ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

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

VARIOS SEÑORES DIPUTADOS

EXPEDIENTE N.º 16.679

DEPARTAMENTO DE SERVICIOS PARLAMENTARIOS

PROYECTO DE LEY

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

Expediente N.º 16.679

ASAMBLEA LEGISLATIVA:

La protección de datos de las personas en la actualidad se constituye en uno de los grandes temas jurídicos que deben ser abordados en la sociedad del siglo XXI. Las tecnologías de la información se constituyen en medios de manejo y difusión rápida de los datos, sin mayor consideración ni control. La realidad costarricense no es ajena a toda una diversa gama de situaciones que se presentan con la información que viaja a través de la red de internet o que la encontramos ubicada en bases de datos públicas y privadas. Frente a esto, debemos tomar en consideración todo lo relativo a la protección de derechos fundamentales de las personas, entre ellos, los derechos de la personalidad y el derecho a la intimidad entre otros.

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 por medio de sus administraciones. Quizá el riesgo mayor está representado por el creciente desarrollo de la informatización de los particulares, los cuales utilizan cada vez los 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 solo 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 información[1].

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 Frankfort 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 solo 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 perfilarle, 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

[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 Hábeas 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 solamente 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.º 12.827, con el título “Adición de un nuevo capítulo IV, denominado Del Recurso de Hábeas Data“, al título III, de la Ley de la Jurisdicción Constitucional, Ley N.º 7135, de 19 de octubre de 1989.

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 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 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**

[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 Frankfort 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.

> **en juego no solo 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 solo 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 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 leyes 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 importancia[4]. 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.

En América Latina se han decidido por la constitucionalización de este derecho Colombia y Brasil[5], también Paraguay en la Constitución de 1992 (art. 136) y Ecuador en su reciente Constitución, de 18 de junio de 1996[6]; 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

[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.

[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 hábeas corpus, permitiera al ciudadano 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 de 18 de junio de 1996. "Toda Persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre si 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 sí fueran erróneas o afectaren ilegítimamente sus derechos.
Se exceptúan los documentos reservados por razones de seguridad nacional".

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, Grecia[7], Noruega y Suecia. También Canadá y Japón. Italia aprobó a inicios de mayo de 1997 su Ley de Protección de Datos[8].

Estas leyes demostraron ser esenciales como complemento de las garantías generales del Estado de Derecho, no solo como limitativas de esas ansias exhorbitadas 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.- Necesidad de aprobación de una ley de protección de la persona frente al tratamiento de datos para Costa Rica

Esta iniciativa del importante desarrollo que ha realizado la Sala Constitucional en esta materia, abordando los temas de protección de datos; hábeas data; acceso a la información pública; y derecho a la intimidad, entre otros. 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.

---

[7] 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 Nr. 675 de 31 de diciembre de 1996: Tutella delle persone e di altri soggetti rispetto al trattamento de dati personalli, 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).

El presente proyecto de ley, recoge los esfuerzos realizados por la Comisión Permanente de Asuntos Jurídicos al haber dictaminado por unanimidad este expediente el pasado 21 de noviembre de 2006 y el cual por vencimiento de plazo cuatrienal fue archivado. Esta iniciativa retoma completo el texto que presenta el dictamen unánime mencionado el cual quedó dividido en cinco capítulos.

El capítulo I, es denominado “Disposiciones generales” y se refiere al objeto y fin de la iniciativa, así como a 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. En este sentido la Comisión Permanente de Asuntos Jurídicos hizo un gran esfuerzo en la revisión de estos términos, precisando y ampliando algunos de ellos con el fin de que el texto quedara claro y preciso.

El capítulo II, “Principios básicos para la protección de los 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.

Un capítulo III, “Transferencia de datos personales”, 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, incorporando algunas excepciones.

El capítulo IV, denominado “De la Agencia para la Protección de Datos Personales (Prodat)”, crea un órgano de desconcentración máxima adscrito a la Defensoría de los Habitantes, denominado Agencia para la Protección de Datos Personales, la cual gozará de independencia funcional y de criterio en el desempeño de sus funciones. Este 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. Sus funciones se caracterizan por ser: preventivas (inscripción y autorización de las bases de datos y protocolos

de actuación, inspecciones oficiosas, etc.); y 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. La Agencia estará compuesta por cinco departamentos: 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 “Procedimientos”, desarrolla la intervención en archivos y bases de datos, así como un régimen sancionatorio aplicable a los administradores de ficheros y los procedimientos internos para ejercer la competencia disciplinaria contra los funcionarios de la Agencia y el procedimiento correspondiente que se podría implementar contra el Director (a) o Subdirector (a) de la Agencia, en caso de que incurra en una causal de sanción.

