iberIUS | Red Iberoamericana de Documentación e Información Judicial

Revista iberIUS

Estudios sobre el tratamiento de la Documentación Judicial

La protección de datos personales

Escriben Humberto Quiroga Lavié (ARGENTINA) | Hernan Lionel Elman (ARGENTINA)
Mariana Gutiérrez Dueñas (COLOMBIA) | Samuel Páez Pisco (COLOMBIA) | Alfredo Chirino Sánchez (COSTA RICA)
Miguel Ángel Serrano (ECUADOR) | Rafael Santiago Herníquez Amaya (EL SALVADOR)
Equipo de Dirección del CENDOJ (ESPAÑA) | Guillermo Corzo (GUATEMALA)
Miguel Ángel Vargas Díaz (PARAGUAY) | Ana Luisa Geraldes (PORTUGAL)
Hermógenes Acosta de los Santos (República Dominicana) | Beatriz Rodriguerz Acosta (URUGUAY)

Editorial de la Secretaría Técnica de la Red

AÑO2 NÚMERO2 AGOSTO 2006

ÍNDICE

Editorial de la Secretaría
De la Red IberIUS

Tal como estaba previsto, este segundo número de la Revista electrónica de la Red de Centros de Documentación Iberius trata del estado de la cuestión de la protección de datos personales en la Jurisprudencia en varios de los países miembros de la Red.

Como se sabe, el número cero fue una descripción de las actividades y situación de cada Centro, que después del Encuentro de Mayo de 2006 se ha actualizado, y el número primero del acceso a la Jurisprudencia en el marco de Internet en los países miembros de Iberius.

Es general, como también se conoce, en el ámbito de los ordenamientos procesales de los países miembros de Iberius, el respeto a los principios de publicidad, inmediación y contradicción, contenidos en el derecho a un proceso con todas las garantías, que impone inexorablemente que toda condena se fundamente en una actividad probatoria que el órgano judicial haya examinado directa y personalmente y en un debate público en el que se respete la posibilidad de contradicción.

Desde esta perspectiva la publicación de las resoluciones judiciales resulta necesaria además para que se posibilite el más amplio acceso y conocimiento a la interpretación que de las leyes realizan los Tribunales de Justicia.

Pero la exigencia de máxima difusión y publicidad del contenido íntegro de las resoluciones jurisdiccionales no es de carácter absoluto y cabe ser excepcionada en determinados supuestos y como cualquier otra exigencia, dicho principio puede resultar limitado por la eventual prevalencia de otros derechos fundamentales con los que entre en conflicto.

El acceso a los datos identificativos de las partes de una sentencia podrá quedar restringido, por ejemplo, cuando el mismo pudiera afectar al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda, así como, con carácter general, para evitar que las sentencias puedan ser usadas con fines contrarios a las leyes.

Pero estas cuestiones no tienen el mismo tratamiento en los países miembros de la Red. Y en especial cuando se trata de la protección de los datos en las Bases de Datos de difusión de la Jurisprudencia.

Este número dos de la Revista trata precisamente del estado de la cuestión en algunos de los países al día de hoy.

Secretaría Técnica de la Red
Agosto de 2006

Hacia la verdadera protección
Del Derecho a la Intimidad

Dr. Humberto Quiroga Lavié y Lic. Hernán L. Elman*

La revolución que significa la sociedad del conocimiento, y muy especialmente la difusión del uso de Internet, ha potenciado la disyuntiva entre publicidad y privacidad. En ese marco, distintas iniciativas buscan alcanzar un necesario equilibrio. El Poder Judicial no se encuentra ajeno a esta realidad, por lo que se describen los esfuerzos realizados en ese sentido.

CONCEPTO Y NATURALEZA JURIDICA DEL HABEAS DATA

En la sociedad del conocimiento, el ciudadano difícilmente pueda permanecer en el anonimato. Conciente o inconcientemente, voluntaria e involuntariamente, brinda diariamente detalles, información personal, da a conocer sus datos personales en múltiples formas, muchas veces ignorando, y en el mejor de los casos solo presintiendo, que existen los medios para que toda su persona, es decir su patrimonio, su estado financiero, su formación académica, sus hábitos de consumo y la forma en que aprovecha su tiempo de ocio, sus preferencias sexuales, religiosas o políticas, e incluso su historia clínica, se encuentren detalladamente registrados en archivos susceptibles de ser utilizados indebidamente.

La generación de bancos de datos con información personal, en muchos casos sensibles, relativos a personas físicas y de existencia ideal, sin ninguna posibilidad de control, o incluso la mera presunción respecto a la eventual existencia de dichos registros, desconociéndose el uso que pudiera darse a los datos allí contenidos, terminaría dejando a la ciudadanía en situación de total desprotección. Es decir que la ausencia de instrumentos legales de protección en la materia por parte del Estado, generaría un permanente estado de indefensión e incertidumbre por parte de los ciudadanos. Por esa razón los titulares de la información contenida en los bancos de datos deben tener garantizado el derecho de acceder a la información allí contenida a los efectos de tomar conocimiento de su exactitud, para requerir la correspondiente modificación, corrección o rectificación, incluso para que los datos o información sean suprimidos de los registros, cuando ellos fueren inexactos u obsoletos, cuando conllevaren una discriminación por razones de raza, religiosas, ideología u otra circunstancia personal o de

grupo, salvo que el registro estuviera especialmente habilitado para realizar una constatación de esa naturaleza, cuestión que debe considerarse excepcional, en especial teniendo en cuenta que los datos sensibles deben quedar exentos a toda registración.

La reforma de la Constitución Nacional de la República Argentina de 1994, introdujo el "habeas data", es decir el derecho de toda persona a interponer la acción de amparo "para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos públicos o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos" (tercer apartado del art. 43 C.N.).

De este modo el habeas data no es simplemente una herramienta legal, sino que se trata de una garantía constitucional por la cual toda persona tiene garantizado el derecho de conocer si información que le concierne personalmente se encuentra registrada y disponible, y pueda actuar en consecuencia de ese conocimiento. Se trata de una garantía que viene a tutelar el derecho a la intimidad, variable fundamental de la dignidad humana, consagrado tradicionalmente en el ratificado texto histórico del art. l9 de la Constitución Nacional.

El habeas data tiende a proteger al individuo contra calificaciones sospechosas, mecanismos prejuiciosos que tiene no solo el Estado conducido por autoritarios para discriminar o perseguir personas, sino también las corporaciones de intereses privados con el objeto de medrar con el manejo o manipuleo de la información privada. El habeas data es el remedio que permite que cada ciudadano se defienda de dichos excesos, a fin de que pueda realizar su replica jurisdiccional o política.

La sociedad organizada a partir de redes de información que alimentan registros o bancos de datos de diversa índole, a los cuales o desde los cuales se puede acceder con notable facilidad y sin control de ninguna naturaleza, como es el caso del Registro Civil, de los padrones electorales, de los registros de la propiedad inmueble o automotor, de los existentes en bancos públicos o privados, en tarjetas de crédito, en hospitales o establecimiento sanitarios, en universidades o escuelas, en sindicatos u obras sociales, y hasta en la misma Dirección General Impositiva, según sea el caso, hacen del habeas data el remedio jurisdiccional adecuado a los efectos de evitar violaciones a los derechos.

La doctrina ha instalado la cuestión vinculada a qué derechos ha venido a proteger el habeas data. Entendemos que el bien jurídico protegido es la intimidad de las personas titulares de los datos que son archivados. Distintos autores consideran, asimismo, que el habeas data custodia el derecho a la autodeterminación

informativa, que busca controlar la identidad informativa de la persona, a fin de proteger el derecho a su perfil y el derecho a su imagen, o que simplemente tiene por mira evitar el abuso informático, y aun sin tal abuso, preservar el honor, la dignidad, la información sensible, la privacidad, la verdad, la autodeterminación informativa, también la igualdad, vale decir toda una gama de situaciones jurídicas que hacen a la personalidad.

En la sociedad del conocimiento, el ciudadano difícilmente pueda permanecer en el anonimato. Conciente o inconcientemente, voluntaria e involuntariamente, brinda diariamente detalles, información personal, da a conocer sus datos personales en múltiples formas.

El habeas data tiene por finalidad impedir que en bancos o registros de datos se recopile información respecto de la persona titular del derecho que interpone la acción, cuando dicha información esté referida a aspectos de su personalidad que están directamente vinculados con su intimidad, no correspondiendo que ella se encuentre a disposición del público o sea utilizada en su perjuicio, por órganos públicos o entes privados, sin derecho alguno que sustente dicho uso. Se trata, particularmente, de información relativa con la filiación política, las creencias religiosas, la militancia gremial, el desempeño en el ámbito laboral o académico o académico, entre muchos otros objetivos.

El titular de la acción de habeas data tiene derecho a exigir las siguientes modificaciones en los registros o bancos de datos:

a) Lla supresión de la información registrada, cuando ella fuere falsa o, siendo verdadera, no hubiere sido autorizado su registro por el damnificado, salvo competencia dispuesta por ley para hacer el registro por parte de la autoridad o, eventualmente, del particular que tiene a su cargo el banco de datos. Dentro del concepto de falsead deben comprenderse, latu sensu, a los datos erróneos u obsoletos, pues dichos vicios afectan la veracidad del dato.

b) También la supresión procede cuando los datos almacenados fueren discriminatorios, lo cual implica que se encuentra prohibida en la norma la recolección de datos sensibles, en razón de que, por lo general, ellos pueden ser utilizados con una finalidad discriminatoria.

c) la rectificación de la información, cuando la misma fuere incorrecta, no debiendo el titular del derecho justificar daño alguno como

consecuencia de la incorrección producida. La falsedad es mala en si misma y no puede existir ninguna justificación para mantenerla en un banco de datos, cuando estuviera suficientemente probada su existencia. Como bien sostiene Ekmekdjian, en materia de derecho a la privacidad la capacidad dañosa de la intrusión se presume juris et de juri: sólo es necesario probar el daño[1].

d) la confidencialidad de la información, esto es prohibir que el responsable del registro la haga pública, salvo que por imperio de la ley hubiere obligación de difundirla. Esto último sólo será posible si dicha obligación es razonable, en relación con el interés público que la hubiere justificado;

e) la actualización de la información cuando hubieren nuevos datos no incluidos en el registro. No hacerlo es una manera de obtener la falsedad, por insuficiencia, de la información que va a ser utilizada por el servicio al cual sirve.

Desde ya que se encuentra legitimado a interponer el habeas data la persona titular de los datos almacenados, pero también, en virtud de la protección integral que a la familia le otorga el art. l4 bis constitucional, lo están los padres del titular del derecho, el tutor o el curador, el defensor de menores o incapaces, todos ellos en representación del aquel, frente a la imposibilidad de actuar por si mismo. No vemos tampoco razón alguna para excluir del ejercicio del derecho a las personas jurídicas, a través de sus representantes legales: el manipuleo de la información las afecta lo mismo que a cualquier persona física[2].

Pero también pueden considerarse legitimados el Defensor del Pueblo, en defensa de los derechos humanos, por ejemplo en protección de la vida de un individuo carente de familia, quien en estado de imposibilidad de hacerlo por si mismo, debe ser representado por alguien para acceder a su legajo médico archivado en un sanatorio.

La ley 25.326 ha dispuesto la reglamentación legal del habeas data constitucional, consagrado en el art. 43, tercer apartado, de nuestra Ley Fundamental.

La ley dispone que "su objeto es la protección integrar de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el art. 43, párrafo tercero, de la Constitución Nacional" (Art. I)

[1] Tratado de Derecho Constitucional, T. IV, pag. 92

[2] Conf. Sagües, Nestor, Amparo, Habeas Data y Habeas Corpus en la reforma constitucional

A continuación la norma agrega que "las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal".

Siguiendo al modelo español, nuestro legislador ha incluido en el art. 2º de la ley de habeas data una serie de definiciones sobre conceptos que son objeto de su regulación, apartándose de una tradición legislativa existente en nuestro país de no considerar pertinente incluir definiciones "lexicográficas legislativas" (una suerte de diccionario dentro de la ley).

Los conceptos definidos por la ley son los siguientes:

a) Datos personales: " Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables":

b) Datos sensibles: "Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual". En el caso de los datos referidos a la salud habrá situaciones donde será necesario registrar el dato, por razones de interés público, pero no se podrá informar a quien pertenece: caso del listado de portadores del H.I.V.

c) Archivo, registro, base o banco de datos (en el texto vetado sólo se decía: registro o banco de datos): "Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuera la modalidad de su formación, almacenamiento, organización o acceso".

d) Tratamiento de datos: "Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias".

No se ha incluido a la "confidencialidad", lo cual es grave pues dicha función registrada se encuentra expresamente prevista en nuestro art. 43 constitucional.

e) Responsable de archivo, registro, base o banco de datos (el texto vetado no hablaba de "archivo ni de base de datos): "Persona física o de existencia ideal, pública o privada, titular de un archivo, registro, base o banco de datos".

f) Datos informatizados: "Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado".

g) Titular de los datos: "Toda persona física o persona de existencia ideal con domicilio legal

o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley".

h) Usuario de datos: "Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos".

i) Disociación de datos: "Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable"

La ley 25.326 es verdaderamente amplia y compleja, abarcando múltiples aspectos de los datos personales, en tanto se pronuncia en relación a: la licitud de los archivos de datos, la calidad de los datos, la lealtad en el almacenamiento, la necesidad de que el contenido de los registros coincida con la finalidad del mismo, la exactitud y actualidad de los datos, la completitud de los datos (los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados), la facilidad de acceso por el titular, la destrucción de datos innecesarios, el consentimiento previo del titular de los datos, lo que se les debe informar a los titulares de los datos, las distintas categoría de los datos (fundamentalmente en materia de datos sensibles), la necesidad de ofrecer la seguridad de los datos registrados, el deber de confidencialidad del responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales, la cesión de datos personales, la revocación del consentimiento de la cesión del registro, y a la transferencia internacional de los datos personales, creando órganos de control y aplicación, e incluyendo sanciones.

El habeas data no es simplemente una herramienta legal, sino que se trata de una garantía constitucional por la cual toda persona tiene garantizado el derecho de conocer si información que le concierne personalmente se encuentra registrada y disponible, y pueda actuar en consecuencia de ese conocimiento

Internet, Poder Judicial y Reglas de Heredia

La verdadera revolución que implicó la difusión masiva del acceso a Internet en la última década, ha facilitado por un lado la posibilidad de hacer realidad el postulado de publicidad de los actos de gobierno, pero ha generado, al mismo tiempo, justificadas preocupaciones

respecto a la publicidad de información personal de carácter sensible, así como en relación a la posibilidad de publicación de datos falsos o desactualizados, con las consecuencias de cada caso. Es allí donde comienza el debate en relación al límite o balance entre transparencia y privacidad, una delgada frontera entre el mejor intencionado cumplimiento de principios socialmente reconocidos y valorados, y la flagrante violación de garantías consagradas en la Constitución Nacional.

Durante el Seminario Internet y Sistema Judicial realizado en la ciudad de Heredia (Costa Rica), los días 8 y 9 de julio de 2003, con la participación de poderes judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay, se definieron las reglas mínimas para la difusión de información judicial en Internet, también conocidas como Reglas de Heredia) en virtud de la ciudad sede del encuentro), las que han sido consideradas en nuestro país como marco general para la definición del reglamento relativo a la información judicial, como el que veremos mas adelante.

Las referidas reglas establecieron que la finalidad de la difusión en Internet de las sentencias y resoluciones judiciales será: "a) El conocimiento de la información jurisprudencial y la garantía de igualdad ante la ley; b) Para procurar alcanzar la transparencia de la administración de justicia" (Regla 1). Reconociéndose al interesado el derecho a oponerse por razones particulares a que los datos que le conciernan sean objeto de difusión, salvo cuando la legislación nacional disponga algo distinto.

A los efectos de solucionar la disyuntiva planteada previamente entre publicidad y privacidad, se entiende que "Prevalecen los derechos de privacidad e intimidad, cuando se traten datos personales que se refieran a niños, niñas, adolescentes (menores) o incapaces; o asuntos familiares; o que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos; así como el tratamiento de los datos relativos a la salud o a la sexualidad; o victimas de violencia sexual o domestica; o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales. En este caso se considera conveniente que los datos personales de las partes, coadyuvantes, adherentes, terceros y testigos intervinientes, sean suprimidos, anonimizados o inicializados, salvo que el interesado expresamente lo solicite y ello sea pertinente de acuerdo a la legislación" (Regla 5). A su vez "prevalece la transparencia y el derecho de acceso a la información pública cuando la persona

concernida ha alcanzado voluntariamente el carácter de publica y el proceso esté relacionado con las razones de su notoriedad. Sin embargo, se considerarán excluidas las cuestiones de familia o aquellas en los que exista una protección legal específica." (Regla 6). "En todos los demás casos se buscará un equilibro que garantice ambos derechos". (Regla 7), resultando este espacio el ámbito mas propicio para agitados debates jurídicos, académicos e incluso ideológicos.

La promulgación del Reglamento de Administración y Uso del sitio web del Poder Judicial de la Nación en Internet, fue anterior a la redacción de las Reglas de Heredia, no obstante ello, dejó expresado en su artículo tercero que "queda prohibido incorporar a 'el Sitio' la publicación de toda aquella información que viole lo establecido por la Constitución Nacional, los tratados internacionales a los que la Nación Argentina está adherida, las leyes nacionales y provinciales, o las ordenanzas municipales, o que sin llegar a infringirlas posean contenidos inmorales, contengan información privada o secreta o persigan fines de lucro". Con esta previsión normativa no se ha hecho otra cosa que preservar los derechos consagrados en la ley de protección de datos personales o de hábeas data, incorporando las garantías establecidas en todo el plexo normativo vigente, y aún más, que sin llegar a violar aquellos principios, contengan información privada o secreta.

Este ha sido el fundamento normativo en el cual se han basado los distintos proyectos que pretendieron garantizar la privacidad de las personas, para lograr el buscado balance transparencia-privacidad.

No obstante, el hecho de que no se hayan tomado recaudos especiales para el cumplimiento de aquella disposición reglamentaria, desde la vigencia del Reglamento solo ha sido presentada una petición, formulada por el Perito Contador Ricardo Bálsamo, en relación a los motivos de la publicación en la base de datos de peritos disponible en el sitio de Internet del Poder Judicial de la Nación, de sus datos personales -como ser su domicilio particular y teléfono-, y su solicitud de que los mismos fueran eliminados, por considerar que la situación resultaba violatoria de su derecho a la intimidad, y que ponía en riesgo la integridad física suya y de su grupo familiar, por encontrarse realizando tareas de veedor en una causa penal.

Se determinó que el objeto de la base de datos era permitir que los peritos pudieran corregir, de ser necesario, errores en su ficha personal, a los efectos de poder ser sorteados para las causas que pudieran requerirlos. Si bien el acceso a la base de datos que contenía información del interesado al tiempo de la presentación no era irrestricto, ya que se hacía

necesario conocer el número de de documento de un perito para ingresar a su ficha personal, se resolvió que en forma perentoria la información relativa a los datos personales del Cdor. Bálsamo fueran sometidos a confidencialidad, hasta tanto se pudieran estudiar e implementar distintas alternativas para el acceso a la base de datos de peritos con otras restricciones -como puede ser una clave de acceso- a los efectos de resguardar la privacidad de otros eventuales afectados.

Proyecto de Reglamento de Información Judicial

La sanción de la ley 25.326 de Protección de datos personales, ha impulsado al Consejo de la Magistratura a iniciar los estudios necesarios para adecuar las disposiciones legales a las particularidades de los datos que obran en los registros del Poder Judicial de la Nación, produciéndose un dictamen puesto a consideración pública. A partir de entonces, el debate se ha centrado básicamente alrededor de una cuestión que si bien resulta importante, no debería hegemonizar la atención respeto a las decisiones que a los efectos de garantizar la protección de datos personales, deban tomarse:

El texto propuesto dispuso la exclusión de los Registros del Poder Judicial de todo control e inscripción ante la órbita administrativa del organismo de control creado por los artículos 21 y 29 de la ley 25.326 de Habeas Data, por entender que corresponde al Poder Judicial, de modo exclusivo, el control sobre sus registros. Una posición alternativa entiende que corresponde hacer una distinción entre registros administrativos y jurisdiccionales, considerando bajo el ámbito de la ley de orden público 25.326 a los bancos de datos del Poder Judicial que contienen información personal, entendiendo que los expedientes judiciales informatizados representan un neto ejercicio de facultades jurisdiccionales de exclusiva competencia del Poder Judicial. La Comisión de Reglamentación del Consejo, redactora del Proyecto de Reglamento de Información Judicial, no coincide con dichas apreciaciones, con fundamento en la independencia del Poder Judicial de la Nación, tanto en lo jurisdiccional como en lo administrativo, de todo registro y de todo control del Poder Ejecutivo, en los

La difusión masiva del acceso a Internet en la última década, ha facilitado por un lado la posibilidad de hacer realidad el postulado de publicidad de los actos de gobierno, pero ha generado, al mismo tiempo, justificadas preocupaciones respecto a la publicidad de información personal de carácter sensible

términos de la forma republicana de gobierno (artículo primero de la Constitución Nacional), señalando que donde la ley no distingue (en este caso la Constitución Nacional), el interprete no debe distinguir.

Más allá de este debate, el Reglamento ha dado respuesta a otra serie de cuestiones sobre las cuales podían existir distintos criterios de interpretación, y reconoce la necesidad de protección de la privacidad de las personas. En su artículo primero, expresa que "la finalidad de la obtención de todos los datos registrados en el Poder Judicial de la Nación está directa y exclusivamente vinculada con las funciones de este Poder del Estado. En tal sentido, la publicación de cualquier información deberá preservar el ejercicio de dichas funciones, sin que afecte el desempeño de las actividades jurisdiccionales ni la privacidad de las personas alcanzadas por ellas".

Bajo la premisa de que el criterio general es la publicidad, se establecen los supuestos especiales de reserva de la información contenida en los registros, instruyendo sobre la necesidad de evitar que las personas aparezcan identificadas con su nombre completo cuando se refiera a datos sensibles, reservando la identificación de los actores en casos de juicios laborales o en materia de familia, entre otros, o la reserva completa de actuaciones como ser aquellas en que tramitan causas penales o la base de datos del Cuerpo Médico Forense, y disponiéndose el tratamiento que deben recibir ciertos registros, como el caso del que da cuenta de los juicios de la Cámara Nacional de Apelaciones en lo Comercial, del que podrían nutrirse las empresas dedicadas a la provisión de informes crediticios.

El Proyecto de reglamento incorpora, asimismo, otros elementos interesantes, como la mención a las Reglas de Heredia (artículo octavo), como principio interpretativo general, y el reconocimiento del derecho de los titulares de los datos de acceder a los registros en los que estuvieran comprendidos.

Son aún variadas las cuestiones que restan por resolverse, y abarcan no solo el aspecto político y jurídico sino esencialmente las posibilidades técnicas de concreción de las medidas adoptadas y por adoptarse, pero lo cierto es que en estos últimos años se ha tomado verdadera y sincera conciencia de la necesidad de volver operativa una garantía constitucional básica e inseparable de los derechos humanos fundamentales como lo es el derecho a la intimidad ✧

El Dr. Humberto Quiroga Lavié es Consejero Académico del Consejo de la Magistratura del Poder Judicial de la Nación, en representación del Consejo Interuniversitario Nacional.

El Lic. Hernán L. Elman es Director del Centro Digital de Documentación Judicial (CENDDOJ) del Consejo de la Magistratura del Poder Judicial de la Nación.

Hacia la Protección de Datos Personales En la Construcción de la Bodega de Datos, De la Rama Judicial de Colombia

Mariana Gutiérrez Dueñas y Samuel Páez Pisco*

Resulta de especial interés para la Sala Administrativa del Consejo Superior de la Judicatura de Colombia, emprender en esta oportunidad la tarea de revisar el tema de la protección de datos personales propuesto para el segundo número de la Revista IberIUS, dado el impulso que se ha querido dar a la aplicación de las denominadas "Reglas de Heredia"[3], como desarrollo, entre otros, del acuerdo que surgió del I Encuentro Iberoamericano de responsables de centros y unidades de documentación judicial pertenecientes a la Red IberIUS, realizado en diciembre de 2003, en San Sebastián, España, en el sentido de avanzar en la protección de datos personales en el ámbito de la justicia en general.

Antes de abordar el tema de los aspectos tecnológicos que se ha propuesto la Sala Administrativa, y que apuntan a la protección de datos personales, veamos un poco el marco normativo previsto en nuestro país.

Desde el punto de vista jurídico, en Colombia, a raíz de la expedición de la Constitución Política de 1991, y en desarrollo de lo dispuesto en su artículo 15[4], se ha dado especial importancia a la protección de datos personales, como consecuencia necesaria de la aplicación del derecho al buen nombre y a la intimidad que corresponde a todo individuo. Sin duda, el citado artículo ha tenido un interesante desarrollo en nuestro país, en particular en lo que atañe al ejercicio del denominado derecho de *habeas data*, y al punto de encuentro entre el derecho a la intimidad y el derecho a la información[5],

[3] Reglas mínimas para la difusión de información judicial en internet. Recomendaciones aprobadas durante el Seminario Internet y Sistema Judicial realizado en la ciudad de Heredia (Costa Rica), en julio de 2003 con la participación de poderes judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay.

[4] Constitución Política de Colombia, Artículo 15.- "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley."

[5] A propósito de la libertad de información, vale la pena citar el artículo 20, de la Carta Política, que garantiza a toda persona "*la libertad de expresar y*

ambos consagrados en nuestro ordenamiento como derechos fundamentales constitucionales.

Vale la pena destacar el indiscutible reconocimiento al derecho al buen nombre y a su no vulneración por los operadores de las distintas bases de datos informáticas. El buen nombre, alude, según la Corte Constitucional de nuestro país, "*al concepto que del individuo tienen los demás miembros de la sociedad en relación con su comportamiento, honestidad, decoro, calidades, condiciones humanas y profesionales, antecedentes y ejecutorias. Representa uno de los más valiosos elementos del patrimonio moral y social de la persona y constituye factor indispensable de la dignidad que a cada uno debe ser reconocida*"[6]

Para la Corte, "*Se atenta contra este derecho cuando, sin justificación ni causa cierta y real, es decir, sin fundamento, se propagan entre el público -bien en forma directa y personal, ya a través de los medios de comunicación de masas- informaciones falsas o erróneas o especies que distorsionan el concepto público que se tiene del individuo y que, por lo tanto, tienden a socavar el prestigio y la confianza de los que disfruta en el entorno social en cuyo medio actúa, o cuando en cualquier forma se manipula la opinión general para desdibujar su imagen".*

Sin embargo, también la Corte reconoce que este derecho no es gratuito; para ella, "*Por su misma naturaleza, exige como presupuesto indispensable el mérito, esto es, la conducta irreprochable de quien aspira a ser su titular y el reconocimiento social del mismo. En otros términos, el buen nombre se adquiere gracias al adecuado comportamiento del individuo, debidamente apreciado en sus manifestaciones externas por la colectividad*".

