercado global y una significativa pérdida de credibilidad en los foros internacionales que siempre han visto a esta Nación como un caso excepcional dentro del área.

2. La necesidad de una legislación de tutela frente al tratamiento de datos personales.

Las tecnologías de la información y la comunicación han hecho posible que se construyan los instrumentos indispensables para que el advenimiento de una sociedad panóptica se encuentre a la vuelta de la esquina. Ya no es posible mantener en el ámbito privado ciertos aspectos de nuestra personalidad, como los deseos, las apetencias, las inclinaciones comerciales, religiosas, políticas o hasta intelectuales. Basta con dar seguimiento a las pautas de consumo o de visita de un ciudadano, lo que es hoy muy sencillo gracias a los servicios de compra electrónicos, para conocer cuál es el perfil individual de un ciudadano o incluso los perfiles de un grupo de ciudadanos, lo que lo reduce en su dignidad y lo convierte en un verdadero objeto de los procesos de información¹.

Esta grave condición de la sociedad en que vivimos puede conducir, como lo advierten estudiosos de la materia, como el profesor de la Universidad de Frankfurt del Meno, Dr. Spiros Simitis y el vicepresidente

del Tribunal Constitucional Alemán, Prof. Dr. Winfried Hassemer, a que los derechos individuales se conviertan en letra muerta, al conducir al ciudadano a un verdadero estado de pánico y a una resistencia a ejercer sus derechos individuales ante el riesgo de ser observado y catalogado durante el proceso de su ejercicio como ciudadano. Sería como derogar su "status civitatis" por la vía de garantizar sólo formalmente su condición de ciudadanía, un riesgo que no puede correr una sociedad que se considere democrática.

Si un ciudadano no tiene una capacidad de interactuar en esta sociedad tecnológica con aquellos que pretenden controlarle y perfilarlo, se le estaría quitando la última posibilidad para ratificar su estatus de individualidad. Si el ciudadano no tiene posibilidad de controlar quién tiene acceso a sus datos, con qué objetivos y bajo qué presupuestos, pronto tendrá que desistir del ejercicio de sus derechos fundamentales, ya que muchas libertades públicas (como la libertad de asociación y de reunión, así como las libertades de expresión y de autodeterminación) se convertirían en meras formas sin contenido, ya que aumentarían al mismo tiempo las posibilidades para la manipulación a fin de impedir o al menos amedrentar a quienes deseen ejercer tales libertades, no con prohibiciones directas, sino con la aplicación de consecuencias indirectas al mero ejercicio de un derecho. Si el ciudadano tiene acceso a sus datos, podría controlar y dirigir el sentido social de los mismos, a fin de evitar consecuencias nefastas no a su esfera íntima de manera directa, sino a su posibilidad de participación social.

El derecho a la protección de la persona frente al procesamiento de sus datos personales surge así como una necesidad en el Estado de Derecho, como una necesidad de reflexión sobre los derechos y las libertades públicas en juego, como también de las posibilidades de la persona humana en una sociedad tecnológica.

3. Fundamento constitucional para una tutela del ciudadano frente al tratamiento de sus datos personales.

El respeto a la dignidad humana es un derecho constitucional que tiene dos importantes elementos, por una parte la consideración de que es indispensable acordar a la persona un derecho a su autodeterminación, y, por otra parte, un derecho a interactuar en la sociedad como un eje de imputaciones jurídicas. La posibilidad de respetar la dignidad humana en la sociedad tecnológica, implica que la persona pueda realizar su plan de vida, libremente escogido, sin temor a ser perseguido por la expresión de sus decisiones o su escogencia de caminos para alcanzar sus metas personales, siempre que ello no implique la lesión de esos mismos derechos en otras personas.

La tutela tradicional del ciudadano desde la perspectiva de la intimidad ha demostrado ser insuficiente en la actual sociedad de la información. Esto último es especialmente cierto si se toman en cuenta las nuevas condiciones en que los seres humanos se comunican e interactúan. Cuando la mayor parte de las comunicaciones de los ciudadanos se producen mediante el empleo de tecnología, dicha tecnología define las nuevas condiciones de regulación, las cuales se alejan, cada vez más, de las usuales consideraciones normativas. Como se ha dicho recientemente, la nueva protección de la esfera de la vida privada está definida por la posibilidad de alcanzar una tutela posible de la información. Como lo señala correctamente el autor español Antonio Pérez Luño, la definición de esta tendencia de concebir la "privacy" como una posibilidad del control de informaciones se encuentra ya en el libro de Alan Westin "Privacy and Freedom", quien a finales de la década de los años sesenta años planteó el derecho del ciudadano a controlar las informaciones sobre sí mismo: "a right to control information about one self". Esta tendencia también fue seguida por Lusky (Invasion of Privacy) y por Fried (Privacy, 1968), ambos subrayando claramente la necesidad de que los ciudadanos controlen la información que les concierne, ya no como un mero derecho de defensa frente a las intromisiones de otros, sino ahora, y frente a los riesgos tecnológicos, como un derecho activo de control sobre el flujo de informaciones que circulan sobre sí mismos.

La justificación para otorgar este "status positivus"² del ciudadano se vincula directamente con la tutela de la dignidad de la persona humana, con la necesidad de proteger el libre desarrollo de la personalidad, y con el afianzamiento de la libertad en la sociedad democrática, ya que el control de las informaciones "...aparece como una condición para una convivencia política democrática"³.

Como puede desprenderse claramente de los asertos anteriores, no se pretende limitar el tratamiento electrónico de los datos que es, en sí mismo, una condición para el desarrollo económico de los países. De lo que se trata es de fomentar el control en contra de los abusos con los datos

¹ En Costa Rica ya se han presentado casos graves relacionados con el manejo de datos personales. El mismo proyecto de Ley para introducir el Habeas Data en Costa Rica, relata los prejuicios que se le causaron a un ciudadano al ser incluido injustamente, sin su consentimiento y sin saberlo, en un listado de morosos de un banco, luego de muchas gestiones, y más de tres años de no obtener ningún crédito producto de su inclusión en ese listado, logró, por intermedio del Defensor del Pueblo, que se le excluyera de esa lista. Casos como ese han de ser muy frecuentes y probablemente son sólo la punta del iceberg de una problemática muy compleja que causa daños a muchos ciudadanos. Cfr. la referencia a este caso en la exposición de motivos del proyecto de Ley presentado por el ex diputado Dr. Constantino Urcuyo, bajo el Expediente N° 12827, con el título "Adición de un nuevo capítulo IV, denominado Del Recurso de Habeas Data", al título III, de la Ley de la Jurisdicción Constitucional, Ley N° 7135, de 19 de octubre de 1989.

² La teoría iuspublicista de los "status" iniciada por Jellinek se busca completar hoy día con la propuesta de introducir un "status positivus socialis", que abarcaría los intereses económicos, culturales y sociales. El Prof. Erhardt Denninger de Frankfurt del Meno postula asimismo la existencia de un "status activus processualis", el cual tiene como fundamento la facultad de la persona de participar activamente en los procesos que le afectan, así como en las organizaciones encargadas de la tutela de sus derechos. Cfr. a este respecto, Pérez Luño, Antonio, La tutela de la Libertad Informática, en: Agencia de Protección de Datos, Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, 1996, pp. 94-95.