En virtud de lo anterior y con fundamento en las razones expuestas recomendamos al Plenario legislativo la aprobación del siguiente texto:

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 o actividad 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.

En ningún caso se podrá afectar el secreto de las fuentes de información periodística y el secreto profesional que determinen las leyes correspondientes.

ARTÍCULO 2.- Ámbito de aplicación

1.- La presente Ley será de aplicación a los datos sensibles que figuren en ficheros automatizados o manuales de organismos públicos y privados y a toda modalidad de uso posterior, de datos de carácter personal.

2.- El régimen de protección de los datos de carácter personal que se establece en la presente Ley no será de aplicación:

a) A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.
b) A los ficheros mantenidos por personas físicas con fines exclusivamente personales o domésticos.
c) A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales.
d) A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales.

e) A los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida lo dispuesto en el artículo 10 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos.

3.- Se regirán por otras disposiciones específicas:

a) Los ficheros regulados por la legislación del régimen electoral.
b) Los derivados del Registro Civil.

ARTÍCULO 3.- <u>Definiciones</u>

A los efectos de la presente Ley:

a) Datos de carácter personal: cualquier información relativa a una persona física identificada o identificable.
b) Datos de una persona jurídica: aquellos datos que el ordenamiento no les ha dado el carácter de público.
c) Datos sensibles: datos personales que revelen origen racial, opiniones políticas, convicciones religiosas o espirituales, condición socioeconómica, información biomédica o genética, vida sexual y antecedentes delictivos, operaciones bancarias, registros tributarios, aduaneros o relativos a actividades económicas.
d) 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.
e) Tratamiento automatizado: operaciones que a continuación se indican: producción de registros de datos, aplicación a esos datos de operaciones lógico aritméticas, su modificación, borrado, extracción o difusión.
f) Autoridad encargada del fichero: significa la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo público o privado, 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 registrase y cuáles operaciones se les aplicarán.
g) Interesado: persona física o jurídica, titular de los datos que sean objeto del tratamiento automatizado o manual.
h) 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 4.- Derecho de información en la recolección de los datos

Las personas físicas a quienes se soliciten datos de carácter personal y a las personas jurídicas cuyos datos no se les ha dado el carácter de público; 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:

a) De la existencia de un fichero automatizado o manual de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se les formulen.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercer los derechos de acceso, rectificación, actualización, cancelación y confidencialidad.
e) 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 o de la información derivada de la actividad ordinaria de la institución o de su giro normal; o de la empresa solicitante.

ARTÍCULO 5.- Consentimiento del interesado

1.- 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 el Director o Directora de la Agencia de Protección de Datos Personales si se le planteare en caso de controversia. Lo anterior vale tanto para los ficheros de titularidad pública o privada.

El consentimiento deberá constar por medio 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:

a) Exista orden motivada, dictada por autoridad judicial competente.
b) 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, u otros datos que por ley especial tengan la misma condición.

ARTÍCULO 6.- <u>Calidad de los datos</u>

1.- Solo 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.

2.- Los datos de carácter personal objeto de tratamiento automatizado o manual no podrán utilizarse para finalidades distintas de aquellas para los cuales los datos hubieren sido recogidos.

3.- Dichos datos serán exactos y puestos al día, de forma que respondan con veracidad a la situación real del interesado.

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 el responsable del fichero por los correspondientes datos rectificados, 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 por el responsable del fichero 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 de la persona 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, salvo disposición legal en contrario.

6.- Serán almacenados de forma tal que se garantice plenamente el derecho de acceso por la persona interesada.

7.- Es obligatoria la cancelación de datos por el fallecimiento o deceso confirmado de la persona, y se define un año como plazo para tal efecto.

8.- Se prohíbe el acopio de datos por medios fraudulentos, desleales o ilícitos.