Ahora bien, en lo que atañe al *habeas data*, establecido expresamente en nuestra Carta Política, la Corte ha señalado que su núcleo esencial está dado por el derecho a la autodeterminación informática, entendida como la "*facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales*",[7] y, por la libertad, particularmente la económica, en el sentido de que podría verse vulnerada, si es restringida en forma indebida por la circulación de datos carentes de veracidad o simplemente no autorizados.

Sobre la manifestación del *habeas data*, la Corte ha señalado tres facultades de la persona a quien se refieren los datos

difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura."

[6] Corte Constitucional. Sentencia T-229 de 1994. Magistrado Ponente: Dr. José Gregorio Hernández Galindo

[7] Corte Constitucional de Colombia. Sentencia SU-089 de 1995. Magistrado Ponente: Dr. Jorge Arango Mejía

recogidos o almacenados, que se derivan de la norma constitucional referida, así: a) el derecho a conocer las informaciones que a ella se refieren, b) el derecho a actualizar tales informaciones y, c) el derecho a la rectificación, tratándose de informaciones que no correspondan a la verdad.

A pesar del gran interés que nos despierta este tema, en lo que atañe al uso, indebido o no, de datos personales, detenernos en el importante número de decisiones que se han proferido para su protección y en la doctrina generada a raíz de estos pronunciamientos, desbordaría el objetivo que nos hemos propuesto en esta oportunidad.

A propósito de los derechos sociales, económicos y culturales, la Constitución Política de Colombia, se refiere en su artículo 42, a la naturaleza de la familia y expresamente señala que la *honra, la dignidad y la intimidad de la familia son inviolables*.

Sobre la protección al derecho a la intimidad, también se han ocupado el Código del Menor y el Código de Procedimiento Penal actualmente vigentes en nuestro país.

Así, por ejemplo el Código del Menor, a propósito de los documentos y actuaciones administrativas o jurisdiccionales que se derivan del proceso de adopción[8], ha señalado una reserva de 30 años, con posibilidad de expedición de copias exclusivamente a solicitud de los adoptantes, del adoptivo que ha llegado a la mayoría de edad, o de la Procuraduría General de la Nación, con fines de investigación, aunque existe la posibilidad de levantamiento de la reserva en casos excepcionales previstos en la ley.

Además, el Código señala la restricción a los medios de comunicación, de realizar transmisiones o publicaciones que atenten contra la integridad moral, psíquica o física de los menores, que inciten a la violencia o hagan apología de hechos delictivos o contravencionales, entre otros.

Tratándose de hechos delictivos en los que aparezca involucrado un menor como autor, partícipe o testigo de los mismos, no se permite entrevistar, dar el nombre, divulgar datos que identifiquen al menor o puedan conducir a su identificación.

La citada prohibición está consagrada además para los casos en que el menor es víctima de un delito, salvo que sea necesario para garantizar el derecho a establecer su identidad o la de su familia si fuere desconocida; de no ser así, se requiere la autorización de los padres o, en su defecto, del Instituto Colombiano de Bienestar Familiar.

A su vez, el Código de Procedimiento Penal vigente[9], también a manera de ejemplo, establece en su artículo 11, a propósito de los

[8] Decreto 2737 de 1989, art. 114

[9] Ley 906 de 2004

derechos de las víctimas, el deber del Estado de garantizar su acceso a la administración de justicia, guardando la debida protección de su intimidad, la garantía de su seguridad, y la de sus familiares y testigos a favor.

El citado código prohíbe hacer registros, allanamientos, incautaciones en domicilio, residencia, o lugar de trabajo, sin que medie orden escrita del Fiscal General de la Nación o su delegado, de conformidad con las normas previstas en el mismo código, salvo en situaciones de flagrancia y en las demás contempladas por la ley.

Lo mismo se prevé en el caso de ser necesaria la búsqueda selectiva en bases de datos que no sean de libre acceso, o cuando fuere necesario interceptar comunicaciones.

Así, debe mediar autorización previa del fiscal que dirija la investigación cuando se requiera adelantar búsqueda selectiva en las bases de datos, que implique el acceso a información confidencial, referida al indiciado o imputado o, inclusive a la obtención de datos derivados del análisis cruzado de las mismas.

Ahora bien, el Consejo Superior de la Judicatura, en desarrollo del mandato previsto en la Ley Estatutaria de la Administración de Justicia[10], en el sentido de propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia, ha avanzado en el estudio de mecanismos tendientes a la protección de datos personales en la publicación de jurisprudencia en el marco de internet, aunque en este tema, debemos reconocer la dificultad que se presenta al marcar la diferencia entre lo público y lo privado.

Por ejemplo, en el caso de las decisiones proferidas por la Corte Constitucional, es claro que todo fallo que se refiere a la constitucionalidad de una norma vigente dentro del ordenamiento jurídico, tiene el carácter no sólo publico sino de obligatorio cumplimiento por los operadores judiciales. No ocurre lo mismo en el caso de la revisión de decisiones relativas al ejercicio de la acción de tutela, a través de la cual existe un pronunciamiento sobre la protección de un derecho fundamental de carácter constitucional. Allí, el derecho a la intimidad

[10] Ley 270 de 1996. Art. 95.- TECNOLOGIA AL SERVICIO DE LA ADMINISTRACION DE JUSTICIA El Consejo Superior de la Judicatura debe propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia. Esta acción se enfocará principalmente a mejorar la práctica de las pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información.

Los juzgados, tribunales y corporaciones judiciales podrán utilizar cualesquier medios técnicos, electrónicos, informáticos y telemáticos, para el cumplimiento de sus funciones.

Los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales.

Los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad, y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley.

de quienes se pueden ver afectados por la decisión, que también debe ser protegido, lleva a concluir en algunos casos la necesidad de omitir el nombre o nombres de las personas involucradas.

En nuestro país, tratándose del derecho a la intimidad, en una providencia judicial, es el juez que profiere la decisión, quien en últimas tiene la facultad de disponer si se omite o no el nombre de las personas sobre las cuales ella recae.

En todo caso, en el tratamiento de la jurisprudencia, creemos en principio que para la creación de líneas jurisprudenciales o para la realización por parte del intérprete de un verdadero análisis jurisprudencial, resulta irrelevante citar el nombre de las partes objeto de una decisión judicial, salvo, claro está, que por la naturaleza de la decisión, su trascendencia nacional, ya sea histórica, social o cultural resulte ser una condición necesaria.

En lo que se refiere a los avances tecnológicos, dentro del Convenio suscrito entre la Comunidad Europea y el Gobierno de la República de Colombia, denominado "Fortalecimiento del sector justicia para la reducción de la impunidad en Colombia", cuya finalidad es fortalecer el sector con miras a la consolidación del Estado de Derecho y a la reducción de la impunidad en Colombia con énfasis en el sistema penal, y que espera dentro de sus resultados que el sistema judicial cuente con modernas herramientas que faciliten su administración y el conocimiento para la toma de decisiones, se ha previsto como una de sus actividades, la modernización del Cendoj, y en particular, el rediseño de la página web de la Rama Judicial

"En lo que atañe al habeas data, establecido expresamente en nuestra Carta Política, la Corte ha señalado que su núcleo esencial está dado por el derecho a la autodeterminación informática, entendida como la "facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales",1 y, por la libertad, particularmente la económica, en el sentido de que podría verse vulnerada, si es restringida en forma indebida por la circulación de datos carentes de veracidad o simplemente no autorizados"

de Colombia, herramienta fundamental de comunicación en el ámbito nacional, y que ha sido un valioso instrumento de apoyo para brindar información oportuna a los servidores judiciales y al público en general sobre la Rama. En materia de protección de datos, el proyecto apunta a definir las tecnologías más

apropiadas para controlar la publicación de la información jurisprudencial disponible en los repositorios diseñados en la Rama Judicial.

Sobre la publicación de jurisprudencia en el marco de internet, esta actividad resulta prioritaria, dado que en la actualidad no contamos con una reglamentación especial para la publicación de datos personales. Nuestro sistema actual de gestión de procesos denominado "Justicia XXI" registra toda la información que atañe a los diferentes expedientes que se diligencian en los despachos judiciales, y permite su consulta directa desde interfaces web publicadas en la página web, salvo, en sana lógica, en la divulgación de la sentencia en aquellos casos no muy frecuentes en los cuales el juez haya ordenado la omisión de ciertos datos, omisión que debe hacerse de manera manual antes de ingresarla al sistema. En esté sentido, a excepción de las seguridades propias que caracterizan el sistema, como tal no contempla mecanismos de protección de datos personales de manera automática.

De esta manera, en el proyecto de construcción de la bodega de datos de la Rama Judicial, adelantado por la Sala Administrativa del Consejo Superior de la Judicatura de Colombia, dentro del citado convenio, se busca desarrollar las capas e interfaces necesarias para proteger los datos y dinamizar la publicación de jurisprudencia en Internet.

En la implementación del software de gestión "Justicia XXI", en la mayoría de los equipos servidores de la Rama Judicial, que se consolida como un estándar en materia de sistemas de información de control y seguimiento de procesos, hemos visto la necesidad documentar y potenciar el sistema para satisfacer las necesidades documentales de la comunidad; para tal efecto, el proyecto de rediseño de la página web de la Rama Judicial contempla en su fase de diagnóstico la definición de los requerimientos técnicos necesarios a implementar en materia de protección de datos y de seguridad que sirvan como pilares en la puesta en funcionamiento de nuevos servicios como la minería de datos e inteligencia web, atendiendo lo establecido en la normativa y/o recomendaciones de los expertos.

Culminada la primera fase, esperamos poder introducir estos mecanismos en la construcción de la bodega de datos, aprovechando los sistemas existentes, es decir, sin que ello repercuta en aquellos que se encuentran en funcionamiento y especializados en la gestión de los despachos.

Para los sistemas de información que no se publican directamente desde el software de gestión "Justicia XXI", se ha previsto desarrollar una capa de inteligencia de negocios que proteja los datos publicados por este medio y que puedan incorporarse a la bodega de datos de la Rama Judicial para

potenciar, de esta manera, los servicios disponibles a la comunidad.

En esta misma vía, en desarrollo de las disposiciones legales y con el ánimo de contribuir al mejoramiento de la eficiencia y eficacia de la administración de justicia, la Sala Administrativa del Consejo Superior de la Judicatura, avanza en la implementación de mecanismos que permitan la agilidad en las comunicaciones. En este sentido, reglamentó la utilización de medios electrónicos e informáticos, para permitir a los servidores judiciales autorizados, remitir actos de comunicación procesal, por correo electrónico, con el aval propio de una entidad certificadora autorizada de acuerdo con la ley.

La utilización de este medio electrónico se perfila como una importante herramienta para el cumplimiento de las funciones de administración de justicia, en el desarrollo de los actos de comunicación procesal susceptibles de realizarse a través de mensajes de datos y método de firma electrónica.

Traemos a colación el tema de la certificación digital, dadas las bondades que en materia de incorporación de tecnología de avanzada, representa para la administración de justicia. De esta manera, están dadas las herramientas para permitir de manera segura a los despachos judiciales enviar comunicaciones, citaciones y notificaciones que puedan surtirse a través de medios electrónicos, dentro del respectivo ámbito de aplicación.

En la resolución de los conflictos judiciales, este es sin duda un paso importante para que en un futuro próximo, el ciudadano pueda interactuar electrónicamente con la administración de justicia de manera ágil, confiable y segura ✧

Sobre el Autor

Mariana Gutiérrez Dueñas es Directora del Centro de Documentación Judicial - Cendoj, de la Sala Administrativa del Consejo Superior de la Judicatura de Colombia.

Samuel Páez es Ingeniero de Sistemas de la División de Información y Comunicaciones del mismo Centro.

Procedimientos legales y administrativos para la protección de datos personales en archivos.

Dr. Alfredo Chirino Sánchez*

Ponencia al Congreso Internacional "Transparencia y Acceso a la Información"
Puebla, México, 24, 25 de Noviembre 2005.

1. Introducción

Es muy importante reflexionar sobre el papel del acceso a la información en el marco del Estado Social y Democrático de Derecho.

El acceso a la información es un requisito indispensable para alcanzar un verdadero Estado Democrático de Derecho, basado en valores tales como la transparencia y el respeto a la dignidad esencial de la persona.

Este derecho fundamental no es más que una parte esencial del derecho a la información, y no puede entenderse separado de este.

Los países de la región tienen una cultura administrativa reacia al acceso a la información, producto, principalmente, de una larga tradición de secreto y de reserva. Para romper esta circunstancia, resulta indispensable no solo un cambio de cultura administrativa, sino también la realización práctica de los principios de acceso sugeridos.

Junto al desarrollo de la libertad de información y del derecho a expresar libremente el pensamiento, tiene un papel importante en el reconocimiento de estas garantías democráticas el respeto a la autodeterminación informativa. Este último derecho es una reivindicación indispensable en una coyuntura histórica donde las democracias se definen por la intensidad y dinamismo del flujo de informaciones: La persona también debe ser protegida en una sociedad que se automatiza.

Un listado de principios de acceso a la información debe contener, al menos, una declaración especial sobre el valor del acceso para combatir la corrupción y alcanzar una mayor participación de los ciudadanos en los asuntos de gobierno. Además deben reconocerse procedimientos ágiles para que las personas accedan a las informaciones y no sean abrumadas por las ingentes cantidades de datos que pueden ser proveídos sobre cualquier materia de interés público.

El costo razonable y proporcional al tipo de informaciones solicitadas es otro requisito esencial.

La administración pública debe ir creando una cultura de acceso, haciendo transparentes a los ciudadanos sus trámites y giros de actividad competencial, con el fin de que puedan permitir un control público de su gestión.

El acceso a la información es un requisito indispensable para alcanzar un verdadero Estado Democrático de Derecho, basado en valores tales como la transparencia y el respeto a la dignidad esencial de la persona

La rendición de cuentas, la transparencia y la participación civil parten de una base común: el acceso a la información, por lo cual deben estructurarse responsabilidades de los funcionarios para incentivar y propiciar el acceso a la información y la protección de los datos sensibles. Las sanciones pueden ser de carácter penal, sin embargo, no deben de dejarse de lado las posibilidades de un derecho de intervención, que saque provecho de las opciones normativas provenientes del derecho civil y del mismo derecho administrativo.

La eficacia, en todo caso, de las reglas sobre acceso a la información pública, como la de cualquier otra normativa, depende de la voluntad de ponerlas en vigencia y del compromiso de los ciudadanos por hacerlas valer en la cotidianeidad, rasgos indiscutibles de la lucha por la vigencia y realización de los derechos humanos, en general.

Es realmente paradigmático que el tema de los riesgos de las tecnologías de la comunicación e información empiece a tener espacio en la discusión jurídica de nuestro margen cultural. Y lo es precisamente porque es muy difícil explicar que algo que contiene una esperanza tan alta de garantizar desarrollo y libertad de nuestros pueblos sea, al mismo tiempo, una puerta abierta para el abuso y el control desmedido. Mantener una sana actitud crítica frente a estos desarrollos es, además, algo que resulta sospechoso y hasta contraproducente para quien ose plantear dichas reservas.

La historia de la protección de datos ha sido, con todo, una historia de la legislación que pretendió dar un estándar de tutela efectivo frente a los riesgos de crear perfiles de los ciudadanos a partir de multitud de detalles y de informaciones que podían ser adquiridos mediante la recopilación y comparación

electrónica de diversas fuentes. Para Simitis, por ejemplo, la historia de la protección de datos tiene una primera fase con la aprobación de la Primera Ley de Protección de Datos del Land Hesse de la República Federal de Alemania[11], el 30 de septiembre de 1970. Luego de esa primera normativa el tema se ubicaría definitivamente en el derecho alemán, y empezaría a desbordarse a diferentes leyes de los Länder y también de la Federación.

También en la década de los sesenta y los setenta del siglo XX surgieron inquietudes, movimientos culturales y legislaciones de tutela en otros países europeos y también en los Estados Unidos de Norteamérica. Su fuente de nacimiento fue también la preocupación por los enormes acervos de datos que empezaban a formarse en manos de la administración central y de algunas compañías privadas. En los Estados Unidos de Norteamérica no pasó desapercibido, por ejemplo, el hecho de la enorme cantidad de datos que empezaban a acumularse en los registros de los bancos de datos de algunas compañías telefónicas, algunos de ellos importantes para la prestación de servicios, algunos otros no directamente vinculados a las tareas y obligaciones que estas compañías asumían con los usuarios.

Lo anterior refleja, singularmente, como la reflexión jurídica sobre el tema suele ir precedida de una alta sensibilidad social sobre los riesgos de ser observado de una manera intensa y sutil, y esta sensibilidad no suele nacer sola, sino que tiene vinculaciones a momentos históricos donde dichos riesgos no son ciencia ficción sino una realidad tangible y amenazante, tal y como ocurrió en la Alemania nazi con la GESTAPO y en la antigua Alemania Oriental con la STASI. Los ejemplos, sin embargo, de control y observación de las prácticas y costumbres del ciudadano han sido una constante en otras latitudes y en diversos regímenes. No obstante, en América Latina la llegada del tema ha sido reciente y probablemente desligada de las angustias y sufrimientos que han motivado los cambios legislativos en otras regiones del mundo.

La discusión de América Latina surge, entonces, con una fresca visión, que bien vale tener en cuenta.

La temática de la protección de datos ha llegado para quedarse en América Latina. A pesar de las muchas décadas en donde el problema ha sido pasado por alto, ha llegado el momento en que tanto el legislador como la literatura empiezan a tomar conciencia de la necesidad de explorar la profunda sensibilidad del fenómeno de la interconexión de datos y de los riesgos de hacer transparentes al control y

[11] Simitis, Spiros, en: Simitis, Spiros, Dammann, Ulrich; Geiger, Hans-Georg; Mallmann, Otto; Walz, Stefan, Kommentar zum Bundesdatenschutzgesetz, Baden-Baden, Nomos Verlagsgesellschaft, 4. Edición aumentada, § 1, Número 1.

al abuso hasta los detalles más íntimos de la convivencia humana.

2. El derecho a la autodeterminación informativa y su discusión

Este derecho se conoce en la discusión jurídica alemana como el derecho a la autodeterminación informativa (informationelle Selbstbestimmung) y tiene precisamente su punto de partida en la intimidad, pero significa más que ésta, es la tutela de áreas de libertad, de las áreas en las que un sujeto puede autodeterminarse, en la gestación y desarrollo de su plan de vida. Aquí entran en funcionamiento, también tutelas procedimentales a este derecho, con el fin de que el ejercicio de otras garantías y derechos pueda ser resguardada. Es por ello que el Tribunal Constitucional Alemán, en su famosa Sentencia sobre la Ley de Censos de 1983, le dio un rango constitucional a la tutela del derecho a la autodeterminación informativa.

3. Situación de la protección de datos en Costa Rica

La respuesta a los problemas del procesamiento de datos personales en Costa Rica se ha manifestado, exclusivamente, en la interposición de recursos de amparo, la mayor parte de ellos caracterizados por ser reclamos por la inclusión de datos incorrectos, imprecisos o inexactos sobre el historial crediticio del impugnante.

Lo anterior puede llevar a la conclusión preliminar de que el ámbito de tutela de la intimidad y privacidad del ciudadano costarricense tiene una única sensibilidad: la de referirse de manera directa a la interacción económica a la "autodeterminación financiera" de la persona, y no necesariamente a los muchos otros ámbitos en que se desarrolla la personalidad de los costarricenses y que son, por derecho propio, las áreas usualmente vinculadas a la discusión legislativa y doctrinal del derecho a la autodeterminación informativa.

En todo caso, resulta claro y evidente que la tarea de tutela ha correspondido directamente a la Sala Constitucional, la cual ha realizado un trabajo de interpretación muy cuidadoso, que ha permitido un rápido proceso de incorporación del derecho a la autodeterminación informativa al bagaje conceptual de nuestra jurisprudencia constitucional, lo cual merece un trabajo de análisis más cuidadoso del que podemos realizar en la presente investigación. No obstante, intentaremos dar un bosquejo de las aristas más importantes del desarrollo jurisprudencial y observar mediante él, cómo ha entretejido nuestro Tribunal Constitucional tanto el ámbito de tutela del habeas data,

como los principios del derecho a la protección de datos.

4. El habeas data como síntesis de la discusión latinoamericana

En la literatura latinoamericana es recurrente la referencia al habeas data, como forma de tutela de los ciudadanos frente al tratamiento de sus datos personales.

La vinculación del habeas data con el habeas corpus es mucho más que casual, y puede encontrarse literatura que defiende un concepto de "habeas data" como una acción similar al habeas corpus[12], esto es, que en lugar de "traer el cuerpo", se trata de "traer los datos". Qué se hará con ellos y qué amplitud de tutela se ofrecerá dependerá, en casi todos los casos de la regulación normativa específica o de la interpretación que den los Tribunales, usualmente constitucionales, a la cuestión.

Suele vincularse a su núcleo de tutela los derechos a la honra, a la buena reputación, a la intimidad y al derecho a informarse[13].

En la discusión del problema del procesamiento de datos en América Latina surge casi por asociación inmediata el concepto de „habeas data". Derivado en gran medida del concepto de „habeas corpus", el habeas data pretende hacer referencia a la posibilidad jurídica de proteger el derecho de los ciudadanos a acceder a las informaciones personales que se encuentren disponibles en registros magnéticos y manuales con el fin de ser revisados, y si representan para la persona un perjuicio, también el de ser corregidos o eliminados.

Debe insistirse que no se trata de un derecho del ciudadano a poseer los datos, ni tampoco de exigirlos como si se tratara de un ejercicio derivado del derecho a la propiedad. Se trata más bien de instrumentar una verdadera garantía procedimental para que realice un derecho sustantivo que a su vez intenta proteger el derecho del ciudadano a saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales. Esta articulación suele ser difícil, ya que el habeas datan no es más que una garantía procedimental, esto es una garantía para acudir a una determinada vía y ahí solicitar los datos o las informaciones que se entiende son lesivas a los derechos protegidos, y como pretensión solicitar la anulación, borrado, obstrucción o corrección de los datos que afectan a la persona. Se trata, entonces,

[12] Sagués, Néstor Pedro, El Habeas Data: Alcances y Problemática, en: Sánchez, Alberto, El derecho público actual. Homenaje al Prof. Dr. Pablo A. Ramella, Buenos Aires, Depalma, 1994, p. 179, cfr. También Chiriboga Zambrano, Galo, La acción de amparo y de hábeas data: garantías de los derechos constitucionales y su nueva realidad jurídica, en: http://www.ildis.org.ec/amparo/hab.htm .

[13] Así, por ejemplo, Chiriboga, La Acción, op. Cit. La Constitución Federal Brasileña considera incluidos dentro del ámbito de tutela del habeas data, tanto a la vida privada, a la honra, el derecho a la imagen, y concentra el ámbito e tutela a las informaciones contenidas en bancos de datos pertenecientes a entidades públicas o de carácter público, lo que está previsto en el Art. 5º, LXXII de la actual Carta Magna brasileña

de un derecho reactivo y no de uno preventivo. Funciona cuando ya ha sucedido un daño, que puede ser, en algunos casos de incalculables proporciones, por la afectación que puede recibir una persona al producirse interconexiones automáticas de los bancos de datos

Concebir al habeas data como un derecho absoluto sobre los datos o un medio procesal para ejercer un poder "cuasi" patrimonial sobre ellos, sería incorrecto. Tan incorrecto, como concebir a la autodeterminación informativa como otra forma para el derecho a poseer los datos. El derecho a la autodeterminación informativa no le concede al ciudadano un definitivo y absoluto poder sobre sus datos[14], sino el derecho a estar informado del procesamiento de los datos y de los fines que se pretende alcanzar, junto con los derechos de acceso, corrección o eliminación en caso de que se cause un perjuicio. Aquí se pone el interés, entonces, en la "autodecisión" o en la "autodeterminación" del individuo, lo que se desea es garantizarle su posibilidad de participación como ciudadano frente a un procesamiento de datos personales que lo puede hacer transparente para el control y reducirlo a un mero objeto del ambiente informativo.

Desgraciadamente, el habeas data latinoamericano se ha concentrado en un derecho reactivo de índole procesal constitucional[15], y decimos desgraciadamente, porque ha hecho que la figura depende de la amplitud y generosidad de la interpretación de los tribunales constitucionales de los diversos supuestos o constelaciones de casos. Los modelos europeos y norteamericanos se inspiran en diversos puntos de partida. En el caso europeo, como ya hemos visto, se ha puesto el acento en establecer deberes, la mayor parte de ellos preventivos, para salvaguardar a la persona antes de que sucede a una posible afectación a su derecho a la autodeterminación informativa. Los Estados Unidos han preferido tutelar acciones individuales bajo el amparo de una ley que defiende específicamente la privacidad de los hogares y de las personas[16].

El habeas data, en nuestra concepción, se queda a medio camino, entre la tutela integral de los ámbitos de autodeterminación del ser humano, y la posibilidad de construir una tutela preventiva de las lesiones que como inmensos riesgos se ciernen sobre las posiciones jurídicas de los ciudadanos en una sociedad orientada a la información. No debe dejarse de lado, que

[14] Scholz, Rupert y Pitschas, Rainer, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin, Dunker und Humblot, 1984, p. 27.

[15] Sobre el carácter indudablemente constitucional del habeas data cfr. en lugar de muchos otros: Gozaini, Osvaldo Alfredo, El proceso de habeas data en la nueva ley, en: http://www.abogarte.com.ar/habeasdata1.html

[16] Así Gozaíni, Proceso, op. Cit.

los derechos de la tercera generación[17], en la clasificación de Pérez Luño, surgen ante el fenómeno inevitable de la "contaminación" provocada por ciertos usos de las nuevas tecnologías[18]. El derecho a la autodeterminación informativa es uno de estos derechos, y exige que la regulación normativa sea coherente con su naturaleza. Es por ello que deben tomarse en cuenta no sólo los derechos de acceso y control, sino también previsiones de carácter técnico que salvaguarden, con efectividad, los derechos involucrados[19].

La inevitable limitación que ofrece una garantía exclusiva en el ámbito procedimental se manifiesta, muy especialmente en Brasil, donde la Constitución misma limita el ejercicio del habeas data contra incorrectos datos e informaciones contenidos en bancos de datos públicos, lo que es una decisión incorrecta, si se le evalúa, por ejemplo, desde la perspectiva del cambio de posiciones acaecido en la década de los ochenta y noventa del pasado siglo, cuando los privados adquirieron un enorme poder informático y lo utilizaron para vender datos personales y con ello generar un riesgo insospechado para la capacidad de autodeterminación de las personas.

El habeas data poco va a lograr si conserva esa naturaleza de mera garantía procedimental[20], ya que obligará a poner todas las cartas en el ejercicio ex post de la jurisdicción. Sería mucho más práctico avanzar en dirección del reconocimiento de un derecho del ciudadano a desarrollar un plan de vida, de crear las condiciones de su autorrealización en una sociedad de conocimiento. Si el problema se visualiza desde allí, podrá comprenderse que lo que hay de por medio se trata realmente del viejo problema de otorgar un verdadero y efectivo status civitatis a la persona, para que pueda desarrollar su personalidad y definir las condiciones dentro de las cuales interactuará con sus semejantes.