³ Así, Pérez Luño, Antonio, Los Derechos Humanos en la Sociedad Tecnológica, en: Losano/Pérez Luño/Guerrero Mateus, Libertad Informática y Leyes de Protección de Datos Personales, Madrid, Centro de Estudios Constitucionales, 1989, p. 330.

y las informaciones, afianzando los derechos y las garantías del ciudadano, y promocionando la participación social de todos en la construcción de mejores condiciones para la comunicación y la producción de conocimiento.

El derecho a la tutela frente a los abusos en el tratamiento de las informaciones es solo un correlato del derecho a la información, que es una de las bases trascendentales para fundar un moderno estado democrático. Si la moderna sociedad depende de que las informaciones circulen, entonces también debe construirse una verdadera ética informativa, que no solo acarree una nueva forma de entender el manejo y tratamiento de las informaciones, sino también la sistemática tendencia hacia la transparencia, evitando, de esta manera, que los datos se sistematicen, se procesen y se utilicen de espaldas a los afectados, lesionándolos en sus intereses económicos, pero sobre todo en sus posibilidades de interacción social. Lograr esto y alcanzar al mismo tiempo las condiciones para la sociedad de mercado es un importante reto para el legislador y una complicadísima situación de ponderación de intereses, donde entran en juego no sólo las necesidades de información de la sociedad, y la nueva configuración de las relaciones económicas entre los países, sino que habrá de considerarse igualmente el interés del ser humano no sólo a gozar de mayor información en todos los ámbitos del conocimiento y de la cultura (freedom of information), como también la necesidad de tutelar a la persona frente al uso desmedido de sus datos personales.

La correlación práctica y posible de los intereses en juego ya planteados, consistentes en la necesidad de la tutela individual del ciudadano y de las condiciones de desarrollo de una verdadera economía electrónica, basada en la circulación de informaciones de la más variada índole, ha llevado a los estados a explorar la concordancia práctica de las variables económicas con un derecho denominado "derecho a la autodeterminación informativa". Se trata, a no dudarlo, de un redimensionamiento del derecho a la intimidad, que cobra una nueva jerarquía normativa por su concordancia práctica con otros derechos constitucionales tales como el derecho a la protección de la dignidad humana, a la libertad individual, a la autodeterminación y el principio democrático, que antes de ser utilizados como puntos de sustentación vacíos y sin contenido, adquieren una nueva perspectiva en el Estado de Derecho.

4. La diferencia de los estándares de tutela alcanzables por medio de través del hábeas data y las leyes de tutela de la persona frente al tratamiento de informaciones.

Es de cita frecuente que las leyes de protección frente al tratamiento de datos personales son innecesarias si existe una adecuada protección constitucional mediante amparos especiales, denominados en nuestro margen cultural "recursos de hábeas data".

En realidad, los recursos de hábeas data no son más que instrumentos o mecanismos de garantía procesal que se acuerdan a favor de las personas que han sufrido una lesión en su ámbito de intimidad producto de usos abusivos de sus datos o informaciones. Se trata, en general, entonces, de un derecho procesal reactivo frente a una lesión ya ocasionada. No tienen una vocación preventiva de las lesiones y sus efectos son casi siempre acordados a favor del afectado y no tienen efectos extensivos hacia quienes sufren las mismas lesiones.

Es curioso, y este es un fenómeno que merece mayor estudio e investigación, que en el ámbito latinoamericano la gran evolución hacia ley de tutela se haya convertido en una mera reglamentación del hábeas data, el cual, en teoría, depende más bien del desarrollo de la jurisprudencia de tutela que vayan sentando los tribunales constitucionales, la cual, en el caso de Costa Rica, ha sido cada vez más generosa. Este avance de la jurisprudencia nacional en materia de hábeas data hace conservar la esperanza de que, tarde o temprano, podremos contar con un estándar de tutela reactivo de indudable importancia⁴. No obstante, al igual que en otros países, aún es necesario acordar tutelas preventivas, que reaccionen antes de que se ocasionen riesgos de incalculables proporciones para una gran cantidad de ciudadanos.

El estado actual de la discusión en América Latina se debate entre impulsar reformas legislativas que garanticen facultades de control sobre las informaciones personales de los ciudadanos y la necesidad de incorporar prescripciones constitucionales que amplíen la tutela que recibe la intimidad.

⁴ La jurisprudencia de la Sala Constitucional ha evolucionado notablemente desde los fallos de la primera etapa en contra de los archivos criminales administrados por el Organismo de Investigación Judicial. En una de las primeras sentencias se considera el suministro de informaciones conservados en ese archivo a terceras personas como lesivo al principio de legalidad y a la dignidad de la persona. Una segunda sentencia se muestra más tímida cuando considera que es posible que ese archivo criminal pueda conservar los registros individuales aun después de su vencimiento. Posteriormente, y ya en el orden de fallos más reciente, el Voto 4154-97, ya habla expresamente del hábeas data y su regulación, planteando que el objeto de este recurso es la protección a conocer o rectificar la información pública o privada que exista sobre ella. El Voto 1345-99, dos años después, abre la posibilidad de una tutela de acceso, con base en el derecho a la autodeterminación informativa, para que la gente pueda conocer las informaciones que sobre ellas se encuentren allí registradas, e incluye una descripción de los derechos que lo asisten. En un fallo más sistematizado, el 5802-99, la Sala Constitucional entra a analizar el registro y los bancos de datos y los objetivos del hábeas data, así como los principios que rigen el ejercicio de estos derechos.

En América Latina se han decidido por la constitucionalización de este derecho Colombia y Brasil⁵, también Paraguay en la Constitución de 1992 (art. 136) y Ecuador en su reciente Constitución, de 18 de junio de 1996⁶; y en Argentina la Constitución de las provincias de Jujuy, La Rioja, San Juan; Córdoba; San Luis; Río Negro, Tierra del Fuego y Buenos Aires han incorporado cláusulas referidas a la informática y a la protección de la intimidad. La Constitución de la República de Argentina de 1994 ha establecido la acción de amparo para "...conocer los datos a ella referidos, así como su finalidad, contenidos en registros públicos y privados, y en caso de ser ellos falsos o discriminatorios, exigir su supresión, rectificación, actualización y confidencialidad". Existe legislación en materia de tratamiento de datos en Argentina, Chile y Paraguay.

Portugal fue el primer país europeo que constitucionalizó en el artículo 35 de su Ley Fundamental (1976) el derecho de los ciudadanos a controlar las informaciones que sobre ellos circulan, sin embargo, no sería sino hasta 1991 que finalmente se reguló por ley los aspectos concretos de esta declaración. El segundo país europeo en reconocer constitucionalmente la necesidad de tutelar al ciudadano frente a los riesgos de la informática fue España, país que tardó también catorce años en poner en práctica una ley que diera los mecanismos necesarios para alcanzar la mencionada tutela.

En la República Federal de Alemania, la mayoría de las Constituciones de los Länder o Estados han incorporado el derecho a la autodeterminación informativa como uno más en el elenco de los derechos fundamentales.

Actualmente cuentan con leyes de tutela también Alemania, Bélgica, Dinamarca, Francia, Irlanda, Luxemburgo, Países Bajos, el Reino Unido, Austria, Finlandia, Islandia, Grecia⁷, Noruega y Suecia. También Canadá y Japón. Italia aprobó a inicios de mayo de 1997 su Ley de Protección de Datos⁸.

Estas leyes demostraron ser esenciales como complemento de las garantías generales del Estado de Derecho, no sólo como limitativas de esas ansias exorbitadas de información del Estado, sino también como un método práctico y razonable para que el ciudadano pudiera acceder a sus propios datos, almacenados en diversas bases o bancos de datos, y ejercer un control sobre ellos.