9.- Los archivos de datos no pueden tener finalidades contrarias a las leyes ni a la moral pública.

ARTÍCULO 7.- 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 solo 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 8.- 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 27 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.

4.- 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 9.- Deber de confidencialidad

El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto después de finalizada su relación con el archivo de datos. El obligado podrá ser relevado del deber de secreto por decisión judicial en lo estrictamente necesario y dentro de la causa que conoce.

Las comisiones legislativas que por disposición constitucional y reglamentarias les confiera atribuciones de investigación, tendrán acceso a los archivos y bases de datos, siempre que se enmarquen estrictamente en el ámbito de las competencias asignadas.

ARTÍCULO 10.- Cesión de datos

Los datos de carácter personal conservados en archivos o bases de datos públicos o privados, solo podrán ser cedidos a terceros para fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado, en los términos del artículo 5 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.
c) Se trate de la cesión de datos personales al Estado o a una institución pública en materia de seguridad pública, siempre y cuando la cesión resulte necesaria para fines de esta seguridad pública y de la persecución de delitos sin perjuicio de lo establecido en el artículo 24 de la Constitución Política.
d) Se trate de cesión de datos personales referente a estadísticas y censos poblacionales para fines específicos.

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 11.- Derechos y garantías de las personas

Se garantiza el derecho de toda persona a:

a) Obtener a intervalos razonables y sin demora a título gratuito, la confirmación de la existencia de datos suyos en archivos o bases de datos, así como la comunicación de dichos datos en forma inteligible.
b) 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.
c) La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento solo 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.
d) 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.
e) 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 naturales contado a partir de la recepción de la solicitud.

ARTÍCULO 12.- Garantías efectivas

1.- Todo interesado 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 13.- Del derecho de acceso a la información personal

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

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.
d) El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponden a sus sucesores universales y legatarios.

ARTÍCULO 14.- Límites y excepciones al derecho a la autodeterminación informativa del ciudadano

Solo por ley se podrán establecer límites y excepciones en los principios, derechos y garantías aquí enunciados, siempre que aquellas sean justas, razonables y acordes con el principio democrático y de transparencia administrativa y del disfrute pleno de los derechos fundamentales. Los mencionados límites y excepciones 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, de las relaciones internacionales o para la persecusión de las infracciones penales.
b) La protección de los propios titulares de los datos, 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.
d) La adecuada prestación de servicios públicos y de la eficaz actividad ordinaria de la Administración, por parte de las autoridades oficiales.

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

ARTÍCULO 15.- 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
TRANSFERENCIA DE DATOS PERSONALES

SECCIÓN ÚNICA

ARTÍCULO 16.- Transferencia de datos personales. 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 alguna de las siguientes reglas:

a) 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.
b) Que el titular de la información haya autorizado expresa y válidamente tal transferencia y que no haya sido notificada la revocatoria a la Autoridad encargada del fichero.
c) 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, salvo que el titular de los datos personales autorice expresamente su transferencia, la cual se hará sin más trámite.

CAPÍTULO IV
AGENCIA PARA LA PROTECCIÓN DE DATOS PERSONALES (Prodat)

SECCIÓN I
Disposiciones generales

ARTÍCULO 17.- Agencia para la Protección de Datos Personales

Créase un órgano de desconcentración máxima adscrito a la Defensoría de los Habitantes denominado Agencia para la Protección de Datos Personales (Prodat), el cual gozará de independencia funcional y de criterio en el desempeño de las funciones que esta Ley le encomienda. En lo administrativo se ajustará a la organización interna de la Defensoría de los Habitantes, tanto en materia presupuestaria, personal y salarios.

ARTÍCULO 18.- 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:

a) 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.
b) 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, conforme a lo establecido en el artículo 8, inciso 1), de esta Ley.
c) 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.
d) Autorizar la transferencia de datos a tercero, 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, en los supuestos de los incisos a) y c) del artículo 16 de esta Ley.
e) Recibir de las personas los reclamos por infracción a las normas sobre protección de los datos personales.
f) 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.
g) 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 legalmente.
h) Remitir anualmente, un informe escrito de sus labores a la Defensora o Defensor de los Habitantes, con el fin de que sea incluido en el informe que se presenta cada año a la Asamblea Legislativa.

i) Promover y contribuir en la redacción de anteproyectos de ley tendientes a implementar las normas sobre protección de los datos personales.

j) Respetar los diversos grados de autonomía administrativa e independencia funcional, dictar las directrices obligatorias y necesarias a efecto de que las instituciones públicas implementen los procedimientos adecuados respecto del manejo de los datos personales.

k) Fomentar entre los habitantes el conocimiento de los derechos concernientes al acopio, almacenamiento, transferencia y uso de sus datos personales.