Es por ello, que consideramos que un ejercicio del habeas data, sin un correlativo derecho de información sobre las formas en que se realizará el procesamiento, los objetivos y fines del mismo, la extensión, el destino final de los

[17] Las leyes de la primera generación serían, según este autor, las leyes que se concentraban en una autorización previa de los bancos de datos, lo que tenía sentido ya que estas leyes surgieron cuando el procesamiento de datos era centralizado, los equipos voluminosos y fácilmente localizables. Luego surgieron las „leyes de la segunda generación", las cuales pusieron el énfasis en los datos sensibles, a fin de evitar daños a la privacidad y ofrecer alguna garantía frente a posibles prácticas discriminatorias que pudieran tener su origen en el uso de esos datos „sensibles". Luego vendrían las leyes de la tercera generación, interesadas en el „uso" y „funcionalidad" de las informaciones. Aquí ubica Pérez Luño, por ejemplo, a la LORTAD española.. Cfr. Pérez Luño, La Tutela de la Libertad Informática, op. cit., pp. 97-98.

[18] Cfr. Pérez Luño, La Tutela de la Libertad Informática, op. cit., p. 97.

[19] Esta unificación entre herramientas técnicas y protección de datos es promocionada, por ejemplo, por Hassemer, Winfried, Über die Absehbare Zukunft des Daztenschutzes, KJ (Alemania) 1996, pp. 103 y ss.

[20] El art. 5, inciso LXXII de la Constitución brasileña postula: „...ceceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros de bancos de dados de entidades governamentais ou de caráter público; b) para a retificação, quando não se prefira fazê-lo por processo sigiloso judicial ou administrativo".

datos personales le quita transparencia, por un lado al procesamiento mismo de los datos y, por el otro, hace imposible que el ser humano tome nota de que sus datos serán objeto de manejos más allá de su decisión, con incalculables consecuencias para él, tanto dentro como fuera de las fronteras de su país.

5. El "Habeas data" como forma de protección de la persona frente al tratamiento de datos personales en Costa Rica

Un proyecto redactado en el año de 1996 intentó introducir una reforma a la vigente Ley de la Jurisdicción Constitucional No. 7135 del 19 de octubre de 1989, a fin de que se adicionara un Capítulo IV referido al „Habeas Data" en el Título III sobre los recursos, como una forma de „amparo específico" en materia de tutela de la „identidad" o „libertad" informáticas.

Se partía de la premisa de que el amparo en Costa Rica era lo suficientemente amplio como para brindar una tutela a la libertad informática "sostenible", haciendo una curiosa separación entre "habeas datas propio" e "impropio", siendo este último el que garantiza el acceso a la información, frente a la cual se tiene un "interés legítimo"[21].

El así llamado "habeas datas propio" contemplaría los derechos de acceso, modificación, adecuación al fin, confidencialidad, eliminación e inclusión de datos de la persona. No se analiza cuáles etapas del tratamiento de la información serían tuteladas, y parece desprenderse de la argumentación de los motivos del Proyecto, que se atiende al interés en cuanto al dato final, tal y como se encuentra consignado en el banco de datos, no así, por ejemplo, a las fases de recogida y grabación de los datos o, por ejemplo, la transmisión de datos más allá de las fronteras.

El Proyecto consideraba necesario contemplar esta figura procesal, con el fin de lograr una ágil y efectiva forma de acceso "acorde con los derechos en peligro".

En cuanto a los derechos merecedores de tutela a través de esta forma de garantía procedimental se citaban, entre otros la "autodeterminación informativa"[22], la "intimidad" y la „libertad informática", es decir, una serie de contenidos conceptuales abarcadores de otros tantos derechos derivados de la dignidad humana y del libre desarrollo de la personalidad.

Lo que no se entiende, es cómo es que será posible conjurar los peligros de "estigmatización del individuo" y en el "aspecto

[21] Exposición de Motivos, Expediente No. 12827, p. 30.

[22] Exposición de Motivos, Expediente No. 12827, p. 7.

social", cuando toda la apuesta normativa se concentra a permitir la reacción cuando el daño ya se ocasionó, y las ulteriores consecuencias podrían sentirse, sin exageración, en otras latitudes vía el flujo transfronteras de datos personales, uno de los supuestos más importantes de la "aldea global" en la que se ha convertido nuestro mundo.

Los efectos de una regulación como ésta podrían ubicarla como un intento más de "patrimonializar" la tutela de la intimidad, fenómeno que ya hemos discutido en otra parte[23].

6. El acceso a la información y la protección de datos

Luego de discutir sobre las implicaciones del derecho al acceso a las informaciones públicas y sus vínculos con otros derechos humanos, es posible tener claro que cualquier regulación sobre este derecho debería orientarse hacia las alcanzar las siguientes metas, las cuales, además, han sido recogidas por diversas regulaciones jurídicas recientes[24]:

a. Una regulación sobre acceso a las informaciones públicas debe apuntar hacia un mejoramiento efectivo de la calidad de vida de las personas a través del ejercicio de la libertad de acceso.

b. El conjunto regulativo debe permitir, también, la utilización sistemática de medios de participación comunitaria en la toma de decisiones[25].

c. Los procedimientos que se establezcan para permitir el acceso deben ser sencillos y expeditos.

d. Debe instarse a las administraciones a promover una cultura de transparencia, mediante la difusión de informaciones que promuevan el conocimiento por parte de la ciudadanía de sus proyectos y orientaciones.

[23] Cfr. Chirino, Alfredo, La tutela de la autodeterminación informativa como un nuevo bien jurídico penalmente tutelado. El caso del Proyecto de Código Penal de Costa Rica de 1995, en: Revista Nueva Doctrina Penal, Buenos Aires, Argentina.

[24] Los siguientes principios han sido derivados y ampliados del listado planteado por Chong López, Blanca, en su ponencia "Principios Fundamentales del Derecho a la Información", presentada en el foro de consulta ciudadana para la elaboración de la "Ley de Transparencia y Acceso a la Información Pública del Estado de Coahuila de Zaragoza, en México, el 28 de febrero de 2003. Una regulación específica en la materia la contiene, por ejemplo, las reglas de "Acceso del Público a la Información" del Banco Europeo de Inversiones, que puede ser consultada en: http://www.eib.org/Attachments/strategies/pai_rules_es.pdf

[25] La propuesta de leyes modelo realizada por la Secretaría Jurídica de la Organización de Estados Americanos incluye también una propuesta de ley de participación civil, la cual es entendida dentro de una estructura integral de normas que son conducentes a combatir la corrupción administrativa, y la ignorancia de amplios grupos de población que es el terreno fértil para permitir que dicha corrupción se desarrolle. Cfr. Groisman, Enrique Isaac, Ley Modelo sobre Mecanismos de Participación de la Sociedad Civil en la Prevención de la Corrupción, en: Subsecretaría de Asuntos Jurídicos. Departamento de Cooperación y Difusión Jurídica, Organización de Estados Americanos, Construyendo Transparencia. Legislación Modelo para Prevenir la Corrupción, San José, Costa Rica, CONAMAJ, 2001, pp. 67 y ss.

e. La difusión de informaciones[26] debe ser proveída por todos los medios tecnológicos disponibles, en concordancia práctica con las condiciones reales de la población que es receptora de las informaciones.

f. Las administraciones obligadas[27] deben garantizar, además del acceso a las informaciones, también la tutela de las personas frente a eventuales tratamientos de sus datos personales.

g. Las políticas de difusión de información deben orientarse a generar una amplia rendición de cuentas por parte de los funcionarios públicos, de tal manera que los ciudadanos puedan valorar su desempeño.

h. Contribuir a una mejor organización, clasificación y manejo de los documentos en posesión de las entidades públicas.

i. Un sistema de acceso a las informaciones públicas debe contribuir a la democratización de la sociedad y a la vigencia del Estado de Derecho.

j. Debe establecerse un régimen de sanciones administrativas y penales que garanticen el cumplimiento de los objetivos de la legislación.

7. Análisis de la jurisprudencia constitucional

La Sala Constitucional ha venido realizando, entre tanto, una interpretación del artículo 24 que se concreta en el concepto de intimidad como un "...derecho del individuo a tener un sector personal una esfera privada de su vida, inaccesible al público salvo expresa voluntad del interesado".[28] Refiere entonces a la difícil discusión de lo que es la „esfera privada de vida". Para intentar delimitar los marcos de esta esfera privada, el analista se encuentra hoy, en primera instancia, con algunos ejemplos citados por la jurisprudencia, que usualmente conducen a una lectura tradicional de la estructura de la intimidad en la

[26] Las leyes de acceso a la información deben incluir no sólo el derecho de acceso a "información" y "datos", sino que debe incluir también a las actas y a los registros. Esto le permitirá a las personas acceso a dichas actas y registros, así como a formular preguntas, cuando lo que solicitan no es un dato sino más bien una respuesta por parte de la administración, o solicitar que se realicen comparaciones de datos en diversos bancos o bases de datos según determinados criterios, o cuando buscan información que tienen los funcionarios públicos pero que no están registrados.

[27] El ámbito de cobertura de las leyes de acceso a la Información Pública debe extenderse virtualmente a todo el sector público, incluyendo no sólo a la administración central y descentralizada, sino también a los gobiernos y administraciones locales. Las leyes de acceso también deberían incorporar a sociedades del derecho privado que realicen competencias públicas. Esto último es observado como positivo, ya que el sector privado toma conciencia con ello de la importancia de adquirir deberes de responsabilidad cuando asumen esas competencias, y que por tal razón quedan expuestos a la verificación y al derecho de saber de los ciudadanos. Estos últimos encontrarán positivo no tener que lidiar con los depositarios de estas competencias y su idea de que sus informaciones están protegidas por la confidencialidad comercial. Cfr. al respecto The Campaign for Freedom of Information, Response to the Government´s Freedom of Information White Paper, Marzo 26 de 1998, en: http://www.cfoi.org.uk

[28] Sala Constitucional, V. 5736-94, citado según Córdoba, Fallas, Ramírez, Valerín, Constitución Política de la República de Costa Rica. Concordada, Anotada y con resoluciones de la Sala Constitucional, San José, Costa Rica, Asamblea Legislativa, 1996, p. 101.

Constitución costarricense de 1949[29], tales como: la inviolabilidad de los documentos e informaciones privadas y el secreto bancario.

La Sala Constitucional costarricense, sin embargo, ha tomado conciencia de otros problemas que tienden a superar el enfoque tradicional como lo es la dificultad para vivir en una sociedad donde un ciudadano no tiene „...derecho a mantener reserva sobre ciertas actividades u opiniones suyas y obtener amparo legal para impedir que sean conocidas por otros, en especial cuando para conocerlas deban emplearse procedimientos clandestinos..."[30] Y esto es así, toda vez que la mención a los procedimientos clandestinos de acceso a la intimidad no sólo abre el frente de batalla frente al control ilegal y los ataques desproporcionados que sufre la intimidad con la acción de los órganos de la investigación criminal, como porque también toma en cuenta que para un ciudadano „...resulta imposible o muy difícil convivir y desarrollar a plenitud los fines que una persona se propone, sin gozar de un marco de intimidad, protegido de injerencias del Estado y otros ciudadanos"[31].

En efecto, la intimidad, en su concepto constitucional, no sólo protege la „esfera privada" de los ciudadanos como un área donde se excluye del conocimiento de los otros una serie de datos e informaciones, salvo manifestación expresa del afectado, sino que su salvaguarda garantiza también el desarrollo a plenitud de la persona, la posibilidad de la „convivencia" y, agregaríamos nosotros, la

posibilidad de participación activa en el proyecto social, mediante el ejercicio de otros derechos fundamentales.

[29] Esta estructura, que hemos llamado tradicional, ha sido comentada en la investigación titulada: La tutela de la autodeterminación informativa como un nuevo bien jurídico penalmente tutelado, de pronta aparición en la Revista Nueva Doctrina Penal, de la Editorial del Puerto, donde hacemos referencia a los problemas que enfrenta el derecho penal para asumir una tutela moderna de la intimidad, aspecto que tiene mucho que ver con la superación de la estructura tradicional de tutela derivada del derecho constitucional. Cfr. Chirino, La Tutela, op. cit., passim.

[30] Sala Constitucional, V.3308-94 citado según: Córdoba y otros, Constitución Política, op. cit., p. 101.

[31] Ibid.

La intimidad es, entonces, no sólo la salvaguarda de la esfera privada, sino también una garantía de convivencia y participación social. Es una unión de la idea de tutela de una esfera íntima y recóndita, con la idea de libertad en la democracia, y en tal sentido, opera como un punto de entronque con el concepto de autodeterminación informativa, en tanto y en cuanto, se garantice para el ciudadano un derecho de acceso a sus datos personales, como ejercicio activo de tutela de sus posibilidades de participación democrática[32].

Si la interpretación proveniente de la Sala Constitucional se mantiene coherente sobre las líneas de esta reciente jurisprudencia es posible esperar, tarde o temprano, algún fallo de principio que siente las bases del derecho del ciudadano a ser protegido frente a los tratamientos de sus datos personales, pero esto se producirá sí y solo sí la Sala Cuarta decide entender esta relación entre la intimidad y la democracia, es decir, como una garantía para el ejercicio de otros derechos fundamentales previstos en la Constitución de 1949 que definen al ciudadano como una entidad que actúa libre, interactuando con otros y desarrollando su plan de vida libre de intervenciones estatales o privadas, mientras este plan no entre en contradicción con las bases del sistema (Artículo 28, segundo párrafo, de la Constitución de 1949). Se trata de una difícil interpretación, donde los bienes jurídicos en juego, son de difícil equilibrio, como el mismo Tribunal Constitucional lo ha reconocido[33].

Como anotación final debe subrayarse que la aceptación del vocablo "autodeterminación informativa" tiene una serie de consecuencias de orden constitucional, y por supuesto, significa una toma de posición sobre el bien jurídico tutelado. El concepto de "autodeterminación informativa" (Recht auf informationelle Selbstbestimmung) ha sido incorporado por la doctrina y jurisprudencia alemana, y manifiesta un status interpretativo bastante claro, sin embargo, en el ambiente europeo no parece haber una aceptación de este concepto, cuando, por ejemplo, se prefiere

[32] Como lo señala Podlech, comentando la Ley Fundamental de Bonn de 1949, la protección constitucional de la intimidad tiene una dimensión material, constituida por la protección del libre desarrollo de la personalidad, de la autodeterminación informativa, del respeto al ámbito privado del ciudadano, pero también ostenta una dimensión institucional caracterizada por la protección del matrimonio y la familia; y una dimensión espacial constituida por la protección de la habitación. Es decir, que la intimidad o privacidad no se agota en una sola de esas dimensiones, sino que han de atenderse todas ellas en la protección jurídica, ya que la intimidad tiene, en relación con la democracia una conexión directa. Muchos derechos fundamentales, aquí también la privacidad, ganan su legitimidad precisamente de su capacidad para coadyuvar en el funcionamiento de la democracia. Es por ello que las limitaciones a la privacidad y las limitaciones a ésta que pongan en peligro al ejercicio de derechos fundamentales que forman parte esencial de la participación en la democracia, serían inaceptables en un régimen constitucional democrático. Cfr. Podlech, Adalbert, Das Recht auf Privatheit, en: Perels, Joachim (Edit.), Grundrechte als Fundament der Democratie, Frankfurt am Main, Suhrkamp, 1. Edición, 1979, p. 52.

[33] Sala Constitucional V.678-91, citado según Córdoba y otros, en: Constitución Política, op. cit., p. 110.

hablar de un "droit à la vie privèe" o de un "right to privacy", que tienen una mayor orientación a la tutela de la vida privada, tal y como está regulada en el artículo 8 de la Declaración Europea de Derechos Humanos. En estos otros ordenamientos jurídicos sigue presente una fuerte impronta por la tutela de la "esfera privada", la que desde nuestro punto de vista tiene serias dificultades para una efectiva comprensión, análisis e interpretación dogmática de los ataques tecnológicos al derecho del ciudadano a determinar quién, cuando, dónde y bajo qué circunstancias toma contacto con sus datos personales.

8. El problema del acceso y la protección de datos en Archivos y Bibliotecas

El tema del acceso es fundamental para los Archivos y Bibliotecas, los cuales, al ofrecer un servicio público de enorme importancia para el país, promueven la difusión del conocimiento, la educación y la cultura. Por ello, sus servicio se basan en la libre circulación de las informaciones y de las ideas.

Es así como, la Federación Internacional de Asociaciones e Instituciones Bibliotecarias (IFLA) apoya totalmente el Manifiesto de la UNESCO sobre las Bibliotecas Públicas, e insisten sobre la necesidad de que los gobiernos nacionales, estatales y locales proporcionen a las bibliotecas la legislación y la ayuda económica adecuadas[34].

El uso libre y eficaz de Archivos y Bibliotecas depende, casualmente, de adecuadas técnicas que permitan al usuario el acceso cierto y transparente a la información que necesita para formarse en los campos y áreas de su interés, lográndose en el proceso un mayor desarrollo de los países y un aumento de la información disponible a través de las publicaciones e investigaciones que se realicen.

La IFLA propone algunas acciones que deberían de ser tomadas en cuenta por Archivos y Bibliotecas para desarrollar un efectivo acceso a la información:

"...Las bibliotecas deben estar suficientemente dotadas para poder informar, mantener el personal y contar con los recursos necesarios para ayudar a las personas en su formación permanente, su independiente toma de decisiones y su desarrollo cultural y económico.

Los bibliotecarios tienen la responsabilidad profesional de ofrecer en las bibliotecas que dirigen todas las perspectivas sobre los temas actuales e históricos; las colecciones y los servicios no deberán estar sujetos a ningún

[34] Cfr. Comité de acceso a la Información y Libertad de Expresión, Informe Preparado para la Reunión del Consejo De La IFLA en Copenhague, Dinamarca 1997, en: http://www.ifla.org/IV/ifla63/II

tipo de censura ideológica, política, racial, lingüística ni religiosa.

Las asociaciones y las bibliotecas deberán recusar cualquier forma de censura que impida el cumplimiento de su responsabilidad de facilitar información y formación.
El derecho de una persona a utilizar la biblioteca no ha de ser denegado o limitado por razones de origen, edad, sexo, raza, religión, nacionalidad, situación social o económica, o por sus ideas.

Las bibliotecas deben respetar el derecho a la intimidad personal, tanto en el uso de información como en el manejo y conservación de datos personales"[35].

9. Acerca de la protección de los datos personales en los servicios bibliotecarios y archivísticos

En las legislaciones sobre archivo y servicios de biblioteca de la República Federal de Alemania, especialmente en la Ley de Archivos estatales de Baden- Württenberg ("Landesarchivgesetz Baden-Württemberg, § 5 Recht auf Auskunft und Gegendarstellung") Se consigna, simple y llanamente, el derecho de todo ciudadano a que su autodeterminación informativa sea protegida también en ese ámbito. Se protegen no solo los archivos y registros manuales, así como también los registros electrónicos, que contengan informaciones personales.

Las leyes de acceso a la información que han sido aprobadas, principalmente en Europa, reconocen la protección de la información sensible de los ciudadanos, que también es conservada en actas y registros magnéticos y manuales de la administración.

La sensibilidad de la información personal debe ser definida por las leyes de protección de datos, utilizando diversos criterios[36]. En

[35] Ibid.

[36] Se citan como principios básicos de la protección de datos personales los siguientes: a) El principio de la justificación social, que significa que la recolección de datos personales debe tener un propósito general y usos específicos que sean socialmente aceptables; b) El principio de minimalismo en el tratamiento de datos personales, esto es que el tratamiento debe reducirse al mínimo indispensable para cumplir con los fines legales establecidos; c) Principio de recolección de los datos a partir del consentimiento del afectado, que implica que los datos personales solo serán recopilados a partir de un consentimiento informado expreso del afectado por el tratamiento de datos; d) Principio de recolección lícita, los datos solo podrán ser recopilados mediante procedimientos lícitos, sin fraude o engaño al afectado; e) Principio de Sujeción al fin del procesamiento de datos, los datos solo podrán ser tratados para cumplir el fin para el que originalmente fueron recopilados, y para el cual se prestó consentimiento por parte del afectado, cualquier desviación de ese fin convertiría en ilícito el tratamiento de datos; f) Principio de confidencialidad, los datos serán recopilados para cumplir el fin legal y no serán revelados, ni podrán estar disponibles para terceros, si no hay de por medio un consentimiento del sujeto afectado o una autorización legal al efecto; g) Principio de seguridad técnica del tratamiento, se deberán de tomar las previsiones según el estado de la técnica para salvaguardar la integridad de los datos de accesos ilícitos y para velar por que no se pierdan o se destruyan; h) Principio de transparencia del tratamiento de datos, los ciudadanos deben conocer los procedimientos para tratar los datos, con el fin de que puedan valorar la existencia, propósito, uso y métodos de operación de los sistemas de protección de datos; i) Derecho al olvido, los datos no pueden ser conservados para siempre, una vez cumplido el fin legal deben ser destruidos; j) Principio de control por medio de instancias especiales, se trata de que el derecho de la protección de datos ser realice por medio

general, se entiende por información de carácter personal aquellos datos, así como cualquier información concerniente a persona físicas identificadas o identificables[37]. Al no decir que ha de entenderse concretamente por "datos personales" se abre la puerta a una consideración amplia de los mismos, lo que resulta conforme a las modernas tendencias en el derecho a la protección de los datos personales, en donde el carácter de los datos carece de interés ya que en el estado actual del procesamiento de datos todos los datos son importantes, toda vez que éstos pueden compararse, transmitirse y reelaborarse en fracciones de segundo con el fin de crear perfiles y cuadros completos de los ciudadanos. Los "datos personales" no están constituidos únicamente por datos alfanuméricos, sino que pueden también estar constituidos por imágenes y sonido[38]. Modernos desarrollos en la tecnología de reproducción, grabación y almacenamiento de datos hace posible, hoy día, que sean tan fácilmente accesibles los datos alfanuméricos, como también informaciones fotográficas y sonoras, que pueden ser digitalizadas y accesadas vía telemática, como hoy se ofrece de manera amplia en diversos servicios de Internet.

Así las cosas, los ciudadanos podrían pedir a las Bibliotecas y Archivos públicos, que sus informaciones personales falsas, inexactas o incorrectas sean rectificadas, con el fin de que el derecho a la autodeterminación informativa no sea lesionado, siempre y cuando el ciudadano demuestre un interés legítimo en tal actividad. Ha de reconocerse que no siempre la lesión ha sido provocada por la Biblioteca o el Archivo, sino que la lesión proviene de la actividad de alguna persona o institución que ha publicado la información, afectando algunos principios de la protección de datos.

En la Ley de Archivos de Baden-Württemberg se extiende este derecho al cónyuge, a los hijos y a los padres del afectado.

de organismos de control independientes, los cuales puedan realizar una tutela preventiva de los ciudadanos; k) Principio de acceso y rectificación, también conocido como el principio de participación individual, este principio alude al derecho del ciudadano a conocer los datos que sobre sí mismo están siendo procesados o tratados, revisarlos y rectificarlos cuando contengan información falsa, imprecisa o inexacta. Esto principios se pueden dividir en dos grandes grupos: los principios referidos al sujeto y los principios referidos al fichero y al tratamiento de datos, ambos son trascendentales en un acercamiento constitucional a este tipo de tutela.

[37] Las recientemente discutidas "Reglas Mínimas para la Difusión de Información Judicial en Internet", o "Reglas de Heredia", analizadas en un foro organizado en la Ciudad de Heredia, Costa Rica, por autoridades judiciales y técnicas de diversos países de Iberoamérica, definen los datos personales de la siguiente manera: "Datos personales: Los datos concernientes a una persona física o moral, identificada o identificable, capaz de revelar información acerca de su personalidad, de sus relaciones afectivas, su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva o familiar, domicilio físico y electrónico, número nacional de identificación de personas, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad o su autodeterminación informativa. Esta definición se interpretará en el contexto de la legislación local en la materia."

[38] Cfr. García Beato, María José, Principios y derechos en la Ley Orgánica 5/1992, de 29 de octubre, y en la Directiva 95/46 CE, en: Agencia de Protección de Datos, Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid, 1996, pp. 36-37.

Como puede observarse, no puede mantenerse la situación de Costa Rica sobre protección de datos con un mero recurso de amparo. Resulta indispensable una ley específica de protección de datos que permita resolver estos y otros difíciles problemas de los servicios de información.

10. ¿Una ley de protección de datos para Costa Rica?

La propuesta de introducir una ley de protección de datos en Costa Rica, resulta ser una manifestación más de la necesidad de llenar un vacío grave en la tutela del ciudadano frente a los riesgos de la moderna sociedad de la información; donde ésta adquiere un valor indudable, abriendo la puerta a nuevas formas de desarrollo humano, pero también a nuevos peligros de construcción de una sociedad panóptica sin lugar para el ocultamiento o para el secreto.

El Proyecto de la Diputada Margarita Penón, presentado con la firma de otros diputados y diputadas para su discusión legislativa, incluye una serie de aspectos de enorme importancia para el desarrollo de la tutela preventiva del ciudadanos, haciendo efectivos los principios de la protección de datos más modernos.

El Proyecto, entre otros aciertos, trata adecuadamente los aspectos tecnológicos - los que por otra parte son decisivos – y permite esperar de ella una acción muy amplia en los servicios de información públicos y privados, y los que vayan a desarrollarse a futuro conforme nuestra sociedad se integre en la así denominada sociedad digital.

Es muy difícil explicar que algo que contiene una esperanza tan alta de garantizar desarrollo y libertad de nuestros pueblos sea, al mismo tiempo, una puerta abierta para el abuso y el control desmedido

La evolución del derecho comparado presenta gran número de ejemplos de cómo será la estructura futura de las formas de tutela del derecho a la autodeterminación informativa: preventiva más que reactiva, dirigida a potenciar los derechos de información del ciudadano, la utilización de órganos independientes y con capacidad técnica para contrarrestar los avances vertiginosos de la tecnología de la información; así como también

el desarrollo de leyes específicas en los diversos campos en que el procesamiento de datos personales incide.

La idea de tutela parece, además, orientada a considerar como fundamentales aspectos tales como la "seguridad de los datos"; los "derechos de información del afectado"; y sobre todo, la inclusión del principio de proporcionalidad, con especial referencia al sub principio de "necesariedad" y de „apego a los fines del procesamiento", que permiten augurar una interesante actividad administrativa de tutela preventiva.

Debe de tomarse en cuenta que esta proyecto no elimina el "habeas data", ya que seguirá existiendo y conviviendo con este tipo de normas, en su carácter de garantía procesal, es decir, una forma de tutela de un derecho fundamental a través de un procedimiento, lo que tiene como punto de partida, que el derecho fundamental estará claramente planteado, y que los contornos de la tutela son prístinos. Estos dos últimos aspectos parecen estar muy claros en el Proyecto de Ley Penón, no sólo porque crea y organiza la tutela y, en segundo lugar, porque da lugar para una determinación sobre el derecho a tutelar.

11. Conclusiones

La información se ha convertido en un valor de cambio en la actual sociedad tecnológica, ella permite no sólo alcanzar muchas metas que el Estado Social se veía imposibilitado de cumplir con eficiencia, como también ha permitido influir en diversas formas de interacción entre los ciudadanos, muy especialmente en su comunicación. Es por ello que resulta necesario abrir un debate nacional para crear conciencia sobre el problema.

Junto al derecho a la información y a ser informado, cobra una especial importancia hoy en día el derecho a la intimidad.