5. Una ley de protección de la persona frente al tratamiento de datos en Costa Rica en la coyuntura actual de desarrollo de nuestra sociedad de la información.

En 1996 hubo una iniciativa legislativa, impulsada por el entonces diputado Constantino Urcuyo, para introducir en Costa Rica una regulación específica al hábeas data en la Ley de la Jurisdicción Constitucional. Se trataba de diseñar una reglamentación para una forma de amparo específico en materia de tutela de la identidad o libertad informáticas. Un proyecto importante para la época, que inició el debate dogmático sobre este importante tema y dejó un antecedente trascendental para propuestas posteriores como la que ahora se presenta al debate legislativo. Sin embargo, el proyecto de ley que hoy se presenta se aleja de una regulación específica del hábeas data, que en el interín se ha convertido en un instrumento de tutela reactivo que ha sido ampliamente aplicado por nuestra Sala Constitucional, tomando como base la misma Ley de la Jurisdicción Constitucional, así como la interpretación amplia y garantista que la propia Sala ha hecho del artículo 24 de la Constitución Política.

Luego de la propuesta original del Dr. Urcuyo, hoy resulta indispensable transitar nuevos caminos y ofrecer al país una regulación integral del derecho a la autodeterminación informativa, completando la

⁵ El tema del hábeas data en Brasil parece iniciarse con motivo de la preocupación del Prof. José Alonso da Silva por conceder un medio para que los ciudadanos tuvieran acceso a las informaciones que sobre ellos estuvieran registradas por entidades públicas y privadas. Para ello conformó una Comisión Provisoria de Estudios Constitucionales, presidida por el Dr. Alonso Arinos de Mello Franco, la cual empezaría a trabajar para encontrar un medio expedito que, al igual que el habeas corpus, permitiera la ciudadanía acceso a estas informaciones. Después vendrían otros proyectos, como el "Muda Brasil" y el "Proyecto de Constitución de la Comisión de Sistematización", los cuales irían también en el mismo sentido, poniendo especial atención al acceso a informaciones en manos de entidades policiales y militares. Sobre la evolución de estos proyectos cfr. Nusdeo, Marcos y Folgosi, Rosolea, "Hábeas Data", en: RDP-87, Brasil, pp. 90 ss.

⁶ Artículo 30 de la Constitución de la República de Ecuador, Ley N° 000. R0/969, de 18 de junio de 1996. "Toda Persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma o sobre sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su finalidad. Igualmente podrá solicitar ante funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquellas si fueran erróneas o afectaren ilegítimamente sus derechos.

⁷ Se exceptúan los documentos reservados por razones de seguridad nacional". Grecia puso en vigencia su ley de protección de la persona frente al tratamiento de datos personales el 19 de marzo de 1997.

⁸ Ley N° 675 del 31 de diciembre de 1996: Tutela delle persone e di altri soggetti rispetto al trattamento di dati personali, publicada en el Supplemento ordinario alla "Gazzetta Ufficiale", Nr. 5 del 9 de enero de 1997, que entró en vigencia el 8 de mayo de 1997. La ley ha sido recientemente reseñada por Losano, Mario, Das italienische Datenschutzgesetz, en: Revista Computer und Recht (Alemania). Nr. 5 de 1997. p. 308 (Nota al pie 2).

tutela reactiva que ya ofrece nuestro máximo tribunal constitucional. Es necesario, pues ofrecer una propuesta que ofrezca mecanismos preventivos, a la altura del desarrollo tecnológico incesante que parece poner en entredicho todas las propuestas legislativas imaginables que se han venido dando en el Derecho Comparado.

El actual proyecto parte de la premisa de que la vía del hábeas data ya ha sido adecuadamente aplicada por la Sala Constitucional, y ya ha ido ampliándose su uso, incluso, para establecer ciertos elementos de calidad en el tratamiento de datos. Resulta evidente, entonces, que debe incluirse en una legislación una consideración amplia de las etapas del tratamiento de la información que forman parte normal de todos los procesos informativos en el ámbito público y privado, incluyendo, por supuesto, el flujo transfronterizo de datos.

Para ello, el proyecto está dividido en cinco capítulos: el primero llamado disposiciones generales que se refiere al objeto y fin de la iniciativa, así como una lista de definiciones de algunos de los conceptos contenidos en su articulado, procurando siempre emplear únicamente los más aceptados por la doctrina de vanguardia.

El capítulo II principios básicos para la protección de datos regula con detalle los diversos aspectos relacionados con el derecho de las personas respecto del manejo de sus datos, reconociendo los deberes de obtención del consentimiento del afectado, calidad, seguridad y cesión de los datos, categorías de datos que requieren de una protección mayor a la regla general (datos sensibles), garantías efectivas de acceso a la información personal, corrección, supresión y actualización de la misma. Prevé asimismo, la posibilidad de que las entidades públicas y privadas diseñen sus propios protocolos de actuación en materia de protección de datos para que, una vez aprobados por la Agencia para el Control de Datos Personales (PRODAT), permitan a dichas entidades una actuación ágil y sencilla, en tanto se sometan a los términos de sus propios protocolos.

Un capítulo III lleva como título Movimiento internacional de datos, estableciendo como regla general la imposibilidad de que los administradores de archivos públicos o privados, transfieran a terceras personas en el extranjero, informaciones pertenecientes a otros. Se exceptúan de la anterior regla los casos en que el titular de los datos haya dado válidamente su consentimiento o bien el PRODAT haya autorizado la cesión y la empresa receptora esté domiciliada y actúe en un país que ofrezca un nivel adecuado de protección de datos personales.

El capítulo IV De la Agencia para la Protección de Datos Personales (PRODAT) regula la naturaleza jurídica, estructura interna y atribuciones del PRODAT. Se busca con ello dotar al país de un órgano regulador del tratamiento de datos personales, dotado de suficiente independencia y de las herramientas técnicas y material humano necesarios para llevar a cabo su trabajo en forma efectiva y objetiva. No se pretende crear una abultada y tradicional estructura administrativa, sino una unidad de dimensiones moderadas, pero integrada por profesionales calificados con acceso a las últimas tecnologías en materia de informática y apenas el personal de apoyo indispensable, a fin de que su creación no implique una significativa carga en el presupuesto de la República y a la vez pueda cumplir con su objetivo. Se trataría de un órgano dotado de independencia funcional, adscrito al Poder Legislativo, con una naturaleza jurídica similar a la de la Defensoría de los Habitantes de la República, para así garantizar su imparcialidad en la protección de los derechos de las personas. Sus funciones propuestas son tanto preventivas (inscripción y autorización de las bases de datos y protocolos de actuación, inspecciones oficiosas, etc.) como reactiva (atención de denuncias, imposición de órdenes y sanciones administrativas, etc.). A la cabeza del órgano se propone elegir a una persona con experiencia, capacidad y solvencia moral suficientes para afrontar el reto de defender a las personas ante las diversas entidades, públicas y privadas, sin importar su investidura o poder. El PRODAT estaría compuesto por cinco órganos: la dirección, la subdirección, el Registro de archivos y bases de datos, el Departamento de Inspección y el Departamento de Divulgación, este último encargado de crear conciencia entre los habitantes y el mercado acerca de la necesidad de velar por el buen uso de sus datos.

Un capítulo V regularía los procedimientos de intervención en archivos y bases de datos, el régimen sancionatorio aplicable a los administradores de ficheros y los procedimientos internos para ejercer la competencia disciplinaria contra los funcionarios de la Agencia.