El director o directora; el subdirector o subdirectora de la Agencia para la Protección de Datos Personales, gozarán de independencia funcional y de criterio, en el ejercicio de sus facultades y atribuciones legales y reglamentarias.

ARTÍCULO 19.- 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 elegido de una lista de cuatro personas integrada en forma alternativa con equidad de género, que se conformará mediante un concurso público bajo la supervisión y nombramiento definitivo de la defensora o defensor de los Habitantes. El director o directora de la Agencia, deberá cumplir con los requisitos establecidos en esta Ley y no podrá encontrarse en ninguno de los supuestos de impedimentos o incompatibilidad para ejercer dicho cargo. El director o la directora nacional de Protección de Datos Personales permanecerá en su cargo durante seis años, y podrá ser reelecto o reelecta hasta por una vez. Durante su gestión, podrá ser removido de acuerdo con el régimen administrativo y laboral aplicable, garantizándose en todo momento el debido proceso.

ARTÍCULO 20.- Requisitos

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

ARTÍCULO 21.- 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 por 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 22.- Subdirección

La Agencia para la Protección de Datos Personales tendrá un subdirector o subdirectora, quien será escogido de una lista de cuatro personas integrada en forma alternativa con equidad de género, que se conformará mediante un concurso público bajo la supervisión y nombramiento definitivo de la Defensora o Defensor de los Habitantes. El subdirector o subdirectora de la Agencia, deberá cumplir con los requisitos establecidos en esta Ley para el director o directora y no podrá encontrarse en ninguno de los supuestos de impedimento o incompatibilidad para ejercer dicho cargo. El subdirector o la subdirectora nacional de Protección de Datos Personales permanecerá en su cargo durante seis años, y podrá ser reelecto o reelecta hasta por una vez. Durante su gestión, no podrá ser removido sino por justa causa, garantizándose en todo momento el debido proceso.

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. Por medio de normativa interna, 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 23.- 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 los nombramientos.

ARTÍCULO 24.- 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 bajo la estructura administrativa, presupuestaria, procedimientos y competencias de la Defensoría de los Habitantes. Deberá capacitar permanentemente a su personal en el manejo de nuevas herramientas tecnológicas y nuevas formas de manejo de datos personales.

Este personal está obligado a guardar secreto y deber de confidencialidad de los datos de carácter personal de que conozca en el desarrollo de sus funciones.

ARTÍCULO 25.- Prohibiciones

Todos los empleados de la Agencia para la Protección de Datos Personales tienen las siguientes prohibiciones:

a) 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.
b) Interesarse personal e indebidamente en asuntos de conocimiento de la Agencia.
c) 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.
d) 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 26.- Organigrama

La Agencia para la Protección de Datos Personales estará compuesta al menos de los siguientes órganos:

a) El director o directora nacional.
b) El subdirector o subdirectora nacional.
c) El registro de archivos y bases de datos.
d) El departamento de inspección de archivos y bases de datos.
e) 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 27.- Registro de archivos y bases de datos

Todo archivo, registro, base o banco de datos público y privado administrado con fines de distribución, difusión o comercialización, que contenga

datos sensibles 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 inscribirlos.

Asimismo, deberá inscribir:

a) Los protocolos de actuación a que hace referencia el artículo 15 de esta Ley.
b) Cualesquiera otras informaciones que las normas de rango legal 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 28.- <u>Departamento de inspección de archivos y bases de datos</u>

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 controlar 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 29.- 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 30.- 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 31.- 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 32.- 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. Todo 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 interesado, 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 interesado, 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 33.- Efectos de la resolución estimatoria

Si en su acto final, el director o directora nacional determinare que la información del interesado 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 34.-

Los responsables de los ficheros y los encargados de su tratamiento estarán sujetos al régimen disciplinario establecido en la presente Ley.