El manejo de la información, su tratamiento y transmisión se han convertido hoy en día, junto con las tecnologías que hacen posible esto de una manera rápida y confiable, en las actividades económicas de mayor crecimiento, y sin duda, cumplirán un papel determinante en la forma en que los ciudadanos realicen muchas de sus actividades cotidianas.

Y será sin duda la que determinará el futuro y el desarrollo del mundo, muy especial el de los países de nuestro continente, los cuales están enfrentados en este momento a un dilema enorme provocado por las nuevas interacciones del mercado y el fortalecimiento de tendencias encarnizadas que forma parte de toda declaración de derechos en una sociedad democrática, así como el derecho a la intimidad, que en nuestra Constitución Política, tiene, al menos desde la perspectiva del texto formal, una relación inescindible con la libertad.

En efecto, la tutela de la intimidad es uno de las garantías más importantes del ciudadano, la cual adquiere con el desarrollo de la llamada "sociedad de la información" una relevancia todavía más señera, ya que las herramientas de la moderna tecnología hacen posible, no sólo plantear las bases para un desarrollo más integral de la persona y alcanzar algunos sueños democráticos, como lo es la posibilidad de que cada ciudadano se interese por los asuntos públicos y pueda intervenir directamente en las decisiones que puedan afectar sus derechos, sino que también engendran graves peligros, ya que facilitan el manejo, organización y comparación de una gran cantidad de datos sobre los ciudadanos, los cuales pueden ser así utilizados para controlarle y limitarle sus ámbitos de libertad.

En un trabajo publicado hace algunos años en Costa Rica, se ha sostenido que la utilización del recurso de amparo para tutelar al individuo frente a posibles abusos en el tratamiento de sus datos personales es un medio solamente temporal para alcanzar dicha tutela . Por el carácter tan técnico de esta materia, y tomando en cuenta que los riesgos para el ciudadano se presentan en todas las etapas del procesamiento de los datos, desde que se recopilan hasta que eventualmente se transmiten, el recurso de amparo revela muchas limitaciones, sobre todo que la reacción judicial puede perfectamente producirse cuando los daños para el derecho fundamental ya no pueden ser reparados, o cuando la mera exhibición de los datos o la imposición de una indemnización no realice el objetivo esencial de la tutela. Resulta, por ende, necesario, explorar la posibilidad de una tutela ampliada por medio de una ley específica que tome en cuenta los aspectos concretos del derecho a la autodeterminación informativa, como punto de partida en el camino hacia una tutela eficiente del ciudadano frente al tratamiento de sus datos personales.

El proyecto Penón nos propone ya un camino para alcanzar este estándar de protección, y da los mecanismos para permitir el desarrollo de formas de tutela más eficientes.

El desarrollo de un nivel de tutela razonable en este campo es un requisito esencial del Estado de Derecho, hacia allí debemos tender si queremos adquirir las condiciones para un desarrollo humano posible en una sociedad de la información ✧

**** El Dr. Alfredo Chirino Sánchez es Director de la Escuela Judicial, y Catedrático de Derecho Penal de la Facultad de Derecho de la Universidad de Costa Rica.***

Protección de Datos
En el Ecuador

Ing. Miguel Ángel Serrano,*

La protección de los datos de las personas naturales y jurídicas se establece para mantener la privacidad, su seguridad física y aspectos relacionados con la existencia misma pero también es necesario que los datos personales sean públicos para efectos de planificación nacional, toma de decisiones, reformulación de prioridades, etc.

La protección de datos a una información pública como es la de las causas judiciales conlleva el análisis de la normativa jurídica de manera tal que se otorga la información conforme indica el artículo 94 de la Constitución Política del Ecuador, acerca del habeas data, y se restringe la información al público en base a lo que las leyes de Ecuador disponen.

En lo relacionado a la primera instancia, en lo que concierne al sorteo electrónico de causas, los sistemas informáticos generan el proceso aleatorio y de manera inmediata el solicitante de la demanda obtiene el número de la judicatura en el que se sorteó la causa. De esa información almacenada en la base de datos es la que posteriormente se publica diariamente en el sitio Web.

Los datos a publicarse en el sitio Web de la Función Judicial de Ecuador y sus páginas Web solo se establecen después de que físicamente se ha creado el documento escrito dentro del proceso de tramitación de causas judiciales.

Toda la etapa investigativa que realiza el Ministerio Público y la Policía Nacional no se publica en el sitio Web de la Función Judicial ni en las pantallas tipo touch screen (sensibles al tacto) que existen en los diferentes distritos judiciales.

La ley de comercio electrónico existente en el Ecuador en su artículo 2 da igual valor probatorio al documento escrito que al documento electrónico pero la misma ley y su reglamento aclara que debe existir un tercero en el proceso de envío y recepción de mensajes electrónicos. Este tercer elemento es la "Entidad de certificación de información" la cual hasta la fecha, no existe legalmente constituida en el Ecuador. Por esta razón se envían las notificaciones electrónicas a los casilleros electrónicos de los abogados litigantes solo con una concepción informativa. La información existente en nuestro sitio Web y sus respectivas páginas Web distritales son de tipo informativa y no tienen la calidad de certificación de respaldo.

La protección de datos a una información pública como es la de las causas judiciales conlleva el análisis de la normativa jurídica de manera tal que se otorga la información conforme indica el artículo 94 de la Constitución Política del Ecuador, acerca del habeas data, y se restringe la información al público en base a lo que las leyes de Ecuador disponen.

Toda esta concepción en la protección de datos implica una infraestructura tecnológica con una serie de elementos de seguridad en la red de datos certificada, en los servidores transaccionales, en los motores de bases de datos, en los servidores Web, en los enlaces o telecomunicaciones, en la red "militarizada", en la red "desmilitarizada", etc. que nos encontramos implementando en los diferentes distritos judiciales del país con las restricciones presupuestarias que tiene la Función Judicial del Ecuador.✧

**** El Ing. Miguel Ángel Serrano es Director Nacional de Informática. Función Judicial Ecuador***

Habeas Data en El Salvador, Mecanismo De Protección de Datos, ¿Para qué?

Lic. Rafael Santiago Henríquez Amaya*

Aunque en El Salvador se trata de proteger el derecho a la autodeterminación informativa a través del proceso de amparo, éste no ha resultado ser un instrumento plenamente eficaz, en un mundo en el que el uso de las nuevas tecnologías avanza con mucha rapidez y, en el cual el comercio electrónico es una realidad. Resulta de vital importancia, el establecimiento de una ley especial (que conlleve un recurso procesal ad hoc como el hábeas data), en la que no existan vacíos legales que permitan el inadecuado uso de datos personales y dejen al ciudadano desprotegido frente a empresas y oficinas gubernamentales que ceden sus datos sin control; situando a El Salvador como un posible facilitador de los movimientos internacionales de datos.

Para entrar a hablar sobre *habeas data*, lo primero que debemos saber es su significado, el cuál, según la jurisprudencia de la Sala de lo Constitucional de la Corte Suprema de Justicia de nuestro país, constituye un mecanismo o instrumento que protege al individuo contra el uso ilegal o indebido de los datos personales por parte de entidades públicas o privadas, tutelando de una forma eficaz el derecho a la autodeterminación informativa. De tal manera que constituye una garantía cuyo fundamento en la normativa constitucional responde a la necesidad de los sujetos de proteger sus derechos ante la amenaza del acceso y uso indiscriminado de sus datos personales; es decir, que se trata de un instrumento judicial que entra en funcionamiento a petición de parte, cuando ésta ha cumplido con el requisito prejudicial de solicitar a la empresa que posee o maneja sus datos personales, le exhiba los mismos con el objeto de verificar los que han sido incluidos en los ficheros automatizados y comprobar la veracidad de los mismos. De no obtenerse la respuesta requerida, el Estado, a través de dicho mecanismo, interviene solicitando la exhibición, modificación, supresión, o actualización de los datos, según el caso, con la consiguiente responsabilidad civil para la empresa demandada en caso de comprobarse la vulneración al derecho en cuestión, sin perjuicio de la responsabilidad penal a que hubiere lugar.

En el ordenamiento jurídico salvadoreño no aparece la figura del *habeas data* como instrumento diseñado para la protección específica del derecho a la autodeterminación informativa como manifestación del derecho a

la intimidad, ello no significa que tal derecho quede totalmente desprotegido, pues partiendo de lo que establece el inciso primero del artículo 2 de la Constitución, que "*toda persona tiene derecho a (…) y a ser protegida en la conservación y defensa de los mismos*"; asimismo, el artículo 247 de la misma Carta Primaria, también en su primer inciso sostiene: *"Toda persona puede pedir amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia por violación de los derechos que otorga la presente Constitución";* le infiere que los derechos reconocidos expresa como implícitamente, deben ser garantizados a toda persona a través de los mecanismos de protección establecidos para su ejercicio. De manera que aunque no se disponga de una ley que prescriba los presupuestos procesales para materializar tal figura, se puede decir que la protección del derecho en mención puede ser efectuada a través del proceso constitucional de amparo (ya que éste se encuentra regulado en la Constitución como el instrumento de garantía que tiene por objeto tutelar los derechos constitucionales), no importando la naturaleza de la empresa o ente a quien se le atribuya la vulneración de dicho derecho.

Siendo el amparo en nuestro país, el medio utilizado para conocer las violaciones al derecho a la intimidad en el tráfico electrónico o autodeterminación informativa (ésto en ausencia de un mecanismo propio para ello como lo es el *habeas data*), la Sala de lo Constitucional de la Corte Suprema de Justicia ha sido constante en establecer como presupuestos básicos para la procedencia del proceso de amparo contra particulares, los siguientes: que el particular responsable del acto se encuentre en una situación de poder, que el acto u omisión sea parte del ámbito de constitucionalidad y que no existan mecanismos judiciales o administrativos de protección frente a actos de esa naturaleza; o que de haberlos, sean ellos insuficientes para garantizar los derechos del afectado o se hayan agotado plenamente para remediar el acto contra el cual reclama.

Por lo anteriormente expuesto, se afirma que frente a la ausencia de un desarrollo legislativo de la figura relacionada que establezca el procedimiento y los mecanismos de defensa pertinentes, la admisión de la pretensión constitucional relativa a señalar actuaciones que han supuesto afectación al derecho a la autodeterminación informativa, encaja dentro de la figura del amparo; y, en específico del amparo contra particulares cuando se trate de una empresa; por cuanto, el mal manejo de los datos personales que se atribuya a una autoridad, comprueba la configuración del primer presupuesto de procedencia del proceso de amparo; es decir, la existencia de una especie de situación de predominio de una autoridad en relación con la posición de un ciudadano.

Es menester realizar algunas consideraciones sobre el contenido jurídico de la

autodeterminación informática como manifestación del derecho a la intimidad y, su forma de ejercicio en la realidad social actual, a efecto de que su conceptualización sirva de marco de referencia para valorar si con su afectación se necesita o no en nuestro país, un medio de protección específica para este derecho.

El Habeas Data constituye una garantía cuyo fundamento en la normativa constitucional responde a la necesidad de los sujetos de proteger sus derechos ante la amenaza del acceso y uso indiscriminado de sus datos personales

En cuanto al reconocimiento de la autodeterminación informática como manifestación del derecho a la intimidad expresado en el texto constitucional, ha de partirse de lo que establece el inciso 2º. del citado artículo 2, que señala: "S*e garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".* En referencia específica a la intimidad personal, la Sala de lo Constitucional de la Corte Suprema de Justicia ha dicho que el contenido de tal derecho hace alusión al ámbito que se encuentra reservado *ad intra* de cada persona, en el que se originan los valores, sentimientos, etc., vinculados a la propia existencia de su titular y cuyo conocimiento importa únicamente a éste, y en su caso, a un círculo concreto de personas seleccionadas por el mismo; por tanto, en dicho ámbito opera la voluntad del individuo para disponer de todos aquellos aspectos que puedan trascender al conocimiento de los demás.

A pesar de que el derecho a la intimidad parte de la esfera privada del individuo, el mismo no se puede alejar del contexto social donde se ejercita; es decir, que no se desliga completamente del entorno social en el cual adquiere sentido y se relaciona con los otros miembros del colectivo social en forma individual o agrupada, lo que implica que el ejercicio de tal derecho puede encontrarse limitado por las necesidades sociales y los intereses públicos.

Efectivamente, la Sala de lo Constitucional expresó en la sentencia de amparo 118-2002, de fecha 2/03/2004, que "el derecho en estudio, ha ido perdiendo su carácter exclusivamente individual y asumido con mayor fuerza un papel colectivo y social importante, sin que ello signifique la eliminación de la nota

que identifica tal carácter –la individualidad– pues ésta se integra con un contenido público que viene a definirla y a complementarla frente a las nuevas circunstancias que van generándose en el tiempo. Así, el suministro de datos particulares que una persona proporciona a la administración pública mediante el empleo de fichas, solicitudes, entrevistas, es un suceso que le compete a la persona misma; y, sin embargo, es de interés también para los demás miembros de un determinado conglomerado social con una finalidad específica. A pesar de ello, el peligro que puede suscitar tal situación consiste más que en el conocimiento y posesión de los datos, en la posibilidad del uso inadecuado de los mismos".

Justamente, a raíz de dicho uso, surge la siguiente interrogante: **¿Qué riesgos implica el tratamiento inadecuado de datos personales?** La peligrosidad del uso inadecuado de las tecnologías de la información para la protección de datos del individuo se pone de manifiesto, básicamente, a través de las siguientes circunstancias: "(1) La publicación de datos que por su naturaleza pertenecen a la esfera íntima de la persona o que pueden ser tomados como elementos para prácticas discriminatorias; (2) La publicación de información errónea, inexacta, incompleta, desactualizada, parcializada, etc.; (3) La potencialidad de la informática para recopilar y almacenar masivamente datos de cualquier naturaleza sobre las personas y la facilidad para acceder a esa información; (4) La manipulación y/o "cruce" de los datos almacenados que permiten crear perfiles virtuales de las personas (conocer sus pautas de comportamiento, sus tendencias políticas, religiosas, sexuales, entre otras), que pueden resultar valoradas, bien o mal, para las más diversas actividades públicas o privadas; (5) el riesgo de que la información de las personas sea conocida y manipulada por grupos ilegales para diferentes fines (terrorismo, chantajes, extorsiones, saboteos, discriminaciones, etc.) y (6) La utilización de la información para fines no permitidos por la ley o no autorizados por el titular del dato".[39]

Frente al peligro anteriormente advertido existe una manifestación del derecho a la intimidad, que es precisamente el **derecho a la protección de los datos** y consiste en que el individuo pueda controlar el uso o tratamiento de los mismos, a fin de impedir una lesión a su esfera jurídica. Con la protección de datos, el derecho que se trata de proteger no es solamente el de la intimidad, sino algo con mayor profundidad que, en los ordenamientos de ámbito anglosajón, se ha dado en llamar *"privacy"* y que nosotros hemos adaptado al castellano como "privacidad".

La protección se realiza sobre el dato, de manera que éste no pueda ser tratado o elaborado, y convertido en información, nada

[39] Nelson Remolina Angarita. "Documentos GECTI sobre el Habeas Data y la Protección de Datos Personales". Bogotá, Colombia. Págs. 8-9.

más que para aquellos fines y por aquellas personas autorizadas para ello. Esta necesaria protección es un límite a la utilización de la informática ante el temor de que pueda agredir la intimidad de los ciudadanos, personal o familiarmente, y que pueda cortar el ejercicio de sus derechos.

Es por tanto el titular de los datos el único que, como norma general, puede decidir cuándo, dónde, cómo y por quién se tratan sus datos de carácter personal.[40]

El derecho a la protección de datos ha sido denominado de diversas formas, según el autor que lo formule; y así, se le conoce como derecho a la autodeterminación informativa o derecho a la intimidad informática; pero, indistintamente de su formulación, éste debe ser entendido como *aquél que tiene por objeto preservar la información individual que se encuentra contenida en registros públicos o privados, especialmente la almacenada a través de los medios informáticos, frente a su utilización arbitraria.* De modo que a partir del acceso a la información, exista la posibilidad de solicitar la corrección, actualización, modificación y eliminación de los mismos. Esto según jurisprudencia de nuestro país, pero, el continente europeo y otros países de Latinoamérica llevan a la práctica dicha protección por medio de un mecanismo especial como veremos a continuación, destacándose la verdadera importancia que tiene la protección de datos de carácter personal.

La Protección de Datos de Carácter Personal es una materia que ha tomado importancia en los últimos años a nivel mundial, fundamentalmente a raíz de la aprobación de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal; dicha importancias surge debido a la equiparación y transformación del derecho a la protección de datos personales en un derecho fundamental de las personas.

El derecho fundamental al que hacemos referencia tiene una estrecha relación con el derecho a la intimidad y al honor, encuadrándose éstos últimos dentro del art. 2 de nuestra Constitución, la cuál, como se mencionó con anterioridad, trata de proteger la conservación y defensa de los mismos a través del proceso constitucional de amparo. De igual forma, en diversos artículos de las normas primarias de cada país en el resto del mundo, se busca la protección específica del derecho a la autodeterminación informativa como manifestación del derecho a la intimidad, como por ejemplo, en el art. 18 de la Constitución de España; mencionamos dicho país, porque en su Constitución, el derecho en mención se incluye como un "nuevo" derecho fundamental, que adopta la denominación de libertad informativa o autodeterminación informática, protegiendo el "control que a cada una de las personas le corresponde sobre la información que les

[40] IFAI: Informe sobre Protección de Datos. "¿Qué es la protección de datos?". México. Pág. 6.

concierne personalmente, sea intima o no, para preservar el libre desarrollo de la personalidad".

"Es por dicha protección que podemos afirmar que el derecho a la intimidad en el ámbito informático implica lo siguiente: I. que todo individuo tiene derecho de acceder a la información personal y especialmente a aquella que se encuentre contenida en bancos de datos informatizados; II. que todo individuo ha de tener la posibilidad y el derecho a controlar, de forma razonable, la transmisión o distribución de la información personal que le afecte, III. que debe existir, en el ordenamiento jurídico, un proceso o recurso que permita hacer efectivos los puntos señalados. Todo ello con la finalidad de establecer la estructura mínima que permita el manejo fiable de los datos personales de los individuos que se encuentren en banco de datos mecánicos o informáticos para conservar la veracidad, integridad y actualidad de los mismos así como la regulación sobre la inaccesibilidad de otras instancias que no comprueben la existencia de una finalidad que justifique suficientemente la pretensión de conocerlos".[41]

Justamente, por todo lo que implica la protección de datos, es que el Dr. Nelson Remolina Angarita expresa lo siguiente: "Las leyes de protección de datos no se crean para evitar el tratamiento de datos personales sino para exigir que el mismo se realice con un debido proceso y mucha responsabilidad".

A raíz de todo lo anterior, nos surge la siguiente interrogante: ¿Por qué en El Salvador es necesaria la implementación del HABEAS DATA como mecanismo de protección de datos? A lo cuál podemos responder que "el habeas data, es la denominación de origen que mejor representa a los temas de protección de datos personales en Iberoamérica, coloquialmente hablando, si bien desde el punto de vista técnico el hábeas data es una

Esta necesaria protección es un límite a la utilización de la informática ante el temor de que pueda agredir la intimidad de los ciudadanos, personal o familiarmente, y que pueda cortar el ejercicio de sus derechos.

[41] Sala de lo Constitucional. Corte Suprema de Justicia. Sentencia de Amparo ll8-2002. San salvador. El Salvador.

garantía procesal constitucional".[42] En rigor a la verdad, los estudiosos consideran también al habeas data como un derecho fundamental: unos hablan de un aspecto de la libertad informática y otros de autodeterminación informativa.

Lo cierto es que con una ley procesal, la acción de habeas data, y otra sectorial de datos crediticios, ambas fundidas en un mismo cuerpo, El Salvador vendría a confirmar una tendencia que comenzó su andadura en febrero del año 2004, con el documento formulado por la Secretaria de la Presidencia de la República de El Salvador, llamado: *Estrategia Nacional de Gobierno Electrónico*, en el cuál se señala: "El concepto de gobierno electrónico (…) trata de una reforma de Estado, más ambiciosa, más allá del uso de la tecnología o de la prestación de servicios en línea. Se trata de una reforma del Estado, que busca transformar la forma en que el Gobierno se relaciona con los ciudadanos, la empresa privada y diversas organizaciones de la sociedad, por medio de un cambio radical en la gestión administrativa que fomente la eficacia y transparencia en la interacción del Gobierno con sus usuarios".

La *Estrategia Nacional de Gobierno Electrónico* permite desarrollar en nuestro país una sociedad de información y dentro de ella, todo lo relacionado con el comercio electrónico. Dicho desarrollo implica, una protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

Aunque en El Salvador se trata de proteger el derecho a la autodeterminación informativa a través del proceso de amparo, éste **no** ha resultado ser un instrumento plenamente eficaz, en un mundo en el que el uso de las nuevas tecnologías avanza con mucha rapidez y, en el cual el comercio electrónico es una realidad. Resulta de vital importancia, el establecimiento de una ley especial (que conlleve un recurso procesal ad hoc como el hábeas data), en la que no existan vacíos legales que permitan el inadecuado uso de datos personales y dejen al ciudadano desprotegido frente a empresas y oficinas gubernamentales que ceden sus datos sin control; situando a El Salvador como un posible facilitador de los movimientos internacionales de datos ✧

**** El Lic. Rafael Santiago Henríquez Amaya es Colaborador Jurídico del Área Constitucional del Centro de Documentación Judicial de la Corte Suprema de Justicia de El Salvador***

[42] Oscar Puccinelli. Discusión doctrinaria acerca de la naturaleza jurídica del hábeas data, "El Habeas Data en Indoiberoamérica". Editorial Temis. 1999. Pág. 103.

BIBLIOGRAFÍA

1. Constitución de la República de El Salvador. D.L. No. 38, de fecha 15 de diciembre de 1983, P.D.O. No. 234, tomo 281, del 16 de diciembre de 1983.
2. PROYECTO DE COOPERACIÓN INTERUNIVERSITARIA: *Situación de la Libertad Informática en El Salvador. Transmisiones Internacionales y Hábeas data,* Universidad Centroamericana José Simeón Cañas (UCA), San Salvador, El Salvador, 2005.
3. REMOLINA ANGARITA, Nelson: *Documentos GECTI sobre el hábeas data y la protección de datos personales,* Bogotá, Colombia, octubre de 2005.
4. GONZALEZ, María: *Protección Datos Carácter Personal,* Manaca Consulting, España, 2005.
5. DUBIE, Pedro: *¿Quo vadis? Iberoamérica fija un rumbo en protección de datos,* Argentina, 2005.
6. IFAI: INFORME SOBRE PROTECCION DE DATOS, *¿Qué es la protección de datos?*, México, 2005.
7. PUNICELLI, Oscar. DISCUSION DOCTRINARIA ACERCA DE LA NATURALEZA JURIDICA DEL HABEAS DATA: *El hábeas Data en Indoiberoamérica,* Editorial Temis, 1999.
8. SALA DE LO CONSTITUCIONAL. Corte Suprema de Justicia: *Sentencia de Amparo 118-2002,* San Salvador, El Salvador.

Jurisprudencia y Protección de Datos De Carácter Personal

Equipo de Dirección del CENDOJ

Desde la creación del Centro de Documentación Judicial en 1997, una de sus tareas fundamentales ha sido la de recopilar y difundir adecuadamente la jurisprudencia de los Tribunales españoles, de acuerdo con la normativa interna e internacional en este ámbito. Con ello se trata de ofrecer al colectivo judicial en particular, al resto de los operadores jurídicos, y al conjunto de los ciudadanos, los criterios de decisión de los órganos judiciales.

Esta labor de difusión planteaba desde el inicio un buen número de dificultades y de interrogantes. Dificultades de naturaleza técnica, que se han venido abordando con importante esfuerzo del equipo de trabajo del Centro de Documentación Judicial, y considerables dificultades de coordinación para recopilar de manera eficaz la información proveniente de los diversos órganos judiciales.

En cuanto a los interrogantes, se centraban no sólo en determinar cuáles eran los objetivos y los límites de la difusión, sino de manera muy destacada en conciliar la labor de dar a conocer los criterios de decisión de los Tribunales con los derechos de los ciudadanos en materia de protección de datos de carácter personal.

En las siguientes líneas pretendemos abordar precisamente esta cuestión, puesto que la situación en la que ahora nos encontramos, la difusión de los criterios de decisión de los Tribunales con exclusión de los datos de carácter personal, ha exigido algunas reflexiones previas y la puesta en práctica de actuaciones de tratamiento de las diversas resoluciones para lograr el objetivo exigido legalmente. Haremos también referencia a las actuaciones a realizar en el futuro, que centran los esfuerzos del Centro para conseguir los fines de protección de datos de manera más eficaz.

Desarrollaremos los siguientes epígrafes:

1) Dudas previas: relación entre difusión y publicidad.
2) Marco de actuación. Situación de partida.
3) Actuaciones concretas desarrolladas.
4) Perspectivas de futuro.

Dudas previas: relación entre difusión y publicidad

Era obligado hacerse esta pregunta porque los conceptos de publicidad en sentido procesal y de difusión de la jurisprudencia de los criterios de decisión, no siempre han estado suficientemente diferenciados. La respuesta a esa duda tiene, sin embargo, una relevancia clara en el tratamiento que haya que dar a las resoluciones dictadas por los órganos judiciales en cuanto a los datos personales.

Dicho de otra manera, la publicidad de los actos procesales como principio consagrado desde el propio texto constitucional y, como una manifestación del mismo, la obligación de leer las sentencias en audiencia pública, podría llevar a pensar que esa publicidad se extiende de tal manera que cualquier ciudadano tiene derecho a conocer las resoluciones judiciales en todo su contenido, incluidos los datos de carácter personal.

Este planteamiento, sin embargo, no es el correcto, y ha tenido que ser la jurisprudencia la que aclarase los conceptos y fijara definitivamente las bases para el cumplimiento adecuado de las exigencias constitucionales.

La publicidad procesal en sentido estricto aparece expresamente regulada en la Ley Orgánica del Poder Judicial en su art. 232, donde se señala que las actuaciones judiciales serán públicas, con las excepciones que prevean las leyes de procedimiento. Esta declaración general aparece, sin embargo, matizada en los artículos siguientes (art. 234 y 235 LOPJ) que se refieren en concreto al acceso a la información de los procedimientos, a los libros, archivos y registros, estableciéndose como requisito de tal acceso que se reúna la condición de interesado o como se señala en el primero de tales preceptos, que se acredite "interés legítimo".

La publicidad procesal no ampara la pretensión de cualquier ciudadano de acceder a los datos de cualquier procedimiento, y que sólo tienen acceso a ellos los que reúnan la condición de interesados.

En cuanto a las sentencias, tema que nos ocupa en este artículo, la ley se pronuncia en términos similares, y así el Art. 266 LOPJ dispone que las resoluciones judiciales, una vez extendidas y firmadas por el Juez o por todos los Magistrados que las hubieren dictado, serán depositadas en la Oficina judicial y se permitirá a cualquier "interesado" el acceso al texto de las mismas.