Por las razones expuestas sometemos a consideración de las señoras y los señores diputados el presente proyecto de ley.

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA, DECRETA:

LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES

CAPÍTULO I

Disposiciones generales

SECCIÓN ÚNICA

Artículo 1°—**Objetivo y fin.** La presente Ley tiene como objetivo garantizar a cualquier persona física o jurídica, sean cuales fueren su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida privada y demás derechos de la personalidad; asimismo, la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Artículo 2°—**Definiciones.** A los efectos de la presente Ley:

- Datos de carácter personal:** cualquier información relativa a una persona física o jurídica identificada o identificable;
- Datos sensibles:** datos personales que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, información referente a la salud, vida sexual y antecedentes delictivos.
- Archivo, registro, fichero o base de datos:** Conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, automatizado o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso
- Tratamiento automatizado:** operaciones que a continuación se indican, efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: registros de datos, aplicación a esos datos de operaciones lógico aritméticas, su modificación, borrado, extracción o difusión.
- Autoridad encargada del fichero:** significa la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sea competente con arreglo a la ley para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.
- Afectado:** persona o jurídica, titular de los datos que sean objeto del tratamiento automatizado o manual.
- Disociación de datos es:** tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

CAPÍTULO II

Principios básicos para la protección de los datos

Artículo 3°—**Derecho de información en la recolección de los datos.** Las personas a quienes se soliciten datos de carácter personal deberán ser previamente informados de modo expreso, preciso e inequívoco directamente o por apoderado con poder o cláusula especial; las personas jurídicas por medio de su representante legal o apoderado con poder o cláusula especial:

- De la existencia de un fichero automatizado o manual de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se les formulen.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercer los derechos de acceso, rectificación, actualización, cancelación y confidencialidad.
- De la identidad y dirección del responsable del fichero.

Cuando se utilicen cuestionarios u otros impresos para la recolección, figurarán en los mismos en forma claramente legible, las advertencias a que se refiere el apartado anterior.

No será necesaria la información a que se refiere el apartado a), si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de la circunstancia en que se recaban.

Artículo 4°—**Consentimiento del afectado.**

- El titular de los datos deberá dar por sí o por su representante legal o apoderado el consentimiento para la entrega de los datos, salvo que la ley disponga otra cosa dentro de los límites razonables. La razonabilidad deberá ser considerada por la Agencia de Protección de Datos Personales si se le plantea en caso de controversia. Lo anterior vale tanto para los ficheros de titularidad pública o privada.

El consentimiento deberá constar a través de autorización por escrito o por otro medio idóneo, físico o electrónico. Dicho consentimiento podrá ser revocado sin efecto retroactivo, por cualquiera de los medios permitidos para acreditar la aquiescencia. No será necesario el consentimiento cuando:

- Exista orden motivada, dictada por autoridad judicial competente.
- Los datos se obtengan de fuentes de acceso público irrestricto y se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, y fecha de nacimiento.

Artículo 5°—**Calidad de los datos.**

- Sólo podrán ser recolectados, almacenados y empleados datos de carácter personal para su tratamiento automatizado o manual, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimos para los que se han obtenido.
- Los datos de carácter personal objeto de tratamiento automatizado o manual no podrán utilizarse para finalidades distintas de aquellas para las cuales los datos hubieran sido recogidos.
- Dichos datos serán exactos y puestos al día, de forma que respondan con veracidad a la situación real del afectado.

- 4) Si los datos de carácter personal registrados resultaren ser inexactos en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas, actualizados o complementados. Igualmente serán cancelados si no mediare un consentimiento legal y legítimo o estuviere prohibida su recolección.
- 5) Los datos de carácter personal serán cancelados cuando hayan dejado de ser pertinentes o necesarios para la finalidad para la cual hubieren sido recibidos y registrados.
No serán conservados en forma que permita la identificación del interesado en un período que sea superior al necesario para los fines con base en los cuales hubieren sido recabados o registrados. Sin embargo, en ningún caso serán conservados los datos personales que puedan de cualquier modo afectar a su titular, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados.
- 6) Serán almacenados de forma tal que se garantice plenamente el derecho de acceso por el afectado.
- 7) Se prohíbe el acopio de datos por medios fraudulentos, desleales o ilícitos.
- 8) Se prohíbe registrar o archivar juicios de valor.

Artículo 6°—Categorías particulares de datos. Los datos de carácter personal de las personas físicas que revelen su origen racial, sus opiniones políticas, sus convicciones religiosas o espirituales, así como los datos de carácter personal relativos a la salud, a la vida sexual y a sus antecedentes delictivos, no podrán ser almacenados de manera automática ni manual en registros o ficheros privados, y en los registros públicos serán de acceso restringido.

Ninguna persona estará obligada a suministrar datos sensibles. Los datos sensibles sólo podrán ser recolectados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

Sin perjuicio de lo establecido en el párrafo anterior, las asociaciones religiosas, las organizaciones políticas, sindicales y aquellas que agrupen a los individuos de acuerdo con sus preferencias sexuales o ideológicas, podrán llevar un registro de sus miembros, para uso exclusivo de su fin asociativo.

Artículo 7°—Seguridad de los datos.

- 1) Todo archivo, fichero, registro o base de datos, público o privado destinado a proporcionar informes debe inscribirse en el Registro de archivos y bases de datos contemplado en el artículo 25 de la presente Ley.
- 2) El responsable del fichero deberá adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- 3) No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que garanticen plenamente su seguridad e integridad y los de los centros de tratamientos, equipos, sistemas y programas.
Por vía de reglamento, se establecerán los requisitos y las condiciones que deban reunir los ficheros automatizados y los manuales y las personas que intervengan en el acopio, almacenamiento y uso de los datos.
- 5) El responsable del fichero y quienes intervengan en cualquier fase del proceso de recolección y tratamiento de los datos de carácter personal, están obligados al secreto profesional.

Artículo 8°—Cesión de datos. Los datos de carácter personal conservados en archivos o bases de datos públicos o privados, sólo podrán ser cedidos a terceros para fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del afectado, en los términos del artículo 4° de esta Ley.

El consentimiento para la cesión podrá ser revocado pero la revocatoria no tendrá efectos retroactivos.

Lo anterior es aplicable a cualquier fichero independientemente de su titularidad pública o privada.

El consentimiento no será exigido cuando:

- a) Así lo disponga una ley.
- b) Se trate de la cesión de datos personales al Estado o una institución pública de salud o de investigación científica en el área de la salud, relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.

El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y este responderá solidariamente y conjuntamente por la observancia de los mismos ante la Agencia de Protección de Datos y el titular de los datos.

Artículo 9°—Derechos y garantías de las personas. Se garantiza el derecho de toda persona a:

- c) Obtener a intervalos razonables y sin demora o gastos excesivos, la confirmación de la existencia de datos suyos en archivos o bases de datos, así como la comunicación de dichos datos en forma inteligible.
- d) La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación de los términos técnicos que se utilicen.
- e) La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.
- f) La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, u otro medio idóneo a tal fin, siempre y cuando en este proceso se tomen las previsiones necesarias para que dicha información no sea modificada o utilizada por terceros.
- g) Obtener, llegado el caso, la rectificación de dichos datos y su actualización o la eliminación de los mismos cuando se hayan tratado con infracción a las disposiciones de la presente Ley.