Cuando se trate de ficheros de los que sea responsable la Administración Pública estarán sujetos, en cuanto al procedimiento y a las sanciones, a lo establecido en la sección IV del capítulo V de esta Ley.

ARTÍCULO 35.- 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 del tercer día, el cual deberá ser resuelto en el plazo de ocho días luego de recibido, agotando la vía administrativa.

ARTÍCULO 36.- 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:

a) Para las faltas leves, una multa hasta cinco salarios base, conforme a la Ley N.º 7337.
b) Para las faltas graves, una multa de cinco a veinte salarios base, conforme a la Ley N.º 7337.
c) Para las faltas gravísimas, una multa de 15 a 30 salarios base, conforme a la Ley N.º 7337; y la suspensión para el funcionamiento del fichero de uno a seis meses.

ARTÍCULO 37.- Faltas leves

Serán consideradas faltas leves, para los efectos de esta Ley:

a) 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 4 de esta Ley.
b) 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 38.- Faltas graves

Serán consideradas faltas graves, para los efectos de esta Ley:

a) 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.
b) Transferir datos personales a otras personas o empresas en Costa Rica en contravención a las reglas establecidas en el artículo 10 de esta Ley.
c) Transferir datos personales a otras personas o empresas radicadas en el extranjero en contravención a las reglas establecidas en el artículo 16 de esta Ley.

d) Recolectar, almacenar, transmitir o de cualquier otro modo emplear datos personales para una finalidad distinta de la autorizada por el titular de la información.
e) 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.
f) Negarse injustificadamente a eliminar o rectificar los datos de una persona que así lo haya solicitado por medio claro e inequívoco.

ARTÍCULO 39.- Faltas gravísimas

Serán consideradas faltas gravísimas, para los efectos de esta Ley:

a) 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 7 de esta Ley.
b) Obtener de los titulares o de terceros, datos personales de una persona por medio de engaño, violencia o amenaza.
c) Revelar información registrada en una base de datos personales cuyo secreto estuviere obligado a guardar conforme la ley.
d) Proporcionar a un tercero información falsa a la contenida en un archivo de datos, con conocimiento de ello.

SECCIÓN IV
PROCEDIMIENTOS INTERNOS

ARTÍCULO 40.- 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.

La aplicación del régimen disciplinario al director o a la directora nacional; al subdirector o subdirectora de la Agencia para la Protección de Datos Personales, deberá efectuarse de conformidad con el procedimiento ordinario que regula la Ley General de la Administración Pública. Para tales efectos, corresponderá al Defensor o Defensora de los Habitantes la conformación del órgano encargado de dirigir el procedimiento. El acto final del procedimiento lo dictará el Defensor o Defensora y contra este cabrá únicamente el recurso de reposición.

ARTÍCULO 41.- 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 42.- 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:

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

ARTÍCULO 43.-

Causas de cesación del director (a) o del subdirector (a) de la Agencia.

El director (a) o subdirector (a) de la Agencia para la Protección de los Datos Personales, cesará en sus funciones, por cualquiera de las siguientes causales:

a) Renuncia del cargo.
b) Muerte o incapacidad sobreviniente.
c) Comprobar su participación en actividades políticas partidistas o el ejercicio de funciones incompatibles con su cargo.
d) Haber sido condenado en sentencia firme por delito doloso.
e) Por faltas gravísimas si así fuere determinado conforme a lo dispuesto en el artículo 39.

ARTÍCULO 44.-

Cuando las faltas a que se refieren los artículos 37, 38 y 39 de la presente Ley, fuesen cometidas en ficheros del que sea responsable la Administración Pública, el director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que proceda adoptar para que cesen o se corrijan los efectos de la falta. Esta resolución se notificará al responsable del fichero, al

órgano del que dependa jerárquicamente y a los afectados, si los hubiera. La resolución podrá dictarse de oficio o a petición de parte.

TRANSITORIO

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.

Clara Zomer Rezler

Alexander Mora Mora

Mario Quirós Lara

Bienvenido Venegas Porras

Elsa Grettel Ortiz Álvarez

Jorge Luis Méndez Zamora

Rafael Elías Madrigal Brenes

Xinia Nicolás Alvarado

José Luis Valenciano Chaves

Andrea Morales Díaz

DIPUTADOS

25 de junio de 2007.

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