Por lo tanto, todas estas declaraciones, hacen referencia al concepto de "interesado", lo que permite deducir ya en una primera aproximación que no cualquier persona puede tener acceso a los procedimientos y al texto de las resoluciones judiciales, sino que aunque se garantiza la publicidad, ésta queda restringida a quien tenga interés en el procedimiento.

A pesar de estas precisiones legales y dadas las variadas interpretaciones que en la práctica se venían dando a estos conceptos, y en particular al término "interesado", la jurisprudencia se ha encargado de ir deslindando los diferentes ámbitos de la publicidad en sentido procesal, y con ello ha contribuido a sentar las bases para las políticas de difusión en cuanto afecta a los derechos de los particulares en materia de protección de datos.

Así, tiene especial relevancia la Sentencia del TS, Sala de los Contencioso Administrativo, de 3 de marzo de 1995 (Recurso nº 1218/91, interpuesto contra el Acuerdo del Consejo General del Poder Judicial de 10 de abril de 1991).

El tema de fondo que dio lugar al recurso ante el TS fue en su origen la decisión de varias Juntas de Jueces, posteriormente ratificada por las respectivas Salas de Gobierno de los Tribunales Superiores de Justicia y por el propio Pleno del Consejo, de no permitir a determinada empresa dedicada al cobro de impagados el acceso a los libros de sentencias de los juzgados.

En esta resolución se introducen importantes precisiones en cuanto a los ámbitos de la publicidad en el procedimiento judicial y se hace una triple distinción que aclara y delimita el derecho de los ciudadanos de acceder a las actuaciones judiciales. Se distinguen tres dimensiones de publicidad:

A) una publicidad amplia, o generalizada, que se refiere al público en general, a cualquier ciudadano, y que le permite acudir a la práctica de las diligencias que han de tener lugar en audiencia pública. Se trata de un derecho derivado de la declaración de publicidad de las actuaciones judicial del art. 120 de la Constitución española y a través de este acceso del público a la práctica de las actuaciones judiciales se produce un control y garantía de tales actuaciones;

B) una publicidad restringida o estricta, y limitada a las partes procesales, centrada pues en los actos de notificación o comunicación en el ámbito del proceso;

C) un ámbito intermedio, en el que el Tribunal sitúa las actuaciones judiciales ya finalizadas, incluida la sentencia, integradas en libros, archivos, o registros, y respecto de las cuales sólo tiene acceso el interesado en virtud de los art. 234, 235 y 266 LOPJ.

El Alto Tribunal entra a analizar, dentro de esta última dimensión de publicidad, el concepto de

interesado y aclara que *"el interés legítimo que es exigible en el caso, sólo puede reconocerse en quien, persona física o jurídica, manifiesta y acredita, al menos «prima facie», ante el órgano judicial, una conexión de carácter concreto y singular bien con el objeto mismo del proceso -y, por ende, de la sentencia que lo finalizó en la instancia -, bien con alguno de los actos procesales a través de los que aquél se ha desarrollado y que están documentados en autos".*

La conclusión más clara de esta resolución es que la publicidad procesal no ampara la pretensión de cualquier ciudadano de acceder a los datos de cualquier procedimiento, y que sólo tienen acceso a ellos los que reúnan la condición de interesados.

Cosa distinta es la labor de difusión, de información general sobre los criterios de decisión de los tribunales, que tiene otro ámbito y otras reglas y está encomendada al Consejo General del Poder Judicial a través de su Centro de Documentación Judicial. No importan los datos concretos del procedimiento, de sus intervinientes o participantes, sino que lo determinante es que los ciudadanos conozcan las líneas de la jurisprudencia de los tribunales, los criterios de actuación o decisión de los mismos, como parte del ordenamiento jurídico del país.

El art.107,10 LOPJ establece como competencia del Consejo General del Poder Judicial la publicación oficial de las sentencias y otras resoluciones del Tribunal Supremo y del resto de órganos judiciales. Así se establece también en el Reglamento de creación del CENDOJ y se ratifica en los acuerdos de pleno de 7 de mayo de 1997 y de 18 de junio del mismo año.

Estos acuerdos de Pleno, así como la Instrucción de la última fecha sobre remisión de las resoluciones al Consejo General del Poder judicial para su recopilación y tratamiento por el Centro de Documentación Judicial, fueron objeto de recurso ante la Sala de los Contencioso-Administrativo del TS en febrero de 2000 (recurso nº526/1997), quien desestimó tales recursos y ratificó con ello la distinción entra publicidad y difusión refiriéndose entre otras cosas a *la competencia del Consejo a través de su centro de documentación de dar a conocer los criterios de decidir de los tribunales.*

Y más próximo en el tiempo, el Reglamento de Aspectos Accesorios de las actuaciones judiciales en su redacción de 15 de septiembre de 2005, hace una distinción clara entre ambos aspectos dedicando una sección a la *publicidad de las actuaciones judiciales* y otra a la *publicación y difusión de las resoluciones judiciales,* en la que se regula el modo en que los órganos judiciales procederán a remitir al Consejo General del Poder Judicial, a través del Centro de Documentación Judicial y con la periodicidad que se establezca, copia de todas las sentencias, así como de otras resoluciones que puedan resultar de interés, que hayan sido dictadas por el respectivo órgano judicial.

Marco de actuación. Situación de partida

El Centro de Documentación Judicial se encontraba, pues, con la competencia y con la obligación de difundir los criterios de difusión del Tribunal Supremo y del resto de los Tribunales españoles, labor que exigía en primer lugar la recopilación de las sentencias. La tarea de recopilación obligaba a acudir a los órganos de origen y coordinar con las diferentes administraciones implicadas la obtención de tales resoluciones de cada uno de los sistemas informáticos de gestión procesal que operan en nuestro sistema judicial.

El Centro de Documentación comenzó recibiendo las resoluciones en papel, y posteriormente en soporte digital, y en la actualidad las propias aplicaciones informáticas permiten que el sistema replique la información periódicamente y que se disponga de ella en breve plazo desde que la resolución es elaborada en cada órgano judicial.

La cuestión relevante que aquí nos ocupa es que todas esas resoluciones llegan al Centro de documentación con los datos personales que llevan consigo, datos relativos a los diversos intervinientes en el proceso.

Esta constatación nos situó de inmediato frente a la problemática de la protección de datos de carácter personal. La ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (y en términos similares su antecesora la ley de 1992) señala en su art. 1 que su objeto es garantizar y proteger, en lo que concierne al tratamiento de los datos, las libertades publicas y los derechos fundamentales, y especialmente el de su honor e intimidad personal y familiar. Y afirma taxativamente que la ley será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Por otra parte, todas las disposiciones normativas que regulan la actividad de difusión que asume el Centro de Documentación Judicial, hacen referencia al respeto a la normativa en materia de protección de datos de carácter personal. Así, la Recomendación 3 (2001) del Comité de Ministros del Consejo de Europa sobre los servicios de tribunales y otras instituciones jurídicas ofertadas a los ciudadanos por las nuevas tecnologías y la Directiva 2003/98/CE del Parlamento Europeo y del Consejo de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público, en las que se considera como responsabilidad pública el poner a disposición del público, bajo forma electrónica fácilmente accesible, las decisiones importantes de la justicia, se hace referencia a la protección de datos de carácter personal, si bien sólo para enunciar que deberá estarse en cada caso a la legislación de cada uno de los países.

Y en la legislación interna, la LOPJ en su art. 107,10, al regular la competencia en materia de publicación oficial de las sentencias, señala que reglamentariamente se desarrollará esta competencia entre otras cosas para asegurar el cumplimiento de la legislación en materia de protección de datos personales. En un sentido similar el Reglamento de Aspectos accesorios de las actuaciones judiciales.

Nos encontrábamos, por lo tanto, con una competencia y una obligación de elaborar una

En este momento una empresa especializada en el sector procede a dar a las resoluciones un tratamiento uniforme y, utilizando un sistema semiautomático, consigue vaciarlas de datos personales

base de datos de resoluciones de los Tribunales que nos permitiera difundir los criterios de decisión por una parte, y con la obligación de respetar la normativa de protección de datos por otra.

Con una doble reflexión: que las explotaciones que pudiera hacer el Cendoj no necesitaban en modo alguno los datos contenidos en las sentencias, es decir, que la finalidad pública que desarrollamos no está relacionada con ningún tipo de explotación de los datos contenidos en las resoluciones, excluyéndose también cualquier aprovechamiento comercial de la base de datos elaborada.

Y, sin embargo, como receptores de los datos sensibles y como difusores de la base de datos de sentencias sentíamos la responsabilidad pública de evitar en la medida de lo posible que pudieran hacerse explotaciones posteriores indeseadas de los datos contenidos.

Por eso, desde el principio vimos la conveniencia de poner los medios necesarios para lograr el procedimiento de disociación previsto en la legislación.

Actuaciones concretas desarrolladas

Precisamente para cumplir con las exigencias legales previstas en la normativa sobre protección de datos de carácter personal, el Consejo ha venido abordando una serie de iniciativas que han permitido cumplir con las exigencias de los derechos en juego.

Para ello, desde los inicios del trabajo del Cendoj se establecieron una serie de contactos con empresas que pudieran dar un tratamiento a las resoluciones recibidas de los diversos sistemas de gestión procesal que fuera acorde con esas exigencias de respeto a la protección de datos de carácter personal.

En este momento una empresa especializada en el sector procede a dar a las resoluciones un tratamiento uniforme y, utilizando un sistema semiautomático, consigue vaciarlas de datos personales.

Consiste este procedimiento en transformar los documentos que llegan en diferentes formatos desde los sistemas de gestión procesal a un lenguaje estándar, el XML (eXtensible Markup Languaje), que permite el marcado de los diversos campos relevantes de las resoluciones.

En el proceso de transformación, se utiliza un programa de marcado de información relevante contenida en la resolución, como el órgano judicial, la fecha de dictado de la resolución, la jurisdicción, el ponente.. .y de vaciado de información sensible (datos de identificación o localización) sobre personas físicas implicadas o citadas en el procedimiento judicial y que deben de ser sustituidas u ocultadas en todo el documento. Para el vaciado de la información sensible, se aplica un programa de sustitución de términos, que exige la comprobación manual para verificar que lo que el programa ha considerado información sensible efectivamente lo es y que el término por el que propone sustituir esa información sensible a lo largo de todo el documento es el adecuado.

El resultado es un documento estructurado en formato XML, que contiene:

- Elementos marcados con información relevante (tipo de órgano, ponente, magistrados,..)
- Elementos listas de ocultación, que contienen el término a ocultar y el término sustituto correspondiente.
- Así como marcas en el texto de la resolución dónde se encuentra cada término a ocultar.

De forma que al visualizar la resolución, siempre se podrá presentar la misma con los datos originales o con los términos sustitutos, ocultando de esta forma la información sensible.

Al Centro de Documentación llega un documento en formato XML, debidamente tratado que contiene las listas de ocultación de la resolución, lo que permitirá en su caso recuperar el documento íntegro por si ello fuera necesario.

Este procedimiento nos permite obtener una base de datos normalizada y debidamente tratada, de aproximadamente dos millones de sentencias en este momento, correspondientes a las resoluciones dictadas por los órganos colegiados desde 1998, y cumplir con ella la misión de difundir los criterios de decisión, centrando ahora nuestros esfuerzos en dotar a esa base de datos de valores añadidos en cuanto a las herramientas de búsqueda y el análisis jurídico.

Perspectivas de futuro.

En la línea de mantener el equilibrio necesario entre respetar la normativa sobre protección de datos de carácter personal y la obligación legal que nos afecta de difundir los criterios de decisión de los tribunales, el Centro de Documentación continuará trabajando para encontrar los procedimientos más adecuados y más eficaces en el tratamiento de la base de datos de sentencias.

Dado el coste que supone el procedimiento actual y la limitación que presenta en cuanto a la cantidad de resoluciones que pueden ser tratadas anualmente, estamos valorando otras posibilidades que acrecienten el automatismo del proceso.

Así, seguimos algunas líneas de investigación con técnicas de inteligencia artificial que permitan utilizar herramientas automáticas de identificación y clasificación de términos y que sean aplicables al proceso de vaciado de datos de carácter personal, con lo que centraríamos el esfuerzo en el control manual posterior del resultado de tal procedimiento disociativo.

Además, también estamos valorando la posibilidad de aprovechar los propios datos personales que se registran en los sistemas de gestión procesal. Las resoluciones se dictan en el marco de un procedimiento registrado y tramitado informáticamente en cada órgano judicial. Si fuera posible homologar el registro de datos sensibles y relacionarlo con la sentencia que va a ser remitida al Centro para su publicación, conseguiríamos niveles de eficacia muy superiores y podríamos abarcar un número mucho mayor de resoluciones, traspasando previsiblemente la barrera de los órganos unipersonales, cuyas resoluciones son en muchas ocasiones de gran interés, y sin embargo no pueden ser difundidas adecuadamente.

Somos conscientes de que la automatización absoluta del proceso de vaciado es aún un objetivo lejano y por eso insistiremos en que la revisión posterior sea lo más precisa y minuciosa posible.

Sobre estas premisas, y en tanto no se produzca el desarrollo reglamentario que aborde los concretos aspectos de la protección de datos de carácter personal en las bases de datos judiciales y su incidencia en nuestra labor como órgano encargado de la difusión de la jurisprudencia, seguiremos trabajando para conciliar los derechos en juego y dedicando los esfuerzos personales, técnicos y de coordinación con la administraciones que sean necesarios para que el resultado final sea una base de datos completa y adecuadamente tratada con arreglo a los criterios legales ✧

Enero de 2006. El Equipo de Dirección del CENDOJ.

Reserva O Publicidad

Lic. Guillermo Corzo*

I. PRINCIPIO DE PUBLICIDAD

El principio procesal de la PUBLICIDAD es un principio generalmente reconocido en las legislaciones modernas, el cual puede definirse como: El derecho a que las diligencias y resoluciones sean del conocimiento no solamente de las partes y de los que intervienen en los procesos, sino de todos en general. Como parte de esa publicidad es que tradicionalmente se han recopilado y publicado los fallos de los diferentes órganos jurisdiccionales, tal el caso de la Gaceta de los Tribunales que se publica en Guatemala desde el año de 1881 hasta nuestros días.

Sin embargo, recientemente ha surgido la discusión sobre la legalidad de la publicación de ciertos datos relativos a las personas, en salvaguarda de su derecho a la privacidad o confidencialidad. Así, en ***materia jurisdiccional*** surge la disyuntiva entre publicar íntegramente las sentencias dictadas por los tribunales de justicia que contienen datos que han sido aportados o que de cualquier manera han salido a luz dentro de los procesos judiciales, o bien, eliminar de la publicación los datos estrictamente personales o que permitan identificar a las partes. En esta línea de pensamiento, principalmente se trata de mantener en reserva ciertos datos considerados como "sensibles" que pueden afectar el buen nombre de las personas, revelar aspectos de su condición económica o financiera, o divulgar situaciones que por razones morales, sociales o de otra índole las personas vinculadas a éstos preferirían que no se divulgaran.

Surge entonces la disyuntiva entre RESERVA O PUBLICIDAD, conceptos que vistos a la luz de la normativa –principalmente de índole constitucional- y valores de cada sociedad, tienen sus argumentos a favor y en contra.

Analizado el tema desde la perspectiva del Derecho, indudablemente la faceta más importante del tema es la relativa a las GARANTÍAS CONSTITUCIONALES que pueden citarse en respaldo de cada uno de estos criterios.

A favor de la tesis de la "reserva" se argumenta la existencia de un derecho

humano a la "*intimidad*", llamado también derecho a la "*autodeterminación informativa",* que permite al individuo vivir su propia vida protegido de toda interferencia en su integridad física o mental, en su honor y reputación, reservándose para sí sus sentimientos, opiniones, gustos, y demás circunstancias personales.

Se cita como fundamento de este derecho en nuestro ordenamiento jurídico, la Constitución Política de la República de Guatemala, que reconoce como derechos humanos la integridad y la seguridad de la persona, la inviolabilidad de su correspondencia, documentos y libros, y la discreción de la información contable o financiera obtenida por el Estado, y como complemento de estos derechos el llamado "hábeas data" que consiste en el derecho que tiene toda persona de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a su corrección, rectificación y actualización.

Por el contrario, en apoyo a la publicación íntegra de las sentencias, en la República de Guatemala encontramos que su Constitución Política contiene entre las Garantías y Derechos Individuales, los principios relativos al derecho a la libertad de información (en sus dos aspectos de libertad de informar y de ser informado), de publicidad de los actos administrativos, de libertad de emisión del pensamiento y de libre acceso a las fuentes de información, los cuales desarrollan los derechos reconocidos en la Declaración Universal de Derechos Humanos de la Organización de las Naciones Unidas, especialmente en su artículo 19.

Concretamente, el artículo 30 constitucional establece la *Publicidad de los actos administrativos,* con la única limitación de los asuntos militares o diplomáticos de seguridad nacional, o de datos suministrados por particulares bajo garantía de confidencia; y congruente con lo anterior, el artículo 35 constitucional establece la *Libertad de emisión del pensamiento,* por cualesquiera

Además de las disposiciones legales que permiten la publicación de las sentencias, existen leyes que obligan a ello como una pena accesoria o como medida de reparación en beneficio del afectado civilmente

medios de difusión, sin censura ni licencia previa. Además, garantiza el libre acceso a las fuentes de información, sin que autoridad alguna pueda limitar ese derecho, estableciendo como contrapartida que quien en uso de esta libertad faltare al respeto a la vida privada o a la moral, será responsable conforme a la ley.

Las normas constitucionales mencionadas también tienen sustento en el Pacto Internacional de Derechos Civiles y Políticos de la Organización de las Naciones Unidas, que establece que toda sentencia penal o contenciosa será pública, excepto en los casos de que el interés de menores de edad exija lo contrario, o en las actuaciones referentes a pleitos matrimoniales o a la tutela de menores (artículo 14); y reconoce el derecho a la libertad de expresión, que comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, derecho que a su vez entraña deberes y obligaciones especiales necesarios para asegurar el respeto a los derechos o a la reputación de los demás y la protección de la seguridad nacional, el orden público, la salud o la moral públicas (artículo 19).

En Guatemala, tradicionalmente se ha sostenido la publicidad de los actos administrativos, y como consecuencia de ello se publican las sentencias que dicta la Corte Suprema de Justicia en la "Gaceta de los Tribunales", que remonta sus orígenes al Acuerdo Gubernativo del 22 de febrero de 1881, emitido por el Presidente de la República fundamentado en que "... la publicidad de las resoluciones judiciales es una eficaz garantía de los individuos cuyas personas y derechos están sujetos a la acción de los tribunales, y lo es al propio tiempo de los funcionarios encargados de la administración de justicia: que hoy es aún más indispensable, porque dotada la República con una legislación nueva, debe darse a conocer la inteligencia que prácticamente se da a sus disposiciones y los términos en que se hace su aplicación racional y filosófica: que esto además podrá contribuir notablemente a facilitar el estudio de los profesores del derecho y el de los jóvenes que emprenden la carrera del foro, abriendo también el campo a ilustradas y fructuosas discusiones y útiles trabajos...".

Actualmente, la publicación de la Gaceta de los Tribunales de la República de Guatemala está a cargo del CENTRO NACIONAL DE ANÁLISIS Y DOCUMENTACIÓN JUDICIAL –CENADOJ-, creado mediante Acuerdo número 037/002 emitido por el Presidente del Organismo Judicial y de la Corte Suprema de Justicia, de fecha 17 de junio de 2002, Acuerdo que entre las funciones globales del CENADOJ señala la de apoyar la actividad jurisdiccional con la selección, ordenamiento, análisis y tratamiento, edición, publicación y difusión de información jurídica legislativa, jurisprudencial y doctrina; y entre las funciones específicas le asigna la de "Difundir

la jurisprudencia de la Corte Suprema de Justicia y otras sentencias seleccionadas de los demás órganos jurisdiccionales del Organismo Judicial" y la de atender las necesidades de información en materia de jurisprudencia, legislación y doctrina de los magistrados, jueces y auxiliares judiciales.

Las motivaciones que en aquel entonces, año 1881, tuvo el Presidente de la República para la creación de la Gaceta de los Tribunales son aún valederas en la actualidad, pues doctrinariamente se reconoce la importancia de la publicación de sentencias en cuanto que:

a) la comunidad jurídica puede comentar las sentencias, actuando como instancia de control;
b) constituye una mejora en la eficacia de los órganos jurisdiccionales, gracias a la información que reciben;
c) coadyuva a la publicidad de las leyes, mediante su interpretación e individualización;
d) garantiza el derecho a la igualdad en el sentido de que casos iguales o similares habrán de ser resueltos en forma igual o similar.

Por ello, la inserción de las sentencias del Tribunal Supremo de Guatemala, en la Gaceta de los Tribunales, es para el conocimiento general, antecedente jurisprudencial y elemento de estudio a base de comentario.

II. PUBLICACIÓN OBLIGADA DE SENTENCIAS:

Además de las disposiciones legales que permiten la publicación de las sentencias, existen leyes que *obligan* a ello como una ***pena accesoria*** o como medida de ***reparación*** en beneficio del afectado civilmente**.**

Tal es el caso de:

a) los delitos contra el honor;
b) delitos relativos al narcotráfico, lavado de dinero y financiamiento del terrorismo; y,
c) los juicios mercantiles relativos a competencia desleal.

a) El Código Penal, contenido en Decreto 17-73 del Congreso de la República, contempla entre las ***penas accesorias*** la publicación de la sentencia y la tiene establecida para los delitos contra el honor (injuria, calumnia y difamación) en los que a petición del ofendido o de sus herederos, el juez podrá ordenar se publique el fallo en uno o dos periódicos de los de mayor circulación en la República, a costa del condenado o de los solicitantes subsidiariamente, cuando estime que la publicidad pueda contribuir a reparar el daño moral causado por el delito.

b) En leyes penales especiales como la Ley contra la Narcoactividad, la Ley contra el Lavado de Dinero u otros Activos y la Ley contra el Financiamiento del Terrorismo,

también se establece como pena accesoria la publicación de la sentencia.

c) En materia mercantil, encontramos que el Código de Comercio prescribe que en los procesos por ***Competencia Desleal,*** en caso de que se determine que estos actos se realizaron por dolo o culpa del infractor, el Tribunal podrá disponer la publicación de la sentencia por cuenta de aquél.

En Guatemala, específicamente, la Internet, no se encuentra regulada por normas jurídicas de carácter nacional, lo que acarrea problemas de diversa índole a sus usuarios, tales como el uso y la regulación de la diversa información que allí se encuentra, así como la protección de la privacidad y datos personales, para que éstos no puedan ser usados indebidamente

III. EXCEPCIONES AL PRINCIPIO DE PUBLICIDAD.

Como excepción a la regla general de publicidad de los actos administrativos, la Constitución Política de la República de Guatemala contempla casos de excepción, en los que se prohíbe su publicidad.

Los primeros casos de excepción los encontramos en el artículo 30 constitucional, relativos a los ***asuntos militares o diplomáticos de seguridad nacional,*** los que por su propia naturaleza no son susceptibles de llegar a incorporarse en un proceso judicial, por lo que no existe controversia sobre su publicación en la Gaceta de los Tribunales.

En ***materia tributaria,*** el artículo 24 constitucional declara ***punible*** la revelación del monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las ***contabilidades revisadas*** a personas individuales o jurídicas, con la salvedad de los balances generales cuya publicación ordena la ley; y priva de eficacia probatoria a los documentos o informaciones obtenidas con violación de esta norma.

En los asuntos relativos al ***derecho de familia,*** los informes que rinden al Juez los Trabajadores Sociales adscritos al Tribunal son de carácter confidencial, únicamente pueden conocerlos el juez, las partes y sus abogados, y no puede dárseles publicidad en

forma alguna, ni extenderse certificación o acta notarial de los mismos.

Por último, en los expedientes relativos a ***menores de edad*** la Ley de Protección Integral de la Niñez y Adolescencia contiene varias disposiciones que limitan la publicidad de las actuaciones al disponer:

a) La discreción y reserva de las actuaciones relativas a la niñez y la adolescencia amenazadas o violadas en sus derechos;

b) Celebración de audiencias en forma reservada.

Esta ley relativa a los menores de edad, al imponer reserva en el trámite del proceso, si bien no hace referencia expresa a la publicidad o reserva de la Sentencia, por el espíritu de la misma que tiende a la protección del menor, implica reserva en su publicación, debiéndose suprimir el nombre del sindicado, así como los demás datos que permitan su identificación, lo cual está acorde a lo dispuesto en el Pacto de Derechos Civiles y Políticos.

-IV-

Con el desarrollo moderno de la tecnología, que permite una comunicación más ágil y en forma masiva, trae consigo ventajas y desventajas en el campo jurídico. En Guatemala, específicamente, la Internet, no se encuentra regulada por normas jurídicas de carácter nacional, lo que acarrea problemas de diversa índole a sus usuarios, tales como el uso y la regulación de la diversa información que allí se encuentra, así como la protección de la privacidad y datos personales, para que éstos no puedan ser usados indebidamente, por lo que es de suma importancia la emisión de normas legales que regulen esta materia, estableciendo los límites, derechos y obligaciones que conlleva.

Se señala la relación de la informática y el derecho, por dos razones: una, porque sirve a la ordenación de las relaciones sociales; y, la otra, porque últimamente han surgido empresas dedicadas a la elaboración de Registros de normas en forma magnética, lo que es de mucha utilidad, pero la difusión de la información jurídica por canales privados no siempre sirve para alcanzar la realización eficaz del principio de publicidad del derecho y la justicia, en un Estado Constitucional.

En Guatemala, el Organismo Judicial a través del CENTRO NACIONAL DE ANÁLISIS Y DOCUMENTACIÓN JUDICIAL –CENADOJ- cuenta con un Registro General, debidamente informatizado, dirigido a poner en conocimiento de todos los ciudadanos y de las personas interesadas en general, lo relativo al Derecho, entendiendo como tal, no sólo las normas sino también su interpretación por los tribunales. A este Registro se puede acceder para tener

conocimiento de las resoluciones de la Corte Suprema de Justicia, así como de las Salas de Apelaciones (éstas últimas a partir del año 2005) y Normas emitidas desde el año 1808, que incluyen los Decretos del Congreso de la República, Acuerdos del Organismo Ejecutivo; Acuerdos del Organismo Judicial, de las Municipalidades de todo el país, de la Corte de Constitucionalidad, Tribunal Supremo Electoral, y del Procurador de los Derechos Humanos; Resoluciones de entes descentralizados autónomos y semiautónomos, como la Superintendencia de Comunicaciones, Superintendencia de Administración Tributaria, Junta Monetaria, Comisión Nacional de Energía Eléctrica, Ministerio Público y otras entidades legalmente facultadas para emitir normas de observancia general, debidamente relacionadas con las normas que las modifican, amplían o derogan.

Toda esa divulgación normativa aunada a la publicación de los fallos de la Corte Suprema de Justicia y las Salas de las Cortes de Apelaciones, indudablemente coadyuva a obtener igualdad, unidad y seguridad en la aplicación e interpretación del derecho. ✧

Sobre el Autor:

El Lic. Guillermo Corzo es Jefe de Legislación y Jurisprudencia del Centro Nacional de Análisis y Documentación Judicial - CENADOJ.
Organismo Judicial, Guatemala, C. A.