La autoridad o el responsable del fichero deben cumplir con lo pedido gratuitamente y resolver en el sentido que corresponda en el plazo de cinco días contado a partir de la recepción de la solicitud.

Artículo 10.—Garantías efectivas.

- 1) Todo afectado tiene derecho a un recurso administrativo sencillo y rápido ante la Agencia de Protección de Datos, con el fin de ser amparada contra actos que violen sus derechos fundamentales reconocidos por esta Ley. Lo anterior sin perjuicio de las garantías jurisdiccionales generales o específicas que la Ley establezca para este mismo fin.
- 2) Toda persona tiene derecho a controlar que sus datos personales existentes en ficheros públicos o particulares cumplan con las reglas previstas en esta Ley, y a obtener en su caso la correspondiente indemnización por los daños y perjuicios que hubieren sido ocasionados en su persona o intereses debido al uso de sus datos personales.

Artículo 11.—Del derecho de acceso a la información. El derecho de acceso a la información garantiza las siguientes facultades del afectado:

- a) Acceder directamente o conocer las informaciones y los datos relativos a su persona.
- b) Conocer la finalidad de los datos a él referidos y al uso que se haya hecho de los mismos.
- c) Solicitar y obtener la rectificación, actualización, cancelación o eliminación y el cumplimiento de la garantía de confidencialidad respecto de sus datos personales.

Artículo 12.—Excepciones y restricciones al derecho a la autodeterminación informativa del ciudadano. Sólo por ley se podrán establecer excepciones y restricciones en los principios, derechos y garantías aquí enunciados, siempre que aquellas sean justas, razonables y acordes con el principio democrático. Las mencionadas excepciones y restricciones solo podrán plantearse para alcanzar fines legales en alguno de los siguientes campos:

- a) La protección de la seguridad del Estado, de la seguridad pública, de la seguridad económica del Estado o para la represión de las infracciones penales.
- b) La protección de las propias personas concernidas, así como los derechos y las libertades de otras personas.
- c) El funcionamiento de ficheros de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existe riesgo de que las personas sean identificadas.

Siempre existirá recurso para que la autoridad judicial decida si en un caso concreto estamos ante una excepción o restricción razonable.

Artículo 13.—Protocolos de actuación. Las personas físicas y jurídicas, públicas y privadas, que tengan entre sus funciones la recolección, almacenamiento y uso de datos personales, podrán emitir un protocolo de actuación, en el cual establecerán los pasos que deberán seguir, en la recolección, almacenamiento y manejo de los datos personales, de conformidad con las reglas previstas en esta Ley.

Para ser válidos, los protocolos de actuación deberán ser inscritos ante el Registro de archivos y bases de datos. La Agencia de Protección de Datos Personales podrá, en cualquier momento, verificar que el titular del archivo esté cumpliendo cabalmente con los términos de su código de conducta.

La manipulación de datos con base en un protocolo de actuación inscrito ante la Agencia hará presumir (*iuris tantum*) el cumplimiento de las disposiciones contenidas en esta Ley, para los efectos de autorizar la cesión de los datos contenidos en un archivo o base.

CAPÍTULO III

Movimiento internacional de los datos

SECCIÓN ÚNICA

Artículo 14.—Transferencia internacional de los datos, regla general. Las personas públicas y privadas encargadas del manejo de bases de datos y los archivos físicos, estarán imposibilitadas para transferir datos que hayan recibido directamente de los titulares de la información o de terceros.

Se exceptúan de la prohibición contenida en el párrafo anterior las transferencias ocurridas con absoluto arreglo a las siguientes reglas:

- Que la Agencia para la Protección de Datos Personales autorice la transferencia a la persona o institución receptora, pública o privada, por corroborar que con dicho traslado no están siendo vulnerados los principios rectores del manejo de datos personales, descritos en esta Ley.
- Que el titular de la información haya autorizado expresa y válidamente tal transferencia.
- Si se trata de una persona o institución pública o privada domiciliada en el extranjero, dicha transferencia solo podrá ser llevada a cabo si, además de las condiciones antes mencionadas, dicho receptor está domiciliado o tiene como base un país que ofrezca un nivel de protección de los datos personales, igual o superior al establecido en Costa Rica.

CAPÍTULO IV

Agencia para la Protección de Datos Personales

(PRODAT)

SECCIÓN I

Disposiciones generales

Artículo 15.—Agencia para la Protección de Datos Personales. Créase un órgano adscrito al Poder Legislativo denominado Agencia para la Protección de Datos Personales (PRODAT), el cual gozará de independencia funcional, administrativa y de criterio en el desempeño de las funciones que esta Ley le encomienda.

Artículo 16.—Atribuciones. Son atribuciones de la Agencia para la Protección de Datos Personales, además de las otras que le impongan esta u otras normas, las siguientes:

- Velar por el cumplimiento de la normativa en materia de protección de datos, tanto por parte de personas físicas como por entes y órganos públicos y privados.
- Llevar un registro de los archivos y bases de datos, en soporte físico e informático, que sean propiedad o estén en administración tanto de personas físicas como de entes y órganos públicos y privados.
- Requerir, de las personas físicas y jurídicas, públicas y privadas, que posean o administren archivos y bases de datos de las descritas en el capítulo I de esta Ley, las informaciones necesarias para el ejercicio de su cargo. Podrá incluso acceder a los archivos y bases de datos en cuestión, a efecto de hacer cumplir efectivamente las normas sobre protección de datos personales.
- Autorizar, previa verificación de los requisitos respectivos y las reglas sustantivas, la transferencia de los datos entre los archivos y las bases de datos inscritos en el registro de archivos y bases de datos o entre estos y otras personas o compañías.
- Recibir de las personas los reclamos por infracción a las normas sobre protección de los datos personales.
- Ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación, de las informaciones contenidas en archivos y bases de datos, cuando contravengan las normas sobre protección de los datos personales.
- Imponer las sanciones administrativas establecidas en la Ley para las personas físicas o jurídicas, públicas o privadas, que infrinjan las normas sobre protección de los datos personales, de acuerdo con las faltas previstas en la Ley.
- Remitir anualmente, un informe escrito de sus labores a la Asamblea Legislativa, en la primera semana de junio, y comparecer en la penúltima semana de junio ante el Plenario Legislativo, para defender oralmente su informe. Una versión abreviada de este informe deberá ser publicado en el Diario Oficial y en algún diario de circulación nacional.
- Promover y contribuir en la redacción de proyectos de ley tendientes a implementar las normas sobre protección de los datos personales.
- Emitir los reglamentos necesarios a fin de regular su régimen funcional, así como especificar la forma de ejercicio de sus competencias. Deberá seguir los procedimientos establecidos en la Ley General de la Administración Pública para la elaboración de las disposiciones de carácter general.
- Respetando los diversos grados de autonomía administrativa e independencia funcional, dictar las directrices necesarias a efecto de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales.
- Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, almacenamiento, transferencia y uso de sus datos personales.

Artículo 17.—Dirección de la Agencia. La Dirección de la Agencia para la Protección de Datos Personales estará a cargo de un director o directora nacional, quien será designado por la Asamblea Legislativa de una lista de cuatro personas integrada en forma alternativa por sexo, elaborada por la Comisión Especial Permanente de Nombramientos. Si, luego de ser efectuada la votación correspondiente, el Plenario no

nombrare a ninguno de los candidatos o candidatas recomendados por la Comisión, este llevará a cabo una nueva votación. De persistir la situación antes descrita, el Plenario deberá elegir al director o directora nacional de entre cualesquiera de las personas que en tiempo postularon su nombre ante la Comisión, que cumplan los requisitos establecidos en esta Ley y no se encontraren impedidos para el ejercicio del cargo. El director o la directora nacional de protección de datos personales permanecerá en su cargo durante ocho años, y podrá ser reelecto o reelecta hasta por una vez. Durante su gestión, no podrá ser removido sino por justa causa, luego de garantizado el debido proceso, por el voto de la mayoría absoluta de los diputados presentes en el Plenario Legislativo.

Artículo 18.—Requisitos. Para ser nombrado director o directora nacional de Protección de Datos Personales se requiere ser ciudadano costarricense, mayor de treinta y cinco años, profesional al menos en grado de licenciatura en una materia afín al objeto de su función, de reconocida solvencia profesional y moral.

Artículo 19.—Impedimentos. No podrá ser nombrado director o directora nacional de Protección de Datos Personales quien, aún cumpliendo los requisitos establecidos en el artículo anterior, sea propietario, accionista, miembro de la junta directiva, gerente, asesor o empleado de una empresa dedicada a la recolección o almacenamiento de datos personales. Dicha prohibición persistirá hasta dos años después de haber cesado sus funciones.

Estará igualmente impedido quien sea pariente hasta en tercer grado de consanguinidad y afinidad de una persona que esté en alguno de los supuestos mencionados en el párrafo anterior.

Artículo 20.—Subdirección. La Agencia para la Protección de Datos Personales tendrá un subdirector o subdirectora, quien será nombrado por la Asamblea Legislativa, de la misma forma y en las mismas condiciones que el director o la directora nacional. Para ser subdirector o subdirectora, se debe cumplir los mismos requisitos que para ser director o directora nacional. Le cubren, además, las mismas incompatibilidades. Además de las otras funciones que le fijen esta Ley y su Reglamento, al subdirector o subdirectora le corresponderá suplir al director o directora nacional en sus ausencias temporales o permanentes; en este último caso hasta tanto la Asamblea Legislativa nombre a un nuevo director o directora nacional. Por medio del reglamento interno, la dirección le podrá asignar otras funciones específicas.

En caso de que quedaren vacantes los puestos de director o directora y subdirector o subdirectora nacionales, asumirá interinamente la dirección el jefe del Departamento de Inspección de Archivos y Bases de Datos de la Agencia.

Artículo 21.—Alternabilidad y paridad. La Agencia para la Protección de Datos Personales, tendrá alternabilidad y paridad de sexo en los cargos de director o directora y subdirector o subdirectora nacionales. el primer nombramiento determinará como aplicar la paridad y la alternabilidad en las elecciones sucesivas.

Artículo 22.—Personal de la Agencia. La Agencia para la Protección de Datos Personales contará con el personal técnico y administrativo necesario para el buen ejercicio de sus funciones, designado mediante concurso por idoneidad. Deberá capacitar permanentemente a su personal en el manejo de nuevas herramientas tecnológicas y nuevas formas de manejo de datos personales.

Artículo 23.—Prohibiciones. Todos los empleados de la Agencia para la Protección de Datos Personales tienen las siguientes prohibiciones:

- Prestar servicios a las personas o empresas que se dediquen al acopio, almacenamiento o manejo de datos personales. Dicha prohibición persistirá hasta dos años después de haber cesado sus funciones.
- Interesarse personal e indebidamente en asuntos de conocimiento de la Agencia.
- Revelar o de cualquier forma propalar los datos personales a que ha tenido acceso con ocasión de su cargo. Esta prohibición persistirá indefinidamente aún después de haber cesado en su cargo.
- En el caso de los funcionarios nombrados en plazas de profesional, ejercer externamente su profesión. Lo anterior tiene como excepción el ejercicio de la actividad docente en centros de educación superior o la práctica liberal a favor de parientes por consanguinidad o afinidad hasta el tercer grado, siempre que no se esté ante el supuesto del inciso a).

La inobservancia de cualesquiera de las anteriores prohibiciones será considerada falta gravísima, para efectos de aplicación del régimen disciplinario, sin perjuicio de las otras formas de responsabilidad que tales conductas pudieran acarrear.

SECCIÓN II

Estructura interna

Artículo 24.—Organigrama. La Agencia para la Protección de Datos Personales estará compuesta al menos de los siguientes órganos:

- El director o directora nacional.
- El subdirector o subdirectora nacional.
- El registro de archivos y bases de datos.
- El departamento de inspección de archivos y bases de datos.
- El departamento de divulgación.

Para ocupar la jefatura de cualquier departamento, se requiere poseer un título profesional en grado al menos de licenciatura, en una carrera relacionada con el cargo.

Artículo 25.—Registro de archivos y bases de datos. Todo archivo, registro, base o banco de datos público y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite la Agencia de Protección de Datos.

El Registro de archivos y bases de datos es el órgano de la Agencia para la Protección de Datos Personales encargado de inscribir:

- Los archivos y las bases de datos propiedad del Estado u otros entes públicos.
- Los archivos y las bases de datos que pertenezcan o sean administrados por personas de Derecho Privado.
- Los protocolos de actuación a que hace referencia el artículo 13 de esta Ley.
- Cualesquiera otras informaciones que las normas de rango legal o reglamentario le impongan.

El Registro de archivos y bases de datos se encuentra sustraído de la potestad de avocación por parte de quien ocupe la dirección nacional.

Artículo 26.—Departamento de inspección de archivos y bases de datos. Corresponde al Departamento de inspección de archivos y bases de datos la tramitación de las quejas y solicitudes recibidas por personas respecto del uso que esté siendo dado a sus datos personales. Actuará como órgano director del debido proceso, pudiendo llevar a cabo las diligencias de investigación necesarias, incluida la posibilidad de exigir de los archivos y las bases de datos el suministro de la información requerida, así como la inspección in situ de tales archivos y bases de datos. Podrá asimismo adoptar las medidas cautelares necesarias para la efectiva garantía del buen uso de los datos personales.

Mediante un sistema de selección aleatoria permanente deberá garantizar que los archivos y las bases de datos a que se refiere esta Ley, cumplan con las normas para la protección de los datos personales.

Artículo 27.—Departamento de divulgación. Compete al Departamento de divulgación la elaboración y ejecución de una estrategia de comunicación dirigida a permitir que los habitantes conozcan los derechos derivados del manejo de sus datos personales, así como los mecanismos que el ordenamiento prevé para la defensa de tales prerrogativas. Deberá coordinar con los gobiernos locales, la realización periódica de las actividades de divulgación entre los habitantes del cantón.

Le corresponde asimismo promover entre las personas y empresas que recolecten, almacenen o manipulen datos personales, la adopción de prácticas y protocolos de actuación acordes con la protección de dicha información.

CAPÍTULO V

Procedimientos

SECCIÓN I

Disposiciones comunes

Artículo 28.—Aplicación supletoria. En lo no previsto expresamente por esta Ley, y en tanto sean compatibles con su finalidad, serán aplicables supletoriamente las disposiciones del libro II de la Ley General de la Administración Pública.

SECCIÓN II

Intervención en archivos y bases de datos

Artículo 29.—Denuncia. Cualquier persona que ostente un derecho subjetivo o un interés legítimo, puede denunciar ante la Agencia para la Protección de Datos Personales que un archivo o base de datos, público o privado, actúa en contravención de las reglas para el manejo de los datos personales, establecidas en el capítulo I de esta Ley.