El acceso a las fuentes de información y el respeto a la dignidad y privacidad en la legislación del Paraguay

Miguel Ángel Vargas Díaz*

Con este trabajo pretendo justificar la reglamentación que hace la ley paraguaya acerca de la protección de la dignidad y privacidad de las personas físicas con relación al tratamiento de los datos de carácter personal, susceptibles de configurar su perfil.

Índice

Desarrollo

1.- Introducción.

Los derechos a la dignidad y a la privacidad, como derechos humanos fundamentales, están expresamente reconocidos en la gran mayoría de las Constituciones y en las Convenciones Internacionales sobre Derechos Humanos. En este contexto es y ha sido una constante preocupación la protección de los datos personales aunque, como bien lo expresa Salvador Darío Bergel, la expresión es de un contenido equívoco, pues en realidad todos los esfuerzos relativos apuntan a la protección del individuo[1].

Pero con prescindencia de esta divergencia, cuadra poner de manifiesto que si bien esta protección se ha materializado a través de convenios internacionales y de leyes dictadas en su consecuencia, hasta hoy día el problema de cómo armonizar el acceso a esa

[1] *El habeas data instrumento protector de la privacidad*. En Revista de Derecho Privado y Comunitario, t. 7, Rubinzal-Culzoni, Santa Fe, Argentina. 1994.

información con el respeto a la dignidad y privacidad de las personas sigue sin resolverse definitivamente. En el Paraguay, al igual que en muchos países de la región, la gran mayoría de la población no ha llegado todavía a advertir la dimensión y trascendencia del vertiginoso avance de las tecnologías que permite a instituciones y personas públicas y privadas contar con enormes volúmenes de información. Esto hace necesario un marco normativo cuyo cumplimiento garantice el uso racional de esos datos personales, de modo tal que permita compatibilizar el desarrollo informático y las necesidades sociales con el respeto a los derechos y libertades de las personas que se encuentran reconocidos por la Constitución como derechos humanos fundamentales.

Hasta hoy día el problema de cómo armonizar el acceso a la información con el respeto a la dignidad y privacidad de las personas sigue sin resolverse definitivamente

El objetivo específico de este trabajo es analizar ciertos problemas conceptuales que involucran a los derechos que se encuentran protegidos, y con estas ideas preliminares, reseñar como se ha venido desarrollando en el Paraguay el proceso de consolidación de la legislación que protege los datos de los individuos ante el abuso en el manejo de la información de carácter privado.

2.- Antecedentes.

Antes de discurrir acerca de la importancia, el objeto y la finalidad principal de la legislación paraguaya sobre la información de carácter privado y la protección de datos de carácter personal, resulta ineludible formular algunas referencias acerca de su antecedente más inmediato que es, sin duda alguna, la Constitución de la República, sancionada en el mes junio del año 1992. Todo esto, sin ignorar desde luego, la alta significación que representó para la materia la aprobación de la Convención Interamericana de Derechos Humanos, también conocida como "*Pacto de San José de Costa Rica*", aprobada y ratificada por ley del Congreso en el año 1989.

Con mayor especificidad, los esfuerzos destinados a la creación de un sistema que garantice la protección del individuo en lo concerniente a la información de carácter privado datan del año 1992. En efecto, la Constitución de la República del Paraguay ha

adoptado como forma de gobierno la democracia representativa, participativa y pluralista, fundada en el reconocimiento de la dignidad humana (art. 1º). La afirmación del reconocimiento de la dignidad de toda persona como basamento de la República reconoce a su vez una variada gama de derechos que la tutelan, y en este orden de ideas se garantiza la protección de la *intimidad*, de la *dignidad* y de la *imagen privada* de las personas (art. 33). De acuerdo con este elenco de derechos, la Constitución del Paraguay previene que la conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, estará exenta de la autoridad pública (art. 33), y al igual que la mayoría de las Constituciones contemporáneas, establece la inviolabilidad de todo recinto privado (art. 34).

Con referencia al derecho a informarse y al libre acceso a las fuentes de información pública, la Constitución, luego de reconocer el derecho de toda persona a recibir información veraz, responsable y ecuánime, establece que dichas fuentes son libres para todos, y con la mira puesta en su entera operatividad encomienda a la legislación ordinaria el deber de reglamentar las modalidades, los plazos, y las sanciones correspondientes a las mismas. Impone a la vez al Poder Legislativo que asegure, en igualdad de oportunidades, el libre acceso al aprovechamiento del campo electromagnético, así como a los documentos electrónicos de acumulación y procesamiento de información pública, sin más limitaciones que las regulaciones internacionales y las normas técnicas (art.30).

Con este panorama, ya no resultaba suficiente que a los individuos se les reconociera su derecho al acceso a la información y a los datos que sobre si mismos, o sobre sus bienes, obraren en los bancos o bases de datos de acceso público, como el derecho a conocer el uso que se haga de ellos. Era necesario dar un paso más,

El legislador paraguayo pretende proteger solamente aquellos datos que contribuyen a configurar el perfil de un sujeto o los que pueden causar un perjuicio a su privacidad

de manera de establecer la prohibición de su recolección. Por lo tanto, el campo estaba abierto al cambio.

3.- La legislación paraguaya que

reglamenta la información de carácter privado. Objetivo.

En el año 2001 quedó sancionada la Ley Nº 1682 que "***Reglamenta la información de carácter privado***", la cual un año después fue modificada a través de la Ley Nº 1969/02. La finalidad principal de estos cuerpos normativos es regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares.

La legislación en análisis no define que debe entenderse por "*medio técnico de tratamiento*" ni por "*tratamiento de datos*", cuestión ésta que ha generado más de una polémica. Sin embargo, y en la medida que la legislación del Paraguay protege la información de carácter privado que pueda ser captada y tratada adecuadamente por cualquier forma que el ingenio humano pueda concebir, creo plenamente factible acudir a la legislación española, la que considera como tales a las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias

Retomando el punto de partida, habrá de advertirse que el objetivo de la ley es proteger, en lo que concierne al tratamiento de los datos personales, los derechos fundamentales de las personas físicas, y especialmente su dignidad y privacidad. Ana Isabel Herrán Ortiz afirma que a través de la configuración de estos principios de protección de datos, el legislador intenta conformar un sistema preventivo de tutela de la persona frente al tratamiento de la información que le atañe, estableciendo un recto equilibrio entre la sociedad de la información y las libertades de los ciudadanos[2].

No obstante, debe prevenirse que el derecho a la protección de datos tiene un objeto más amplio que el del derecho a la intimidad o privacidad, como bien lo ha puesto de manifiesto el Tribunal Constitucional español por medio de la STC 292/2000, de 30 de noviembre de 2000.

4.- Datos especialmente protegidos.

La legislación paraguaya, como regla general, consagra una limitación genérica en lo que guarda relación con el alcance de su aplicación al disponer que en ningún caso

[2] Los principios de la protección de datos en la nueva ley orgánica 15/99.

será aplicable a las bases de datos y a las fuentes de informaciones periodísticas, como tampoco a la libertad de emitir opinión y de informar. Con ello, indudablemente, queda precautelado el derecho constitucional a la libertad de expresión y de prensa.

Se desgaja de la legislación en análisis que no todo dato se encuentra protegido, ya que por un lado autoriza a todas las personas a recolectar, almacenar y procesar datos personales para uso estrictamente privado, y por otro, en su art. 3º establece que es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, siempre que en las publicaciones no se individualicen las personas o entidades investigadas y que se realicen con fines:

a) científicos,
b) estadísticos,
c) de encuestas y sondeos de la opinión pública, y
d) de estudio de mercados.

Desde esta perspectiva, parecería que el legislador paraguayo pretende proteger solamente aquellos datos que contribuyen a configurar el perfil de un sujeto o los que pueden causar un perjuicio a su privacidad. Al respecto, el art. 4º de la ley delimita la esfera sobre la cual se debe operar, ya que en él se recogen los *datos especialmente protegidos*, entre los que se cuentan los denominados *datos sensibles* de personas que estén explícitamente individualizadas o sean individualizables. Este concepto desde luego compromete a definir, o por lo menos a tratar de clarificar, lo que habrá de entenderse por datos sensibles, y brindar aunque sea una breve idea acerca de qué debe entenderse por personas individualizables y por privacidad.

A través de una esclarecida expresión de Giannantonio[3] dentro de la categoría genérica "datos personales" existen datos que tienen una particular capacidad de afectar la privacidad de los individuos o de incidir en conductas discriminatorias, y son precisamente éstos los que han sido calificados por la doctrina como "datos sensibles". La misma ley paraguaya enumera una categoría de ellos, y son los referentes a:

a) pertenencias raciales o étnicas;
b) las preferencias políticas;
c) la información relativa a la salud de la persona interesada;
d) las convicciones religiosas, filosóficas o morales;
e) la intimidad sexual; y
f) en general, los que fomenten prejuicios y discriminaciones, o afecten la dignidad, y la privacidad de las personas.

[3] *Manuale de Diritto dell´informatica*, Padova, 1994, p. 75.

Fijada brevemente la idea acerca de lo que debe entenderse por datos sensibles, le cabe el turno a la privacidad. Una idea preliminar para ver que significa esta voz, ya que su estudio detenido excede el marco de lo que aquí se ha propuesto, puede parecer lógica, aunque no suficiente. La nueva edición del diccionario normativo, recientemente publicada por la Real Academia Española ha admitido la palabra privacidad con el significado de *ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión*. De ahí que el derecho constitucional a la intimidad tenga como función la de proteger a la persona frente a cualquier irrupción que pueda realizarse en la esfera de su vida personal y familiar que ésta desea excluir del conocimiento ajeno y de las intrusiones de terceros contra su voluntad. Finalmente, con relación a las expresiones *personas individualizables o identificables,* debe entenderse naturalmente a aquellas personas que puedan ser fácilmente identificadas, es decir que para ello no se requieran métodos complejos.

límites con el fin de resguardar otros derechos o bienes constitucionalmente protegidos, ese límite debe ser siempre necesario, proporcionado y respetuoso con el contenido esencial del derecho a la dignidad y a la privacidad. De acuerdo con el art. 6º, están fuera del alcance de la protección prevista por el legislador, y por tanto está autorizada la aplicación y difusión de:

En el Paraguay goza de jerarquía constitucional la protección de datos privados, procurando garantizar el respeto de la dignidad y la privacidad de las personas

5. Limitaciones y excepciones.

La legislación en análisis establece ciertas limitaciones y excepciones al ejercicio del derecho de protección de los datos personales, los deberían ser interpretados y aplicados con criterio restrictivo, pues si bien el derecho a la intimidad no es absoluto y la ley puede asignarle

a) los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional;

b) siempre que se trate de datos solicitados por el propio afectado[4]; y

c) siempre que la información sea recabada en el ejercicio de sus funciones por magistrados judiciales, fiscales, comisiones parla mentarias o por otras autoridades legalmente facultadas para ese efecto.

En similar sentido, el art. 5º establece que los datos de las personas físicas o jurídicas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales y financieras, podrán ser publicados o difundidos solamente: cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente; o cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimiento de disposiciones legales específicas; o, cuando consten en las fuentes públicas de información.

6. El habeas data.

Si bien no es un propósito de este trabajo realizar el desarrollo teórico acera de la relación entre derechos y garantías, es sabido que el concepto de garantías luego de una evolución significativa en nuestro medio vino a ser considerado, desde una perspectiva reiteradamente asumida, como el instrumento que sirve para proteger, asegurar, o hacer valer la titularidad o el ejercicio de un derecho[5], ya que en su orígenes se hablaba de ellas como sinónimo de derecho. La Constitución paraguaya del año 1992 ha dedicado a las garantías constitucionales su Capítulo XII, del Título II de la Parte I, bajo el acápite especifico "*De las garantías constitucionales*", usando la expresión en el sentido de procedimientos especiales destinados a la defensa de derechos constitucionales y, excepcionalmente, también legales (caso del amparo), y termina consagrando de manera expresa cuatro garantías constitucionales: la inconstitucionalidad, el hábeas corpus, el

[4] Entiendo que esto debe interpretarse como el acuerdo libre, expreso, y escrito del interesado. Vale de todos modos una palabras para el tópico convocante, las que cuentan con mi adhesión: En una de sus exposiciones, Giannantonio de forma tajante habla del "mito del consenso", señalando que el consenso es insuficiente, y que una normativa basada en la solicitud de recolección y divulgación de la información sobre el consentimiento del interesado constituye la aceptación de la disparidad del poder existente y concreto, y por lo tanto implica una forma de legitimación del arbitrio del más fuerte; (ob. cit. p.27)

[5] cfr. Opinión Consultiva N° 8 CIDH.

amparo y el habeas data[6]. La Constitución no deja dudas sobre el sentido en que usa tal expresión al establecer su finalidad, en el art. 131, donde precisamente bajo el epígrafe "*De las garantías*", señala que para hacer efectivos los derechos consagrados en ella se establecen las garantías contenidas en dicho capítulo.

De todas ellas, el Habeas Data viene a constituir el instrumento adecuado para la protección de la privacidad e intimidad personal frente al desmedido avance de las tecnologías de la información. El objeto concreto de ésta garantía está definida en el art. 135 de la Constitución donde se establece que toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad.

La misma disposición constitucional implícitamente reglamenta el procedimiento a seguir fijando dos momentos diferentes. El primero, el ejercicio del derecho de acceso al banco o base de datos para conocer la información almacenada. En el segundo momento, el magistrado, luego de verificada la información, debe ordenar la actualización, rectificación o la destrucción de aquellos datos, si fuesen erróneos o afectaren ilegítimamente sus derechos.-

7.- Conclusión.

Las ideas aquí expuestas, en su mayoría tratan de cuestiones ya exploradas, ya inventariadas, y que si bien no son originales pueden servir para describir el panorama legislativo paraguayo referente a la protección de la dignidad y privacidad de las personas físicas con relación al tratamiento de los datos de carácter personal.

Quedo puesto de manifiesto que en el Paraguay goza de jerarquía constitucional la protección de datos privados, procurando garantizar el respeto de la dignidad y la privacidad de las personas, y asimismo que dichos disposiciones constitucionales se encuentran reglamentadas por leyes de rango inferior, y que se cuenta con un instrumento eficaz para su defensa como le es el habeas data ✧

El Abogado Miguel Ángel Vargas Díaz es Juez de Primera Instancia en lo Civil y Comercial de Encarnación, Paraguay, Profesor de Filosofía del Derecho en la Universidad Nacional de Itapúa, Especialista en Derecho Procesal Civil por la Universidad Nacional del Nordeste, Corrientes, República Argentina.

[6] Mendonca, Juan Carlos; *La Garantía de Inconstitucionalidad,* Liticolor, Asunción, 2000, p.12-13.

BIBLIOGRAFÍA

1.- *Revista de Derecho Privado y Comunitario*, t. 7, Rubinzal-Culzoni, Santa Fe, Argentina. 1994.

2.- Giannantonio, Ettore; *Manuale de Diritto dell´informatica,* Padova, 1994

3.- Mendonca, Juan Carlos; *La Garantía de Inconstitucionalidad,* Liticolor, Asunción, 2000.

4.- Herrán Ortiz, Ana Isabel; *Los principios de la protección de datos en la nueva ley orgánica 15/99*

5.- Frosini, Vittorio; *La protección de la intimidad: de la informática al bien jurídico informático, en Derecho y Tecnología informática*, Nº 3, Bogotá, 1990, p. 19.

6.- Sagues, Néstor, *Mundo jurídico y mundo privado*, J.A., 29 1975.

A Protecção dos Dados Pessoais no âmbito da celebração dos contratos de seguros

Drª Ana Luísa Geraldes *

Como se realiza a recolha e tratamento de dados pessoais pelas seguradoras - O tratamento indevido de dados pessoais de natureza sensível, v.g., os dados de saúde - Como deve ser prestado o consentimento - Alguns exemplos de práticas abusivas, nesta matéria, em Portugal

A bordagem da temática no âmbito da celebração dos contratos de seguros:

1. A recolha e tipo de dados:

1.1. É sabido que aquando da celebração do contrato de seguro as seguradoras solicitam ao segurado que proceda ao preenchimento de um formulário com os dados que consideram mais relevantes do ponto de vista económico e empresarial por parte das Companhias de Seguro, tendo em conta o objecto e a finalidade do contrato a celebrar.

Nesses impressos ou formulários são os cidadãos contraentes *convidados* a preencher múltiplas quadrículas, com itens diversos, tendentes a recolher dados pessoais do respectivo segurado.

Entre esses elementos, figuram na recolha os dados pessoais de identificação do segurado e, a par destes, outros dados que as seguradoras consideram necessários tendo em vista a cobertura do risco e que se prendem com o tipo de seguro a celebrar - seguro automóvel, seguro vida - bem como outros elementos que qualificam de essenciais para a avaliação e apreciação do respectivo risco. E que terão igual repercussão no montante do prémio a cobrar pela celebração do respectivo contrato de seguro.

São, assim, coligidas pela seguradora, informações que visam, numa primeira fase, *calcular o montante do prémio* a cobrar ao segurado e, numa fase posterior, após a ocorrência do sinistro, *aferir em concreto da existência de factores que lhes permitam, se possível, eximirem-se* do respectivo pagamento ou pagarem o mínimo possível ao segurado.

Destarte, são recolhidos, sobretudo nos contratos de seguro de vida ou de saúde, dados relativos ao estado de saúde do segurado, com informações clínicas detalhadas a seu respeito. Chegando-se ao ponto de ser

solicitada ao segurado, de forma expressa, autorização para ser recolhida junto do seu médico assistente ou médico de família ou até dos respectivos estabelecimentos de saúde, informação clínica a seu respeito, com incidência, principalmente, nos antecedentes familiares do segurado, para além dos seus próprios antecedentes pessoais, onde se incluem perguntas aparentemente inócuas sobre os hábitos desportivos do segurado [43], e até sobre os seus hábitos de vida, formuladas nos seguintes termos:

- consome álcool ?... (quantas vezes por dia?... em que quantidade?...);

- fuma?... (quantos maços por dia?...);

- já consumiu drogas? (de que tipo?... com que idade começou?... qual a frequência?...);

Chegando ao ponto inclusivamente de querer saber, no que concerne às seguradas do sexo feminino, se estas já abortaram... (e quantas vezes?) ou se tomam contraceptivos.

Questões enquadradas num extenso rol de perguntas relativas às doenças que a pessoa já teve, *v.g.*, se já foi operada,... (quando e a quê?...), se sofre de doenças crónicas..., se toma antidepressivos..., se faz medicação e de que tipo,... etc.

Complementarmente, exigem ainda, que o segurado se submeta a todo o tipo de exames médicos.

Ora, muitos destes dados assumem a natureza jurídica de dados sensíveis, como é o caso dos dados relativos ao "consumo de drogas" ou à realização de um "aborto", e integram-se no conceito mais amplo e constitucionalmente protegido pela Constituição da República Portuguesa da "reserva da vida privada".

2. Dados sensíveis:

2.1. Com efeito, à luz da lei de protecção de dados pessoais, estamos perante dados sensíveis, porquanto a lei qualifica como tal os dados de saúde, os relativos a hábitos de vida privada, os da vida sexual e os demais dados enquadráveis no conceito de vida privada, para além daqueles dados referentes às convicções filosóficas ou políticas, à filiação partidária ou sindical ou à fé religiosa - cf., a este propósito, o art. 7°, n° 1, da Lei da Protecção de Dados Pessoais – Lei n° 67/98, de 26 de Outubro.

Destarte, e por força do preceituado na citada Lei da Protecção de Dados Pessoais, o seu tratamento só pode ocorrer se tiver sido dado o consentimento expresso pelo titular dos dados, para a finalidade específica desse tratamento e se para tal se mostrar necessário, e relevante, tendo em conta, *in concreto,* o contrato de seguro a celebrar.

[43] Estes dados não são subsumíveis no conceito de "dados sensíveis", nos termos em que a Lei Portuguesa os define, na alínea a) do artº 3º, da Lei nº 67/98, de 26 de Outubro.

Só para situações elencadas na lei da protecção de dados, como sejam, para efeitos de medicina preventiva, de diagnóstico, tratamento e prestação de cuidados de saúde, o tratamento de dados referentes à saúde e à vida sexual, incluindo os dados genéticos, é legalmente admissível, no quadro normativo do tratamento de dados sensíveis.

Nestas circunstâncias, e sempre que se trate de dados de saúde, pela sua natureza sensível, impôs o legislador que a sua recolha e tratamento carece obrigatoriamente de autorização da CNPD, ou seja, da Comissão Nacional de Protecção de Dados Pessoais, autoridade nacional portuguesa a quem compete autorizar e registar os tratamentos de dados pessoais, bem como controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais, exercendo o seu controlo prévio - cf. art. 28°, n° 1, al. a), e 22º, ambos da Lei n° 67/98.

Contudo, é permitido, à face da lei portuguesa de protecção de dados pessoais, que, no decurso dos contratos de seguros de saúde, as entidades prestadoras de cuidados de saúde possam tratar esses dados sem necessidade de consentimento, se se verificarem os requisitos legais estabelecidos no art. 7°, n° 4, da Lei n° 67/98.

Ou seja: sempre que o tratamento desses dados for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos, e desde que o seu tratamento seja efectuado por um profissional de saúde, obrigado a sigilo ou por outra pessoa sujeita a segredo profissional, e sejam implementadas e garantidas medidas adequadas de segurança da informação, que abarca o controlo dos suportes de dados, o controlo da sua utilização, bem como os controles de introdução, de acesso, e de transmissão. [44]

Quanto a esta matéria entendemos porém que, no âmbito do cumprimento do contrato de seguro, a única forma cabal de assegurar a defesa da privacidade do titular dos respectivos dados pessoais passa por só se permitir que sejam tratados os dados de saúde que se mostrem estritamente necessários e imprescindíveis ao seu legal cumprimento e que apresentem relevância e conexão com a natureza do contrato de seguro outorgado, *v.g., o registo de incapacidade do lesado, a sua percentagem de incapacidade, a natureza da lesão, a localização do dano corporal,...*

E o legislador deveria ter tido a preocupação de consagrar expressamente, na legislação nacional portuguesa, um regime desta natureza em matéria de tratamento de dados

[44] Cf. sobre esta matéria o artº 15º da Lei nº 67/98, de 26 de Outubro.

pessoais no âmbito da celebração dos contratos de seguro, estipulando limites claros às seguradores, de molde a evitar distorções e violações aos direitos dos titulares dos dados pessoais na recolha e tratamento dos mesmos.

Aliás, tem sido este o caminho seguido por alguns ordenamentos jurídicos Europeus.

2.2. A este propósito, cita-se, por exemplo, a própria Bélgica, que, na legislação que regula os contratos de seguros, estabeleceu regras legais que apontam no sentido atrás pugnado, impedindo que as seguradoras recolham e tratem dados relativos à saúde dos segurados que não se mostrem necessários nem tenham qualquer conexão com o seguro que se pretende contratar.

Neste sentido pode ler-se, no art. 95°, da Lei de 25 de Junho de 1992, na redacção que lhe foi introduzida pelo art. 19° da Lei n° 3.341, de 22 de Agosto de 2002, o seguinte:

"O médico escolhido pelo segurado pode remeter os certificados médicos necessários à conclusão ou execução do contrato. Mas estes certificados limitam-se a uma descrição do estado de saúde actual (do segurado) ".

"Estes certificados não podem ser remetidos senão ao médico da seguradora...

"O exame médico necessário à conclusão e à execução do contrato, não pode ser fundado a não ser nos antecedentes determinantes do estado de saúde actual do segurado e não sobre técnicas de análise genéticas próprias para determinar o seu estado de saúde futuro". [45]

"Desde que a seguradora justifique com o acordo anterior do segurado, o médico deste transmite ao médico da seguradora um certificado estabelecendo a causa da morte".

Também a CNIL [46] defende, nesta matéria, o entendimento de que deve ser o segurado a comunicar ao seu médico as indicações relativas ao seu estado de saúde e que são pedidas no contrato de seguro, nomeadamente as causas de exclusão, tal como os critérios de apreciação médica definidos pela companhia de seguros, de modo a que o seu médico não comunique ao médico da seguradora mais do que um certificado médico adaptado, *indicando se o caso de doença do segurado releva ou não para as causas de exclusão do contrato de seguro.* [47]

3. O consentimento:

[45] Sublinhado nosso.

[46] Commission Nationale de L'Informatique et des Libertés (Francesa).

[47] 10 Cf. as comunicações da CNIL dirigidas aos profissionais de saúde, pág. 16.

3.1. Para obstar às proibições legais constatamos que a maior parte das vezes as companhias seguradoras procuram obter dos segurados, previamente, o seu consentimento expresso, através da assinatura de uma "declaração" anexa à apólice e que posteriormente exibem.

Porém, esse consentimento só deve ser considerado válido, para efeitos de permitir a recolha desses dados, se obedecer aos requisitos legais inseridos na Lei de Protecção de Dados Pessoais: ou seja: se se tratar de um consentimento prévio, livre, expresso e esclarecido.

Entendendo-se como tal, em termos normativos, qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objecto de tratamento - art. 3°, al. h), da Lei n° 67/98.

Exige-se, portanto, para que o consentimento revista tais pressupostos, que:

a) ao segurado seja prestada informação concreta;

b) que o seu consentimento seja expresso, livre e informado.

Não podendo consistir num mero consentimento genérico, só deve ser considerado lícito o tratamento e recolha dos dados pessoais, quando tiver sido fornecida e assegurada ao titular dos dados uma informação clara e completa sobre as finalidades do tratamento, esclarecendo-o sobre o objectivo que presidiu à recolha de elementos de natureza privada e tão sensível.

3.2. Esse dever legal de informação já resulta de um outro diploma legal que, em Portugal, regula as cláusulas contratuais gerais (cláusulas que integram por natureza os contratos de seguro, estando inseridas abundantemente nas respectivas apólices), no qual se consagra que o contratante (como por exemplo, a seguradora), que recorra a cláusulas desta natureza, *tem o dever de prestar a devida informação ao segurado* - cf. art. 6° do Decreto-Lei n° 446/85, de 25 de Outubro, com as alterações subsequentes. [48] Estatuindo-se, como regra, no que concerne *à integração ou existência no contrato de cláusulas ambíguas,* o princípio de que, na dúvida, prevalece o sentido mais favorável ao aderente - cf. o n° 2 do seu art. 11º do diploma legal citado.

3.3. Na matéria da protecção de dados pessoais, também a Comissão Nacional de Protecção de Dados Pessoais – CNPD – autoridade nacional portuguesa, tem, por natureza, um papel importante a desempenhar na defesa dos direitos e garantias

[48] Dever esse que engloba a prestação, de acordo com as circunstâncias, de informar a outra parte dos aspectos compreendidos nas cláusulas e cuja aclaração se justifique.

fundamentais dos cidadãos, por forma a garantir que o tratamento de dados pessoais se efective com o absoluto respeito pela reserva da vida privada do titular dos respectivos dados pessoais, direito este constitucionalmente consagrado - cf. art.º 26º da Constituição da República Portuguesa.

Cabe a tal entidade verificar a legal utilização dos dados pessoais recolhidos e o seu tratamento, podendo, de acordo com a lei, nos casos de incumprimento ou violação das regras legais impostas, sancionar o infractor através de procedimentos de natureza contra-ordenacional.