Artículo 30.—Trámite de las denuncias. Recibida la denuncia, el Departamento de inspección conferirá al propietario o administrador del archivo o base de datos, un plazo de tres días hábiles, para que se pronuncie acerca de la veracidad de tales cargos. El denunciado deberá remitir los medios de prueba que respalden sus afirmaciones. Si se tratare de una autoridad pública, dicho informe será tenido bajo juramento. La omisión de rendir el informe en el plazo estipulado, hará que se tengan por ciertos los hechos acusados.

En cualquier momento, el Departamento de inspección de archivos y bases de datos podrá ordenar al denunciado la presentación de la información necesaria. Asimismo, podrá efectuar inspecciones in situ en sus archivos o bases de datos. Para salvaguardar los derechos del afectado, puede dictar -mediante acto fundado- las medidas cautelares que aseguren el efectivo resultado del procedimiento.

A más tardar un mes después de la presentación de la denuncia, el Departamento de inspección debe presentar al director o directora nacional una recomendación acerca de la existencia o no de actos lesivos del derecho a la autodeterminación informativa del afectado. cinco días después, el director nacional deberá dictar el acto final. contra su decisión, cabrá recurso de reconsideración dentro del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido, agotando la vía administrativa.

Artículo 31.—Efectos de la resolución estimatoria. Si en su acto final, el director o directora nacional determinare que la información del afectado es falsa, incompleta, inexacta, o bien que de acuerdo con las normas sobre protección de datos personales, la misma fue indebidamente recolectada, almacenada o difundida, deberá ordenar su inmediata supresión, rectificación, adición o aclaración, o bien restricción respecto de su transferencia y difusión. Si el denunciado no cumpliere íntegramente con lo ordenado, estará sujeto a las sanciones previstas en esta y otras leyes.

SECCIÓN III

Régimen disciplinario aplicable a los archivos y bases de datos

Artículo 32.—Trámite. De oficio o a instancia de parte, la Agencia para la Protección de Datos Personales podrá iniciar un procedimiento tendiente a demostrar si un archivo o base de datos de los regulados por esta Ley, está siendo empleado de conformidad con sus principios.

Dictado el acto inicial por parte del director o directora nacional, el Departamento de inspección de archivos y bases de datos se constituirá en órgano director del procedimiento, para lo cual deberá seguir los trámites previstos en la Ley General de la Administración Pública para el procedimiento ordinario. El acto final del procedimiento deberá ser dictado por el director o la directora nacional. Contra su decisión, cabrá recurso de reconsideración dentro de tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido, agotando la vía administrativa.

Artículo 33.—Sanciones. De concluir el director o la directora nacional que la persona física o jurídica ha cometido una de las faltas tipificadas en esta Ley, deberá imponer alguna de las siguientes sanciones:

- Para las faltas leves, una multa hasta cinco salarios base.
- Para las faltas graves, una multa hasta por diez salarios base y suspensión para el funcionamiento del fichero de uno a seis meses.
- Para las faltas gravísimas, una multa hasta por veinte salarios base y la suspensión para el funcionamiento del fichero de uno a cinco años.

Artículo 34.—Faltas leves. Serán consideradas faltas leves, para los efectos de esta Ley:

- La recolección de datos personales para su uso en un archivo o base de datos sin hacer al interesado todas las advertencias especificadas en el artículo 3° de esta Ley.
- Recolectar, almacenar y transmitir datos personales de terceros por medio de mecanismos inseguros o que de alguna forma no garanticen la seguridad e inalterabilidad de los datos.

Artículo 35.—Faltas graves. Serán consideradas faltas graves, para los efectos de esta Ley:

- Recolectar, almacenar, transmitir o de cualquier otra forma emplear datos personales sin el consentimiento expreso del titular de los datos, con arreglo a las disposiciones del artículo 4 de esta Ley.
- Transferir datos personales a otras personas o empresas en Costa Rica en contravención a las reglas establecidas en el artículo 8 de esta Ley.
- Transferir datos personales a otras personas o empresas radicadas en el extranjero en contravención a las reglas establecidas en el artículo 14 de esta Ley.
- Recolectar, almacenar, transmitir o de cualquier otro modo emplear datos personales para una finalidad distinta de la autorizada por el titular de la información.
- Negarse injustificadamente a dar acceso a un interesado sobre los datos que consten en archivos y bases de datos, a fin de verificar su calidad, recolección, almacenamiento y uso conforme a esta Ley.
- Negarse injustificadamente a eliminar o rectificar los datos de una persona que así lo haya solicitado por medio claro e inequívoco.
- Reincidir en la comisión de una de las conductas tipificadas como falta leve.

Artículo 36.—Faltas gravísimas. Serán consideradas faltas gravísimas, para los efectos de esta Ley:

- Recolectar, almacenar, transmitir o de cualquier otra forma emplear, por parte de personas físicas o jurídicas privadas, datos sensibles, según la definición prevista en el artículo 6 de esta Ley.
- Obtener de los titulares o de terceros, datos personales de una persona por medio de engaño, violencia o amenaza.
- Reincidir en la comisión de una de las conductas tipificadas como falta grave.

SECCIÓN IV

Procedimientos internos

Artículo 37.—Régimen disciplinario interno. Para la aplicación del Régimen disciplinario interno de los servidores de la Agencia, el Departamento de inspección funcionará como órgano director del procedimiento, será competencia del director o directora nacional dictar los actos inicial y final. Contra este último cabrá recurso de reconsideración dentro del tercer día, el cual agotará la vía administrativa. En lo no dispuesto expresamente, y en tanto ello sea compatible, será empleado el procedimiento ordinario previsto en la Ley General de la Administración Pública.

Artículo 38.—**Sanciones.** Las faltas leves serán sancionadas con amonestación verbal o escrita. Las faltas graves con amonestación escrita o suspensión sin goce de salario de hasta por un mes. Las faltas gravísimas serán sancionadas con suspensión sin goce de salario hasta por tres meses o con despido sin responsabilidad patronal.

Al imponer la sanción, el jerarca deberá tomar en consideración, además de la gravedad de la falta, el grado de culpabilidad del funcionario y el daño efectivo o peligro causado con su actuación.

Artículo 39.—**Faltas disciplinarias.** Además de las otras conductas previstas en las normas estatutarias aplicables a la Agencia de Protección de Datos Personales, serán consideradas faltas, para la imposición de las sanciones descritas en el artículo anterior, las siguientes:

- Faltas leves: la renuencia injustificada de participar en las actividades de capacitación programadas periódicamente por la Agencia.
- Faltas graves: el atraso indebido en la atención de una denuncia o solicitud de intervención y la reiteración de una falta leve.
- Faltas gravísimas: el incumplimiento a las prohibiciones descritas en el artículo 23 de esta Ley y la reiteración de una falta grave.

Transitorios

Transitorio único.—**Adecuación de los ficheros actuales.** Las personas físicas o jurídicas, públicas o privadas, que en la actualidad son propietarias o administradoras de las bases de datos objeto de esta Ley, deberán adecuar sus procedimientos y reglas de actuación, así como el contenido de sus ficheros a lo establecido en la presente Ley, en un plazo máximo de un año a partir de la entrada en vigor de la misma.

Rige a partir de su publicación.

Margarita Penón Góngora, Rolando Laclé Castro, Carlos Avendaño Calvo, Ruth Montoya Rojas, Luis Gerardo Villanueva Monge, Ricardo Toledo Carranza, Gerardo Vargas Leiva, Rodrigo Carazo Zeledón, Laura Chinchilla Miranda, Edwin Patterson Bent, Luis Ramírez Ramírez, Marta Zamora Castillo, María Lourdes Ocampo Fernández, Daysi Quesada Calderón, José Miguel Corrales Bolaños, Diputados.

NOTA: Este proyecto pasó a estudio e informe de la Comisión Permanente de Asuntos Jurídicos.

San José, 27 de marzo del 2003.—1 vez.—C-363845.—(34397).

N° 15.194

REFORMA DE LOS ARTÍCULOS 11, 17 y 23 DE LA LEY DE RADIO, N° 1758

Asamblea Legislativa:

Los medios de comunicación colectiva en el mundo son una de las herramientas más poderosas con que cuenta el ser humano para informarse y comunicarse. La radio, uno de ellos, ha sido y, es el medio de información por excelencia, ello debido a muchas de las virtudes que este tiene como lo son: barata en comparación con la prensa y la televisión, tecnológicamente accesible, capaz de superar fronteras y distancias largas, intensamente renovada vía Internet y abierta al futuro de la digitalización.

Desde que nace la radio, hasta nuestros días, la misma ha sufrido una transformación enorme, gracias a los cambios del mundo de la información y la tecnología, permitiéndole a este medio un mayor acercamiento con el ser humano independientemente del lugar en donde se encuentre.

Sobre este fascinante tema el Sr. Antonio Checa, en un artículo titulado “La radio y las minorías al inicio del siglo XXI”, “manifiesta; que todos estos cambios profundos favorecen el acercamiento de la radio a las minorías de todo tipo, hasta el punto de que hoy esa radio es mucho más compañera, confidente o cordón umbilical que ningún otro medio”. (Antonio Checa, La radio y las minorías al inicio del siglo XXI).

Pero al igual que la radio ha modificado casi de manera total la tecnología con que inicia su papel en los medios de comunicación, también al mismo tiempo su rol y su papel se ha tergiversado. La radio inicialmente se gesta como un medio especial para difundir mediante emisiones sonoras programas culturales, educativos, artísticos, informativos o de entretenimiento que respondieran al interés general.

No obstante, ese rol ha dejado de cumplirse parcialmente, para dar paso a otro tipo de programas que hoy no transmiten necesariamente programas que pretendan cumplir con la cultura, la educación, el arte o el entretenimiento y por ende no responden precisamente al interés nacional e individual.

Ante estas circunstancias, se creyó indispensable el conocer acerca del desarrollo de la legislación radial que existe en América Latina sobre dicho tema, específicamente en Argentina, Colombia, Panamá, Paraguay, Uruguay, Guatemala y México con el objeto de revisar si en esta legislación existen reformas actuales que contemplen regulaciones y controles en torno a los nuevos problemas que enfrentan hoy los programas que transmite la radio. De dichas legislaciones se elaboró un cuadro que se adjunta seguidamente a esta exposición de motivos, con aquellos artículos que a nuestro criterio recogen ese sentir y muestran en su contenido el interés expreso que existe por controlar todo aquello que atente contra el orden público y la dignidad humana.

Cuadro Comparativo en el cual se muestra la legislación radial en algunos países de América Latina (1977-2002)

ARGENTINA

Ley de Radiodifusión N° 22.285

Artículo 5°.—Los servicios de radiodifusión deben colaborar con el enriquecimiento cultural de la población, según lo exigen los objetivos asignados por esta ley al contenido de las emisiones de radiodifusión, las que deberán propender a la elevación de la moral de la población, como también así respeto de la libertad, la solidaridad social, la dignidad de las personas, los derechos humanos, el respeto por las instituciones de la República, el afianzamiento de la democracia, y la preservación de la moral cristiana.

(Los servicios de radiodifusión deben propender el enriquecimiento cultural y la elevación moral de la población, según lo exige el contenido formativo e informativo que se asigna a sus emisiones, destinadas a exaltar la dignidad de la persona humana, el fortalecimiento del respeto por las instituciones y las leyes de la República y el afianzamiento de los valores inherentes a la integridad de la familia, la preservación de la tradición histórica del país y los preceptos de la moral cristiana. Las emisiones de solaz o esparcimiento recreativo no deben comprometer, ni en su forma ni en su fondo, la efectiva vigencia de los fines enunciados. El contenido de las emisiones de radiodifusión, dentro del sentido ético y de la conformación cívica con que se difunden los mensajes, deben evitar todo cuanto degrade la condición humana, afecte la solidaridad social, menoscabe los sentimientos de argentinidad y patriotismo y resienta el valor estético. Los licenciarios deberán ajustar su actuación a un Código de Ética que instrumentarla autoridad de aplicación de conformidad con las disposiciones de la presente Ley). Sustituido por Decreto 1005/99 Art. 1 Reg.:8.

Objetivos

Artículo 14.—El contenido de las emisiones de radiodifusión propenderá al cumplimiento de los siguientes objetivos:

- Contribuir al bien común, ya sea con relación a la vida y al progreso de las personas o con referencia al mejor desenvolvimiento de la comunidad.
- Contribuir al afianzamiento de la unidad nacional y al fortalecimiento de la fe y la esperanza en los destinos de la Nación Argentina.
- Servir al enriquecimiento de la cultura y contribuir a la educación de la población;
- Contribuir al ejercicio del derecho natural del hombre a comunicarse, con sujeción a las normas de convivencia democrática.
- Promover la participación responsable de todos los habitantes y particularmente del hombre argentino, en el logro de los objetivos nacionales.
- Contribuir al desarrollo de los sentimientos de amistad y cooperación internacionales.

Protección al destinatario

Artículo 16.—Las emisiones de radiodifusión; no deben perturbar en modo alguno la intimidad de las personas. Quedan prohibidas las emisiones cuyo contenido atente contra la salud o estabilidad psíquica de los destinatarios de los mensajes.

(Las emisiones de radiodifusión; no deben perturbar en modo alguno la intimidad de las personas ni comprometer su buen nombre y honor. Quedan prohibidos los procedimientos de difusión que atenten contra la salud psíquica de los destinatarios de los mensajes o contra su integridad moral). Sustituido por decreto 1005/99 Art. 2.

Protección al menor

Artículo 17.—En ningún caso podrán emitirse programas calificados por autoridad competente como prohibidos para menores de dieciocho años. En el horario de protección al menor que fije la reglamentación de esta Ley. Las emisiones deberán ser aptas para todo público. Fuera de ese horario, los contenidos mantendrán a salvo los principios básicos de esta ley. Los programas destinados especialmente a niños y jóvenes deberán adecuarse a los requerimientos de su formación. En el supuesto en que la hora oficial no guarde uniformidad en todo el territorio de la República, el horario de protección al menor se fijará teniendo en cuenta las diferencias horarias existentes, de modo de no violar las disposiciones del presente Artículo 1°.

Caracteres de la Información

Artículo 18.—La libertad de información tendrá como únicos límites los que surgen de la Constitución Nacional y de esta Ley. La información deberá ser veraz, objetiva y oportuna. El tratamiento de la información por su parte, deberá evitar que el contenido de esta o su forma de expresión produzca conmoción pública o alarma colectiva. La información no podrá atentar contra la seguridad nacional ni implicar el elogio de actividades ilícitas o la preconización de la violencia en cualquiera de sus manifestaciones. Las noticias relacionadas con hechos o episodios sórdidos, truculentos o repulsivos, deberán ser tratadas con decoro y sobriedad, dentro de los límites impuestos por la información estricta.