4. Os princípios da adequação, da necessidade e da pertinência:

4.1. Em termos de autorização de recolha e tratamento de dados pessoais um dos princípios fundamentais a observar radica em aferir, em função do caso concreto, se os dados que a seguradora pretende recolher e tratar obedecem aos princípios da adequação, da necessidade e da pertinência. Isto é: se se mostram necessários, pertinentes e adequados à prossecução da finalidade a atingir e se estão relacionados com a actividade desenvolvida pela seguradora: a de celebração e gestão de contratos de seguro.

É de considerar que observam tais princípios, preservando o fim a que se destinam, apenas os dados pessoais que se mostrarem necessários para a celebração do respectivo contrato, tendo em conta a apreciação do risco, o objecto do contrato, a fixação das condições contratuais e a prestação de serviços decorrentes do contrato a celebrar.

Constatamos porém que, nesta matéria, da aferição em concreto dos referidos princípios da adequação, da necessidade e da pertinência, nem sempre tem sido fácil observar tais regras.

4.2. Assiste-se, também, em certo tipo de contratos de seguro, como nos contratos de seguro vida, celebrados na sequência de pedidos de empréstimo bancário efectuados por particulares para a compra de habitação, que os dados pessoais do segurado acabam por ser cedidos a outras entidades, a terceiros, normalmente entidades pertencentes ao mesmo Grupo a que pertence o Banco que concede o respectivo empréstimo, e que estão vocacionadas para gerir as informações sobre as carteiras e contratos de seguro dos clientes. [49] Estabelece-se, assim, uma troca recíproca de informações entre as entidades bancárias e as seguradoras pertencentes ao mesmo Grupo.

A questão que se pode suscitar é a de saber como, em tais circunstâncias, se podem compatibilizar, por um lado, os interesses das seguradoras em obter e ter na sua posse essas informações e, por outro, o dos segurados, de não divulgação dos seus dados pessoais de natureza sensível, *v.g.,* os dados de saúde, e como preservar a sua confidencialidade.

Tais situações são frequentes quando, por exemplo, se solicita crédito a um Banco para a compra de casa e, antes da concessão do referido empréstimo, as entidades bancárias exigem ao seu cliente a celebração de um seguro de vida, pedindo, para o formalizar, que procedam ao preenchimento de um formulário que integra um leque variado de questões, cuja maioria incide, conforme já se referiu, sobre os seus hábitos de vida e antecedentes familiares, tendo ainda que responder a um questionário extenso e minucioso sobre os seus dados de saúde.

Para além das dificuldades que o teor de certas perguntas suscita e da invasão que tal significa quanto à privacidade do titular dos dados pessoais, constata-se ainda que, em Portugal, constitui prática neste domínio, proceder à entrega dos respectivos formulários directamente ao próprio empregado da agência bancária que, por sua vez, tem a seu cargo efectuar o atendimento e tratar, no Banco, da parte burocrática e administrativa conducente à concretização do respectivo empréstimo ao cliente bancário.

Ora, afigura-se-nos que tal prática deveria ser banida por violadora do direito constitucional de reserva da vida privada, porquanto permite, por esta via, o conhecimento de dados pessoais mais íntimos e que são, por natureza, dados pessoais sensíveis.

Embora as entidades bancárias estejam sujeitas, relativamente a elementos do exercício da sua actividade, à observância do sigilo bancário, tal facto não parece ser

[49] Os Bancos estão autorizados legalmente, por essa via, a comercializar contratos de seguros - cf., a este propósito, o art. 4°, al. n), do Decreto-Lei n° 298/92.

suficiente para que, a coberto de um empréstimo, se permita o acesso a esses dados às respectivas seguradoras, e afigura-se-nos que esse acesso só deve ser facultado se o titular dos dados pessoais prestar, também aqui, expressa e objectivamente, para esse preciso efeito, o seu consentimento prévio.

Devendo igualmente impedir-se que a própria seguradora possa utilizar os dados recolhidos junto dos Bancos para efeitos de realização de acções de *marketing* dos seus produtos, a não ser que tenha obtido previamente o consentimento expresso e informado do titular dos dados, bem como a respectiva autorização por parte da autoridade nacional de protecção de dados pessoais, nos termos do disposto no art.º 28°, n° 1, al. d), da Lei n° 67/98, de 26 de Outubro.

5. Em Conclusão:

1. A Constituição da República Portuguesa e a Lei da Protecção de Dados Pessoais impõem o respeito pela reserva da vida privada enquanto direito fundamental e, como tal, deve ser preservado, impedindo-se o acesso de estranhos a informação e dados pessoais sobre a vida privada e familiar de outrem, bem como a divulgação de tal informação.
2. Estando em causa o acesso, por parte de seguradora, a dados pessoais de natureza sensível – dados relativos à saúde e à vida sexual, incluindo os dados genéticos -, não pode deixar de se ter em consideração que os mesmos se inserem no âmbito da celebração de um contrato de seguro, contrato este de natureza formal, consensual e validamente celebrado pelas partes, onde predomina a vontade, e no qual o consentimento livre, expresso e informado dos outorgantes deve produzir os seus efeitos jurídicos.

3. Impõe, assim, que resulte das cláusulas do contrato de seguro - constituída pelas condições gerais e especiais da apólice, que fazem parte integrante do respectivo contrato de seguro - que o segurado autorize a seguradora a ter acesso aos seus elementos médicos, *v.g.,* nos contratos de seguro do ramo vida, os dados pessoais que fornecem informações médicas sobre as causas da sua morte, doença ou lesão.

4. Para esse efeito é exigível o *"consentimento expresso e informado* " imposto pelo art.º 7°, n.° 2, e alínea h) do artº 3º, ambos da Lei da Protecção de Dados Pessoais, Lei n.° 67/98, de 26 de Outubro, e só o consentimento prévio, livre e específico, com essas características, legitima o acesso, recolha e tratamento dos dados de saúde do segurado por parte da respectiva seguradora ✧

Ana Luísa Geraldes. Juíza Desembargadora do Tribunal da Relação de Lisboa.

Protección de Datos Personales
En la República Dominicana

Hermógenes Acosta de los Santos*

SUMARIO

El reconocimiento del derecho a la intimidad y a mantener en el ámbito privado determinadas informaciones tiene su origen en el derecho anglosajón. No obstante, en la actualidad dicho reconocimiento es casi universal, toda vez

que la protección de los denominados datos personales, aparece en los tratados internacionales de mayor relevancia y trascendencia. Además, muchos países cuentan con leyes que reglamentan de manera general la protección de datos personales; mientras que otros, si bien no cuentan con una reglamentación general sobre la materia, tienen leyes especiales en determinadas áreas, las cuales tratan el tema. La República Dominicana se encuentra entre estos últimos países, es decir, que nuestro país carece de una normativa general sobre la materia.

En efecto, en el ordenamiento jurídico dominicano no existe una ley que regule la protección de datos personales de manera general. Sin embargo, por una parte, en la Constitución dominicana aparece una protección a dichos datos, y por otra parte, varias leyes especiales se refieren a la materia tratada, particularmente nos referimos al artículo 337 del Código Penal, modificado por la ley 24-97, la ley No.55-93, sobre el síndrome de inmunodeficiencia adquirida, (SIDA), del 31 de diciembre de 1993, ley No. 153-98 sobre telecomunicaciones, del 27 de mayo del año 1998, ley No.200-04, sobre libre acceso a la información pública, del 28 de julio del 2004 ,ley No.288-05, sobre regulación de las sociedades de información crediticia de protección al titular de la información. De igual forma, es procedente mencionar, tanto la resolución No. 36-00, dictada por el Consejo Directivo del Instituto Dominicano de las Telecomunicaciones, (INDOTEL) del 19 de diciembre del 2000, que sanciona la interceptación ilegal de telecomunicaciones; así como la resolución dictada por la Suprema Corte de Justicia el 13 de noviembre del 2003, que establece el procedimiento a seguir en las interceptaciones telefónicas.

La inexistencia de una legislación general sobre la materia dificulta la protección de los datos personales, así como la de los derechos que se derivan de dicha protección, es decir, el derecho de confidencialidad, de rectificación, de corrección, de acceso y el derecho de cancelación.

El éxito en la eficacia de la los derechos derivados de la protección de los datos personales dependerá, esencialmente, de las garantías procesales que se establezcan, así como de la severidad de las sanciones que se contemplen.

En el presente trabajo nos circunscribimos a comentar y a reflexionar en torno a la normativa relativa a la protección de los datos personales que en la actualidad existen en el ordenamiento jurídico dominicano. Para el logro de tales objetivos hemos dividido este artículo en dos partes. En la primera parte comentamos las diferentes leyes y resoluciones sobre la materia y en la segunda parte nos referimos a las vías legales o

mecanismo mediante los cuales se garantiza la eficacia de los derechos que nos ocupan.

I. Leyes y Resoluciones que protegen los datos personales

1.Constitución de la República Dominicana

Entre los derechos individuales y sociales contemplados en la Constitución dominicana se encuentra: "La inviolabilidad de la correspondencia y demás documentos privados, los cuales no podrán ser ocupados ni registrados sino mediante procedimientos legales en la substanciación de asuntos que ventilen en la justicia. Es igualmente inviolable el secreto de la comunicación telegráfica, telefónica y cablegráfica".(art. 8.9)

La expresión "correspondencia y demás documentos privados, utilizada por el constituyente, encierra una protección amplísima, de tal suerte que puede afirmarse que mediante el referido texto se salvaguardan los dato personales en general o los datos vinculados a la vida privada de una persona física contenido . Mientras que al establecerse "Es igualmente inviolable el secreto de la comunicación telegráfica, telefónica y cablegráfica", quedan también protegidos los datos personales que puedan ser manejados a través de los mecanismos que modernamente se utilizan para la transmisión de datos.

2. Ley No.55-93, sobre el Síndrome de Inmunodeficiencia Adquirida (SIDA), del 31 de diciembre de 1993

El artículo 3 letra "a" de dicha ley establece que no debe realizarse el diagnóstico de infección por VIH "a" "Para fines laborales, como requisito de ingreso a un trabajo o como condición para la permanencia en el empleo". Mientras que el artículo 22 establece que "Los trabajadores o empleados seropositivos al VIH no están obligados a informar a sus empleadores sobre su condición serológica".

Al prohibirse al empleador requerir exámenes de laboratorios orientados a determinar si el empleado o candidato a empleado padece del VIH, así como el hecho de que el empleado no tenga la obligación de informar al empleador su condición de seropositivo, constituye un reconocimiento del derecho a mantener en secreto informaciones atinentes a la vida privada de una persona, en la especie cuestione que tienen que ver con la salud.

3. Ley No.200-04, sobre libre acceso a la información pública, del 28 de julio del 2004

Con esta ley se persigue crear un mecanismo que les permita a los ciudadanos estar

informado sobre los actos del gobierno, de manera tal que puedan analizarlos y juzgarlos en forma completa, en el entendido de que con ello se garantiza la transparencia y el fortalecimiento de la democracia.

No obstante el interés del legislador en garantizar el derecho de acceso a la información de los ciudadanos, no dejó de lado la protección de la vida privada de terceros que eventualmente pueden verse afectados en ocasión del ejercicio del referido derecho a la información. Puede afirmarse que estamos en presencia de una ley que garantiza la coexistencia del derecho de acceso a la información con el derecho a la protección de la vida privada de las personas físicas.

En efecto, en el artículo 2 de la referida ley se condiciona el derecho de acceso a la información a que no se afecte: "...el derecho a la privacidad e intimidad de un tercero o el derecho a la reputación de los demás...". La protección al derecho de la vida privada aparece también en el artículo 17, texto que establece de manera taxativa las limitaciones al derecho de acceso a la información, entre las cuales se contempla, según consta en la letra "k" del referido texto, "la Información cuya divulgación pueda dañar o afectar el derecho a la intimidad de las personas o poner en riesgo su vida o su seguridad".

Una previsión similar aparece en el artículo 18, texto que contempla las limitaciones al derecho de acceso a la información , en razón de "intereses privados preponderantes". El legislador entiende que existe un interés privado preponderante: "Cuando se trate de datos personales cuya publicidad pudiera significar una invasión de la privacidad de las personas...". Cabe, sin embargo, destacar, que en el mismo texto se establece que la administración pública podría permitir el acceso a la información, aunque ello implique una invasión a la privacidad de las personas, si quien solicita los datos: "...logra demostrar que esta información es de interés público y que coadyuvará a la dilucidación de una investigación en curso en manos de algún otro órgano de la administración pública".

4. Ley No.288-05, sobre regulación de las sociedades de información crediticia de protección al titular de la información

a) Los principios rectores

Los principios rectores que gobiernan el funcionamiento de los burós de informaciones crediticias, aparecen en el artículo 4 de esta ley y en síntesis son los siguientes:

1. derecho de acceso y de rectificación de la persona interesada. Toda persona que demuestre su identidad tiene derecho a saber si se están procesando datos crediticios en relación a ella, así como a

obtener las rectificaciones o correcciones de lugar si dichas informaciones no se correspondieren con la realidad, todo lo cual debe permitirse a la mayor brevedad posible y sin gastos excesivos.

2. Exactitud y pertinencia de los datos suministrados. Corresponde a los aportantes de datos la obligación de ser exactos al momento de suministrar datos e igualmente tienen la obligación de sólo suministrar los datos que fueren pertinentes a las actividades que realicen. Por su parte, el buró de información crediticia tiene la obligación de comprobar si los datos suministrados son o no exactos, así como velar por la actualización periódica de los mismos.
3. Deber de reserva o confidencialidad. Las personas físicas o morales usuarias o suscriptoras del buró de información crediticia, no pueden revelar a terceros las informaciones crediticias que les fueren suministradas. No obstante, cuando se trate de autoridad competente, funcionarios públicos o privados que con motivo de los cargos que desempeñen tengan acceso a la información, desaparece tal prohibición.

b) Necesidad de autorización expresa de los titulares para ser consultados

El artículo 14 de la ley se refiere a la necesidad de que el usuario de los servicios del buró de información crediticia obtenga del titular de las informaciones crediticias autorización por escrito de éste, para poder suministrar la información y hacer uso de ella. La prueba del escrito debe mantenerse por un plazo de 6 meses, vencido éste el titular ya no puede alegar la inexistencia de la autorización. No obstante lo anterior, en caso de autorización verbal, el buró de información crediticia, puede permitir a sus clientes el acceso a la base de datos, a condición de que sea a través de un funcionario o empleado

En el ordenamiento jurídico dominicano no existe una ley que regule la protección de datos personales de manera general (…) La inexistencia de una legislación general sobre la materia dificulta la protección de los datos personales, así como la de los derechos que se derivan de dicha protección.

previamente autorizado y que haya manifestado, bajo la fe del juramento, decir la verdad; que cuente con la autorización de los consumidores en la forma que establece la ley.

Conforme al artículo 37, párrafo III, la referida autorización no es necesaria cuando la solicitud de información al buró , la formule la Superintendencia de Bancos, o las entidades públicas a las cuales se refiere esta ley, en ocasión de una investigación oficial, incluyendo narcotráfico, y combate al blanqueo de capitales, actividades antiterroristas, o por autoridades recaudadora de impuestos para fines fiscales, o la información requerida por cualquier otra institución gubernamental o de carácter oficial.

c) Información prohibidas.

Los usuarios de los servicios del buró de información crediticia, no pueden suministrar a este, según el artículo 15, entre otras, las informaciones siguientes: las que tienen que ver con las características morales o emocionales de las personas físicas, hábitos personales, estado de salud física o psíquicas, conducta o preferencia sexual.

d) Derechos de los titulares de la información.

Según el artículo 18, los titulares de la información tienen derecho a acceder a la informaciones que les conciernen, a la modificación y cancelación de las informaciones ilegales, inexactas, erróneas o caducas, a rectificación de aquellas informaciones que hayan sido difundidas por el buró de información crediticia y que resulten ilegales , inexactas, erróneas o caducas; de igual forma tienen derecho a la entrega de un reporte de su historial crediticio, en un plazo de 15 días hábiles, contados a partir de la recepción de la solicitud. Dicho reporte debe ser claro y preciso.

4.1Sanciones contempladas en la ley.

La ley que nos ocupa prevé sanciones penales y sanciones administrativas, las cuales procederemos a explicar en los párrafos que siguen.

A) Sanciones Penales:

a) Hechos que sanciona esta ley: Mediante esta ley se sanciona el hecho de que un usuario o suscriptor del buró de información crediticia acceda a la base de datos de manera fraudulenta, es decir, sin la autorización del titular de la información, dada conforme a lo previsto en el artículo 14 de esta misma ley (Art.46). Se sanciona

también el hecho de darle a la información obtenida un uso distinto al que se haya consignado en la autorización concedida por el cliente o consumidor (Art. 46 Párrafo I). De igual forma, se sanciona el hecho de que el usuario o suscriptor del buró de información crediticia suministre los datos obtenidos para la comisión de un delito o de un crimen (Art. 46 Párrafo II). Se sanciona el hecho de que una persona física consulte la base de datos de manera fraudulenta y con el uso de clave (Art. 47). Y por último la divulgación, publicación, la reproducción, la transmisión y la grabación del contenido parcial o total de parte de cualquier tipo proveniente del Buró de Informaciones Crediticias, en cualquiera de sus manifestaciones por cualquier medio de comunicación sea impreso, televisivo, radial, electrónico o cualquier otra forma de publicación." (Arts. 45 y 49).

b) Sanciones aplicables: El acceso a la base de datos sin autorización del titular es sancionado con multa de 10 salarios mínimo a 50 salarios mínimos (Art.46). Usar las informaciones obtenidas de la base de datos para fines distintos a lo consignado en la autorización dada por el cliente o consumidor se sanciona con multa de l0 salarios mínimos a 100 salarios mínimos (Art. 46 Párrafo I). La utilización de los datos obtenidos para facilitar la comisión de un delito se sanciona con prisión mínima de 6 meses y máxima de 2 años; mientras que si lo que se pretende con las informaciones es facilitar un crimen se aplican las penas previstas en el Código Penal para los cómplices (Art. 46 Párrafo II). Las personas físicas que consulten la base de datos de manera fraudulenta y con el uso de claves son sancionadas con multa de 20 salarios mínimos y un máximo de 100 salarios mínimos. Finalmente, la divulgación por cualquier medio de las informaciones provenientes de la base de datos del buró de información Crediticia se sanciona con multa de 10 salarios mínimos a 150 salarios mínimos.

B) Sanciones Administrativas:

a) Órgano encargado de aplicar las sanciones administrativas.

Corresponde aplicar las sanciones administrativas que se explicarán más adelante, a la Superintendencia de Bancos de la República Dominicana (Art.50)

b) Se consideran como infracciones administrativas las siguientes:

"51.1.- Incluir en los Reportes de Crédito cualesquiera de las informaciones prohibidas de los BICs, desglosadas en la presente Ley; 51.2- Negarse a facilitar el acceso a la información crediticia al titular de la misma; 51.3.- Denegar, sin fundamento, una solicitud de revisión o una solicitud de rectificación de

la información crediticia requerida por el titular de la información; 51.4.- Negarse a modificar o a cancelar la información de un Titular de la información luego de que éste haya obtenido un pronunciamiento favorable en un procedimiento seguido de conformidad con lo establecido en la presente Ley.

c) Sanción aplicable:

La sanción administrativa que puede ser aplicada por la Superintendencia de Bancos en perjuicio del buró de información Crediticia, es la cancelación de la licencia que permite prestar el servicio. Dicha cancelación procederá cuando el buró de Información Crediticia infrinja de manera grave y reiterada la presente ley y cuando no inicie sus actividades, dentro de los 6 meses contados a partir de la fecha en que la Junta Monetaria del Banco Central expidió la autorización de inicio de actividades (Arts. 52, 52.1 y 52.2).

4.2 Recursos contemplados en esta ley

Los recursos contemplados en la ley que nos ocupa son los siguientes: recurso de reconsideración, apelación o impugnación, contencioso administrativo y de casación. A cada uno de estos recursos nos referiremos en los párrafos que sigue.

El buró de información Crediticia tiene derecho a interponer el recurso de reconsideración contra la decisión administrativa dictada por la Superintendencia de Bancos. Dicho recurso debe interponerse dentro de los 15 días (Art.53). Cabe resaltar, que no se indica a partir de qué momento comienza a correr el referido plazo, e igualmente, tampoco se indica la forma en que debe interponerse dicho recurso. Entendemos que el referido plazo debe comenzar a correr a partir de la fecha en que el buró de información crediticia tiene conocimiento, de manera fehaciente, de la Resolución administrativa que le perjudica, y en lo que concierne a la forma, entendemos que puede hacerse, tanto mediante instancia como mediante acto de alguacil.

La decisión relativa al recurso de reconsideración puede ser recurrida por ante la Junta Monetaria del Banco Central, dentro de los 20 días hábiles, contados a partir de la fecha de la notificación de la Resolución apelada (Art.53). Dicho recurso debe interponerse mediante acto de alguacil (Art. 53).

La decisión relativa al recurso de apelación puede ser atacada mediante el recurso contencioso administrativo, por ante el Tribunal Superior Administrativo, dentro de los 30 días hábiles contados a partir de la notificación de la resolución recurrida (Art.54). El texto de referencia no establece la forma en que debe ser interpuesto el referido recurso, en tal sentido, nos parece

procedente la misma solución dada en ocasión del recurso de reconsideración, es decir, que este recurso puede ser interpuesto tanto mediante instancia como mediante acto de alguacil.

Puede afirmarse que estamos en presencia de una ley [en referencia a la Ley No.200-04, sobre libre acceso a la información pública, del 28 de julio del 2004] que garantiza la coexistencia del derecho de acceso a la información con el derecho a la protección de la vida privada de las personas físicas

La decisión del Tribunal Superior Administrativo es susceptible del recurso de casación, el cual debe interponerse en la forma prevista por la ley sobre el procedimiento de casación (Art. 55). El plazo para interponer el recurso de casación es de 2 meses (Art. 55).

4.3 Efecto suspensivo de los recursos.

Todos los recursos explicados en los párrafos anteriores tienen efecto suspensivo y en tal sentido la Superintendencia de Bancos no puede ejecutar la resolución, naturalmente, si esta hubiere sido objeto de recurso. Dicha suspensión se mantendrá hasta la fecha en que intervenga una sentencia definitiva e irrevocable (Art.. 55).

4.4 Procedimiento de Reclamación para la modificación y cancelación de la información del titular.

En los artículos del 20 al 28 de la Ley comentada, se establece el procedimiento a seguir para la obtención, por parte del titular de la información mantenida en los burós de información crediticia, de la modificación y cancelación de dichas informaciones, procedimiento este que explicamos a continuación.

a) Forma de hacer la reclamación.

La reclamación de modificación y cancelación debe hacerla el titular de la información mediante instancia o mediante acto de alguacil, acompañado de la documentación que le sirve de fundamento, no obstante, si no existieren dichos documentos bastaría con explicar dicha situación (Art. 20). La instancia

o el acto de alguacil debe dirigirse a la unidad especializada del buró de información crediticia (Art. 20).

b) Tramitación de la reclamación.

El Buró de Información Crediticia debe tramitar la reclamación en un plazo de 15 días, contados a partir de la fecha de la recepción de la misma, por ante la unidad especializada de la entidad intermediaria y en caso de que se trate de un agente económico, por ante quien designe éste a tales fines (Art. 21).

Desde el momento en que se realice la referida tramitación, debe inscribirse en el registro la expresión siguiente: "Registro impugnado", la cual se mantendrá hasta que se concluya el trámite (Art. 21 Párrafo I).

c) Plazo para responder la reclamación.

En un plazo de 30 días, contados a partir de la fecha en que se realizó la tramitación, la unidad especializada del intermediario financiero o la persona designada por el agente económico, según el caso, debe responder la reclamación y en caso de que no haya respuesta en dicho plazo, la reclamación se considerará admitida (Art. 22). Esta disposición tiene una gran importancia, ya que constituye un mecanismo de presión y de constreñimiento que evita la negligencia y garantiza que la respuesta a la reclamación se realice dentro del plazo previsto por el legislador.

d) Aceptación o rechazo de la reclamación.

En caso de que la reclamación sea aceptada, el buró de información crediticia debe hacer las correcciones que correspondan (Art. 23). Pero si fuere rechazada dicha reclamación, en el registro de que se trate se mantendrá la expresión: "Registro impugnado", hasta la fecha en que le fuere notificada al buró de información Crediticia una sentencia definitiva e irrevocable que beneficie al reclamante, si fuere este el caso la corrección debe hacerse en los 5 días hábiles contados a partir de la notificación de la sentencia (Art. 23 Párrafo II).

En el caso de que la información suministrada al buró de información crediticia la hubiere hecho una entidad pública, la corrección, si procediere, debe hacerse en un plazo de 45 días (Art. 26).

Finalmente queremos llamar la atención en el sentido de que aunque los textos comentados solo se refieren a reclamaciones que tienen como objetivos la cancelación y modificación de los datos conservados por el buró de

información crediticia, deben entenderse que es un procedimiento que puede utilizarse validamente para hacer valer cualquiera de los derechos derivados de la protección de datos personales, tales como el rectificación y el de acceso a dicha información.

e) Obligatoriedad del agotamiento del procedimiento administrativo.

El procedimiento administrativo constituye un preliminar al procedimiento judicial, dicho procedimiento es de orden público y los tribunales ordinarios no pueden darle curso a ninguna acción hasta tanto no se agoten los procedimientos administrativos (Art. 27). El reclamante tiene un plazo de un mes, contado a partir de la terminación del proceso administrativo, para iniciar las acciones judiciales (Art. 28).

En caso de que se inicie un procedimiento judicial antes de agotarse el procedimiento administrativo, el tribunal de que se trate debe sobreseer dicha acción judicial hasta que la parte interesada realice la reclamación administrativa correspondiente.

5. Ley No. 153-98 sobre telecomunicaciones, del 27 de mayo del año 1998, y resolución No. 36-00, dictada por el consejo directivo del instituto nacional de las telecomunicaciones, el 19 de diciembre del 2000.

Preferimos tratar estos dos instrumentos legales juntos, en razón de la vinculación que existe entre ambos. Dicha vinculación radica en que la resolución de referencia es dictada al amparo de la indicada ley, tal y como lo explicaremos más adelante.

La ley que nos ocupa tiene como finalidad, según se indica en su artículo 2, crear el marco regulatorio básico que se ha de aplicar en todo el territorio nacional para regular la instalación, mantenimiento e instalación de redes, la prestación de servicios y la provisión de equipos de telecomunicaciones.

En lo que respecta a la materia objeto de nuestra atención, en el artículo 5 de la citada ley se establece que las comunicaciones, los datos y las informaciones emitidos por medio de servicios de telecomunicaciones son secretos e inviolables, salvo las intervenciones judiciales, hecha de conformidad con el derecho común. Dicho texto también establece que los prestadores de servicios de telecomunicaciones son los responsables de garantizar el secreto y la inviolabilidad de las conversaciones que se realicen por el referido medio, aunque dicha responsabilidad desaparece cuando la violación sea cometida por usuarios o terceros sin su participación.

La estructura del Instituto de las Telecomunicaciones está conformado por un Consejo Directivo y por una dirección ejecutiva, según lo establece el artículo 80.1. A los fines de este tema conviene establecer la composición del Consejo Directivo, así como la función más relevante de éste.

Este consejo está integrado, según el artículo 81.1. de la manera siguiente: "El Consejo Directivo estará integrado por cinco miembros designados por el poder ejecutivo, distribuido de la siguiente manera: un (1) presidente con rango de Secretario de Estado; el Secretario Técnico de la Presidencia; un (1) miembro seleccionado de una terna elaborada a propuesta de las empresas prestadoras de servicios públicos finales de telecomunicaciones; un (1) miembro seleccionado de una terna elaborada a propuesta de las empresas prestadoras de servicios de difusión, disponiéndose que dos de los candidatos de esta última terna serán propuestos por las empresas de televisión con alcance nacional, y el otro a propuesta de las empresas de radiodifusión sonora y las empresas de televisión por cable; y un (1) miembro escogido directa y libremente, con calificación profesional, que velará por los derechos de los usuarios de servicios de las empresas antes mencionadas."

Las funciones del Consejo Directivo están previstas en el artículo 84, entre las cuales se destaca la de dictar reglamentos y normas de alcance particular, dentro de las reglas y competencia fijada por la presente ley y manteniendo el criterio consultivo de las empresas prestadoras de los diversos servicios públicos regulados y de sus usuarios. Amparado en el texto referido anteriormente, el Consejo Directivo dictó la Resolución No. 36-00, del 19 de diciembre del año 2000, la cual pasamos a comentar.

Mediante la indicada resolución se sanciona la interceptación ilegal de las telecomunicaciones, estableciéndose sanciones económicas severas, sin perjuicios de las acciones civiles y penales que el interesado pueda interponer.

Conforme a esta resolución la interceptación de las telecomunicaciones es legal cuando se hace con la debida autorización de un juez y en los casos en que se haya iniciado una investigación criminal, debiendo tener la interceptación como finalidad exclusiva coadyuvar al esclarecimiento del crimen investigado. En ausencia de los requisitos indicados la interceptación de las telecomunicaciones es calificada de ilegal;

Por la vía de la interceptación de las telecomunicaciones, la persona objeto de la misma así como su familia pierden su intimidad y su vida privada, ya que la persona

física o la institución que la lleva a cabo tiene la posibilidad de enterarse de todo lo que se hable en el seno de la familia de que se trate o en la oficina. Tal realidad justifica que las

Entendemos que en todos aquellos casos en que una persona considere violado o amenazado uno de los derechos derivados de la protección de datos personales, puede acudir ante el juez del amparo a los fines de que le sea restablecido dicho derecho

interceptación de las telecomunicaciones solo se permita de manera muy excepcional y que su realización esté rodeada de las garantías necesarias para que esta se lleve a cabo causando el menor daño posible al sujeto o los sujetos que la padecen. Me parece que la exigencia de una autorización de un juez y supeditarla a que se haya iniciado una investigación criminal, constituyen garantías válidas y capaces de evitar excesos y daños innecesarios.

En todo caso, el derecho que nos ocupa ni ningún otro derecho es absoluto, ello justifica que, aún cuando estamos en presencia de un derecho fundamental, excepcionalmente puede ser desconocido. Esta es la situación que se presenta cuando se permite la interceptación de las telecomunicaciones, se permite la invasión en la vida privada de una persona y eventualmente de su familia, para poder garantizar el orden público, la persecución del crimen y la paz social.

5.1 Sanciones aplicables a las violaciones a esta ley.

En esta ley sólo se contemplan sanciones administrativas, las cuales explicamos a continuación.

a) Organismo facultado para aplicar las sanciones administrativas.

La aplicación de las sanciones administrativas que se explicarán más adelante, le corresponde al Consejo Directivo creado por esta ley (Art 84.i).

b) Tipos de infracciones.

Las infracciones previstas en esta ley se clasifican en muy graves, graves y leves (Art. 104). La interceptación ilegal de telecomunicaciones es considerada como una falta muy grave (Art. 105). Al establecer esta

calificación el legislador quiere resaltar la relevancia y la importancia que tiene para el ser humano la protección de su intimidad y de su vida privada; ya que el darle tal calificación supone una sanción más severa. Al sancionarse de manera severa la interceptación de telecomunicaciones ilegal, se intimida y se desincentiva a aquellas personas físicas y morales que eventualmente pudieren tener interés en hacer uso de dicho mecanismo.

a) Sanciones administrativas aplicables.

La falta muy grave que es la que nos interesa en este momento, se sanciona con un mínimo de 30 cargos por incumplimiento y un máximo de 200 cargos por incumplimiento (Art. 109). Un cargo por incumplimiento equivale a RD$20,000 pesos dominicanos (Art.108). De igual forma, dicha suma debe ser actualizada al momento en que se aplica la sanción y conforme al índice de inflación establecido por el Banco Central (Art.108).

6. Resolución dictada por la Suprema Corte de Justicia el 13 de noviembre del 2003, la cual establece los requisitos que deben observarse en las interceptaciones telefónicas.

Mediante esta resolución la Suprema Corte de Justicia establece el procedimiento que debe seguirse en la obtención de pruebas, utilizando el mecanismo de la interceptación telefónica. Dicha resolución se dicta en razón de que ninguna disposición legal prevé procedimiento a tales fines, y en virtud de lo dispuesto en el artículo 29.2 de la Ley 821 sobre Organización Judicial de 1927, texto que faculta a la Suprema Corte de Justicia a establecer el procedimiento a seguir en todas aquellas materias en que no exista.

La intromisión en la vida privada de una persona es sancionada con prisión de 6 meses a 1 año, y multa de 25 a 50 mil pesos, según lo dispone el artículo 337 del Código penal Dominicano, modificado por la Ley No. 24-97 del año 1997. En razón de que mediante el mecanismo de la interceptación telefónica se corre el riesgo de invadir la vida privada de una persona física y eventualmente de su familia, resulta ampliamente justificada y de mucho interés que dicha práctica sea reglamentada con la finalidad de que puedan obtenerse las pruebas necesarias para el esclarecimiento de un crimen y garantizar, al mismo tiempo, que la intromisión en el ámbito privado cause el menor daño posible.

En la resolución que comentamos, cabe destacar los siguientes aspectos:

a) Causas que justifican la interceptación telefónica.

Las Causas que justifican la interceptación telefónica deben ser apreciadas de manera libre por el juez de la instrucción de la jurisdicción en la cual se investigue el hecho justificativo de la interceptación telefónica. En tal sentido, dicho juez autorizará la interceptación, cuando se reúnan los siguientes requisitos: a) que el servicio o medio intervenido esté siendo utilizado para propósitos ilegales, b) que mediante la interceptación pudieran obtenerse pruebas de la comisión de un crimen, y c) que el mecanismo de la interceptación sea el único o el más favorable medio para la obtención de dicha prueba.

b) Crímenes que justifican la interceptación.

La interceptación telefónica sólo puede ser autorizada cuando las investigaciones estén relacionadas con las infracciones siguientes: Violaciones a la ley sobre drogas y sustancias controladas, Lavado de dinero y activos provenientes del narcotráfico y otros actos ilícitos, Crímenes y delitos contra la seguridad del Estado, Terrorismo, Secuestros, Crímenes contra los derechos humanos, Crímenes cometidos por funcionarios públicos en el ejercicio de sus funciones, Soborno o cohecho de los funcionarios públicos, Crímenes capitales, Infracciones sexuales contra los menores, Violaciones sexuales y violencia intrafamiliar, Interceptaciones ilegales realizadas por personas particulares sin autorización legal, en violación del artículo 337 del Código penal, modificado por la Ley 24-97, Cualquier otro crimen o delito que necesite de la interceptación por su peligrosidad y carácter de antisocial, o por la dificultad de obtener por otros medios la prueba de su comisión.

c) Secreto Profesional.

La interceptación telefónica está limitada a la obtención de las pruebas pertinentes para el esclarecimiento del crimen de que se trata. Se prohíbe, mediante la resolución, interceptar, captar y grabar las comunicaciones o mensajes de cualquier tipo protegidos por el secreto profesional, tales como: las conversaciones entre el imputado y su abogado, las conversaciones o confesiones obtenidas por personas en razón de su ministerio, y las conversaciones de los médicos con sus pacientes relacionadas con la asistencia médica que ofrece el primero.

d) Duración de la medida.

El mecanismo de la interceptación telefónica debe ser utilizado de una manera muy excepcional y en los casos extremos en que el

mismo constituya el único medio de obtención de prueba o el más idóneo, ello así porque las molestias, los inconvenientes y las perturbaciones que crea en la persona que la padece así como en su familia, son evidentes y muy graves. Dadas las circunstancias indicadas anteriormente, la Suprema Corte de Justicia, mediante la resolución comentada, estableció un plazo de duración de la interceptación de 60 días, contados a partir de la fecha de la autorización emitida por el juez, o hasta que se logre el objetivo para la cual fue expedida. No obstante, si en el señalado plazo de 60 días no es posible lograr el objetivo de la interceptación, dicho plazo puede ser prorrogado, pero dicha solicitud debe ser hecha por el Ministerio Público y además deberá estar acompañada de los elementos o de la documentación que justifique plenamente la extensión pretendida.

e) Transcripción de las grabaciones.

En la resolución comentada se evidencia claramente la preocupación de la Suprema Corte de Justicia para que la interceptación telefónica se mantenga dentro de los límites necesarios para el logro de los objetivos trazados, y para lograr en todo lo posible el respeto de la vida privada y de la intimidad de la persona objeto de la interceptación, así como de su familia. En este sentido, se le prohíbe de manera expresa al Procurador Fiscal, sus ayudantes y los auxiliares de la Policía Judicial, incluir, al momento de la transcripción de las grabaciones, informaciones personales, íntimas o familiares.

Cabe destacar que en fecha 19 de julio del año 2002 se aprobó la Ley 76-02, que instituye el Código Procesal Penal. Dicho Código entró en vigencia 24 meses después de dicha fecha, en aplicación de lo dispuesto en el artículo 449 del mismo código. En el artículo 192 del referido código se contempla todo lo relativo a la interceptación telefónica, texto este que coincide en su contenido con la resolución de referencia, salvo en los aspectos que explicamos a continuación.

En efecto, en el Código Procesal Penal se establece que la duración de la medida es de 30 días, pudiendo ser prorrogada por otros 30 días, si existieren causas que la justifiquen, mientras que en la resolución se indica un plazo de 60 días prorrogables. La otra diferencia es que mientras en la resolución la interceptación telefónica procede en una gran cantidad de infracciones, en el Código se establece que la interceptación telefónica, sólo procede cuando se trate de infracciones cuya pena sea superior a los 10 años.

Ante tales discrepancias se impone lo previsto en el Código Procesal Penal, no sólo porque es posterior a la resolución, sino porque se trata de una norma de mayor jerarquía.

II. Mecanismo legales para garantizar la eficacia de la protección de los datos personales y los derechos derivados del mismo.

Conforme a la doctrina de la protección de datos personales se derivan los siguientes derechos: a) derecho de acceso a los datos personales, b) derecho de rectificación, c) derecho de modificación, d) derecho de cancelación, e) derecho de confidencialidad. Por otra parte, la protección de datos personales es considerada como un derecho fundamental de tercera generación, es decir, que forma parte de aquellos derechos individuales y colectivos, como el derecho a un ambiente saludable, a la paz, a la verdad, y al libre desarrollo de la personalidad.

Tratándose de un derecho fundamental, su protección puede obtenerse por la vía del recurso de amparo, recurso este que en nuestro ordenamiento jurídico existe desde 25 de diciembre de 1977, fecha en que el Congreso Nacional ratificó la Convención Americana sobre Derechos Humanos del 22 de noviembre de 1969, mediante la Resolución No. 739, dictada en la indicada fecha.

El procedimiento a seguir para la instrucción del recurso de amparo fue establecido por la Suprema Corte de Justicia, mediante la Resolución de fecha 24 de febrero de 1999. En dicha resolución se establece que el recurso de amparo procederá en todos aquellos casos en que exista un acto arbitrario o una amenaza de acto arbitrario, mediante el cual se desconozca o pretenda desconocer derechos fundamentales.

Entendemos que en todos aquellos casos en que una persona considere violado o amenazado uno de los derechos derivados de la protección de datos personales, puede acudir ante el juez del amparo a los fines de que le sea restablecido dicho derecho. No obstante, el juez del amparo no tiene facultad para aplicar sanciones penales ni establecer indemnizaciones; en tal sentido, la víctima de la violación puede acudir ante los tribunales penales y civiles, con el objetivo de obtener estas últimas pretensiones✧

El Magistrado Hermógenes Acosta de los Santos es Juez Presidente de la Segunda Sala de la Cámara Civil y Comercial de la Corte de Apelación del Distrito Nacional de la República Dominicana.*

Análisis de la Ley No. 17838: Protección de Datos Personales para ser utilizados en Informes Comerciales y Acción de Habeas Data

Dra. Esc. Beatriz Rodríguez Acosta *

El artículo se basa en el análisis de la protección de datos en el Uruguay, y su evolución hasta nuestros días.

El hombre siempre ha tenido un lado "secreto" en su vida, un lado en el cual ha guardado parte de su personalidad, en el que sólo se registran sus pensamientos y deseos más íntimos.

Se ha dicho que "lo íntimo es tan central al hombre que hay un sentimiento natural que lo protege: la vergüenza o pudor, que es la protección natural de la intimidad, el cubrir u ocultar espontáneamente lo íntimo frente a las miradas extrañas"[50]

Con el surgimiento y avance de las nuevas tecnologías esa intimidad, ese derecho a la intimidad se vuelve cada vez más transparente y accesible a todos lo ciudadanos, muchas veces sin el consentimiento de la persona involucrada.

Surge así un nuevo contenido para las bases de datos: el de los datos de carácter personal. Datos que son recopilados por terceros ajenos a las personas a las cuales éstos pertenecen, que pueden modificarlos tanto en forma positiva como negativa, al igual que ser objeto de comercio entre los hombres y muchas veces alcanzar valores muy altos.

El tratamiento informático de estos datos personales, como por ejemplo los gustos y aficiones, los hábitos de compra y el poder adquisitivo, puede ser una fuente de información, que en manos de terceros llega a perjudicar el libre desarrollo de la personalidad o provocar la denegación de derechos.[51]

Evolución de la Protección de Datos Personales

[50] Ricardo YEPES STORK. "Fundamentos de Antropología". EUNSA, Pamplona, 1996. Páginas 77 y 78, citado por Carlos E. DELPIAZZO en "Dignidad Humana y Derecho". Montevideo, 2001. Página 121

[51] Mª Rosa, LLÁCER MATACÁS, "La Protección de los Datos Personales en Internet", en "La regul@ción del comercio electrónico", Dykinson, Madrid, 2003. Páginas 158 y siguientes.

Desde la década de los setenta comienza una evolución en la normativa sobre la protección de los datos personales, apareciendo las llamadas leyes de primera generación en ésta materia, teniendo como características principales la creación de archivos automatizados cuyo contenido eran los datos personales, así como la creación de instituciones que garantizaran el buen uso de éstos y la defensa de los ciudadanos que se pudieran ver afectados.

Las normas que se adopten a este respecto deben ser equilibradas, entre una justa protección del derecho a la privacidad y la posibilidad de emplear sistemas automatizados para el almacenamiento y el manejo eficaz de la información disponible. [52]

Tal es así que países como Alemania, en Hesse, promulgaron en octubre de 1970 la primera ley de protección de datos personales automatizados, y Suecia lo hizo en 1973, pero teniendo esta ley carácter nacional no provincial como la alemana, estableciendo el principio de la publicidad de los bancos de datos personales.

La información referente a los datos personales fue circulando cada vez más en forma independiente, en pequeño volumen, sin que la persona interesada pueda saber "dónde hay datos personales suyos, qué uso se hace de ellos, qué elementos de juicio o valorativos se les añaden y qué consecuencias puede causarle ese uso incontrolado de sus propios datos"[53]

Así llegamos a lo que se llama la segunda generación de leyes, donde los principales exponentes en la materia fueron países como España con la Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal o LORTAD, en 1992, la que fue modificada en 1999 por la Ley Orgánica de Protección de Datos de Carácter Personal o LOPD.

En los Estados Unidos, en diciembre de 1974, se promulgó la Privacy Act, estableciendo el derecho de conocer y acceder a la información, así como el derecho de rectificar.

Como las leyes de primera generación éstas también tienen sus características principales que son: la proliferación de los archivos con datos personales automatizados, pero a diferencia de las anteriores se le otorga mayor garantía a las personas, surgen los llamados derechos de acceso, rectificación, y modificación de información no fehaciente.

En ésta etapa surgen nuevos conceptos como los de dato sensible y habeas data, definiéndoselos como:

[52] Ricardo GUIBOURG y otros. "Manual de Informática Jurídica". Astrea, Buenos Aires, 1996. Página 264 y 265

[53] Carlos E. DELPIAZZO. " Derecho Informático Bancario" I.E.E.M. Montevideo, 1990. Página 37 y siguientes.

Dato sensible: aquellos datos personales que, en atención a resultar los mayormente pasibles de provocar tratamientos discriminatorios a sus titulares, reciben en toda la normativa de la materia una prohibición de principio a su tratamiento automatizado, sin perjuicio de premisas y acotadas excepciones a dicha regla. Son todos aquellos relativos a origen racial o étnico, costumbres sexuales, enfermedades infectocontagiosas, convicciones religiosas o filosóficas y pertenencia a sindicatos.[54]

Habeas data: cauce procesal para salvaguardar la libertad de la persona en la esfera informática, que cumple una función paralela, en el seno de los derechos humanos de la tercera generación, a la que en los de primera generación correspondió al habeas corpus respectos de la libertad física o de movimientos de la persona.[55]

En este período no sólo mediante leyes se reconoce la protección de los datos personales sino que se lo hace en forma constitucional, ya que varios países la han consagrado, entre los que se encuentran Portugal, España, y en América países como: Argentina, Brasil, Colombia, Paraguay, Perú y Venezuela.

Se ha dicho siempre que el ciberespacio es el lugar sin fronteras, en el que los Estados pierden sus límites y toda la protección que se pueda realizar en cada uno de ellos de los datos personales, no es suficiente, ya que al traspasar esas fronteras a otros Estados sin normativa, vuelven a quedar desamparados, por lo que se ha tratado de establecer las llamadas leyes de tercera generación respecto a los datos personales.

Estas leyes ya no tienen el carácter de nacional o local que podían tener sus antecesoras, sino que tratan de lograr un alcance internacional o por lo menos regional, se trata de armonizar y unificar la normativa existente. Dentro de éstas podemos referirnos a la Directiva del Parlamento Europeo y Consejo No. 95/46 que consagra la protección de las personas físicas en cuanto a cómo se tratarán sus datos personales y a la libre circulación de los mismos, logrando que prime una protección adecuada, haciendo eco del principio de reciprocidad entre los diferentes países.

En la Directiva No. 95/46/CE se establece el principio de adecuación mediante el cual los Estados miembros permitirán la transferencia de datos personales a un tercer país si éste otorga las garantías suficientes para esa transmisión, o sea que le proporciona un nivel adecuado de protección y se cumplen en él, antes de la transferencia, las disposiciones legales que los Estados miembros aprueben en

[54] Curso on line Derecho del Ciberespacio." Tecnologías de la información y derechos personales", Módulo 2, Montevideo, 2003.
[55] Antonio PEREZ-LUÑO. " Del habeas corpus al habeas data". Aranzadi, Madrid, 1991. Página 194

aplicación de otros preceptos de la Directiva. Si el tercer país cumple con el nivel de adecuación no necesita garantía para la transferencia de datos con los Estados miembros de la Unión Europea.

En esta etapa se aprueba por las Naciones Unidas la Resolución No. 45/95 en la cual se establecen los principios rectores para la reglamentación de los ficheros computarizados de datos personales, siendo éstos: principio de libertad y lealtad, principio de exactitud, principio de finalidad, principio de acceso de la persona interesada, principio de no discriminación, y de seguridad.[56]

La Protección de Datos en Uruguay

Nuestro país se ha caracterizado por no tener una legislación específica sobre esta materia hasta el 7 de octubre de 2004, día en que se promulga la Ley No. 17838 sobre "Protección de Datos Personales para ser utilizados en Informes Comerciales y Acción de Habeas Data".

Existe normativa en la que se consagra el derecho a la privacidad, a la intimidad, como derecho fundamental, pero sin estar mencionado específicamente, por lo que siguiendo lo establecido por el artículo 16 de nuestro Código Civil, se aplicaban éstas como normas análogas.

"Si bien no tenemos reglas ni organismos, sin duda tenemos principios aplicables al tema. Esos principios derivan tanto a partir de los derechos fundamentales que tienen que ver con el tema, como de la introducción de algunos principios que se han elaborado en otros lugares o en otros foros..."[57]

El tratamiento informático de estos datos personales, como por ejemplo los gustos y aficiones, los hábitos de compra y el poder adquisitivo, puede ser una fuente de información, que en manos de terceros llega a perjudicar el libre desarrollo de la personalidad o provocar la denegación de derechos

Dentro de estas normas podemos mencionar los siguientes artículos de la Constitución, los que están insertos en la Sección II denominada "Derechos, Deberes y Garantías":

[56] Ana BRIAN NOUGRERES y otras. " El Derecho a la Intimidad en la era de las Nuevas Tecnologías". Ponencia del VI Congreso Iberoamericano de Derecho e Informática, Montevideo, 1998. Página 56

[57] Alberto PEREZ PEREZ y otros. " La situación en Uruguay". ¿Seguridad, Privacidad, Confidencialidad? El desafío de la protección de datos personales. Goethe – Institut, Montevideo, 2004. Página 109.

Artículo 7: " Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad. Nadie, puede ser privado de estos derechos sino conforme a las leyes que se establecieren por razones de interés general",

Artículo 10: "Las acciones privadas de las personas que de ningún modo atacan el orden público ni perjudican a un tercero, están exentas de la autoridad de los magistrados."

Este artículo consagra el derecho de no intromisión en la vida privada de los individuos.
Artículo 28: "Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interceptación sino conforme a las leyes que se establecieren por razones de interés general."
Si seguimos lo que establece el Dr. Gros Espiell éste artículo se debe aplicar también a las comunicaciones telefónicas, "cubre no sólo el contenido sino la existencia misma de las comunicaciones telefónicas y, por ende, su difusión y conocimiento por terceros".[58]

Con este artículo podemos marcar "el contraste entre lo que era la preocupación exclusiva del pasado – que no ha dejado de existir actualmente – y lo que es la preocupación del presente. La del pasado era la preocupación de los papeles de los particulares, ahora el problema se refiere a los datos sobre los particulares, o los datos sobre las personas que tengan otros."[59]

Artículo 72: "La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno".

Como hemos mencionado anteriormente el derecho a la intimidad, la privacidad, no está consagrada en nuestro derecho de forma escrita, pero puede ser reconocido por este artículo 72, ya que establece que no se excluyen "otros" derechos que sean inherentes a la personalidad humana, y lo mismo sucede con el concepto de Habeas Data.

Al decir del Dr. Delpiazzo: "la libertad informática se encuentra reconocida en el art. 72 de la Constitución, que incorpora al ordenamiento jurídico positivo nacional la esencia ideológica del jusnaturalismo y, consecuentemente, tutela efectivamente los derechos del hombre inherentes a su personalidad, garantizándolos"[60].

[58] Héctor, GROS ESPIELL, "El art. 28 de la Constitución y las Comunicaciones Telefónicas", en Revista. de Administración Pública, Montevideo, 1999, núm. 25. Página 86.

[59] Alberto PEREZ PEREZ y otros. " La situación en Uruguay", en ¿Seguridad, Privacidad, Confidencialidad? El desafío de la protección de datos personales. Goethe – Institut, Montevideo, 2004. Página 111

[60] Carlos E, DELPIAZZO,. "Posibles medios de protección frente a las responsabilidades derivadas de la gestión de bases de datos en el Derecho

Fuera del ámbito constitucional tenemos algunas disposiciones que también pueden ser aplicadas, pero sin hacer mención específica de la protección de los datos personales, el derecho a la intimidad o la privacidad, como son:

Las disposiciones de la Ley No. 16011, de fecha 19 de diciembre de 1988, más conocida como la" Ley de Acción de Amparo";

La Ley No. 16616, de fecha 20 de octubre de 1994, que regula el Sistema Estadístico Nacional y el secreto que existe sobre la divulgación de los datos proporcionados por las personas al contestar el cuestionario que le realiza el encuestador, estableciendo que: "Los datos individuales aportados con fines estadísticos no pueden ser utilizados con otros fines, ni aún mediando solicitud expresa del informante";

El Decreto No. 396/03, de fecha 30 de setiembre de 2003, regula los datos personales referentes a la salud, la historia clínica del individuo. En este Decreto se establecen principios generales que sirven de criterio de interpretación cuando surjan problemas de aplicación de ésta disposición, así como quién es el encargado de autorizar a terceros para su estudio.

También debemos mencionar la normativa de carácter internacional que fue internalizada a nuestro Derecho como el Pacto Internacional de Derecho Civiles y Políticos, incorporado por la Ley No. 13.751, de fecha 11 de julio de 1969, que en su artículo 17 establece que: "Nadie será objeto de ingerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación".

Lo mismo sucede con el Pacto de San José de Costa de Rica**,** incorporado a nuestra legislación por la Ley No. 15.737, de fecha 8 de marzo de 1985, que en su artículo 11, inciso 2, regula exactamente lo mismo que el Pacto anteriormente mencionado: "Nadie puede ser objeto de ingerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación".

En nuestro país, ya desde décadas pasadas, se han presentado proyectos referentes al tema de protección de datos y acción de habeas data, que no han sido aprobados por las legislaturas, otras veces por sólo una cámara y así sucesivamente, hasta llegar al año 2004, en que se aprueba uno de los proyectos presentados.

uruguayo", en Congreso Internacional de Informática y Derecho, Buenos Aires, 1990. Página 382 y siguientes.

Así surge la Ley No. 17838 que se refiere a la protección de los bancos de datos de carácter comerciales, por lo que no colma todas las expectativas que tenían algunos de los legisladores, los que habían presentado otros proyectos que incluían otros bancos de datos con un contenido más extenso, y sobre los que es necesario legislar, pero ésta es un avance en la materia para nuestro país.

Esta ley se estructura en tres Títulos, el primero de ellos contiene tres Capítulos, los cuales tienen como contenido: el tratamiento de datos personales asentados en archivos, registros, bases de datos, etc., públicos o privados, destinados a dar informes objetivos de carácter general, y los principios generales donde se consagra el alcance del tratamiento de datos personales.

En el segundo Título encontramos también tres Capítulos, en los que podemos ver la regulación de un nuevo concepto que se incorpora a nuestro Derecho, el "Habeas Data", luego la acción de protección de los datos comerciales, y por último establece cual va a ser el órgano de control.

Finaliza la nueva Ley con un Título III destinado a las disposiciones finales y transitorias.

De acuerdo al **artículo 1** las disposiciones de la presente ley establecen como sujetos pasivos tanto a las personas físicas como jurídicas. Además regula el objeto, que está representado por las siguientes acciones: regular el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, así como el tratamiento de datos personales, que se encuentren en archivos, registros, bases de datos, u otros medios similares autorizados, sean públicos o privados.

Como vemos los medios en los cuales están asentados esos datos personales de carácter comercial están enumerados a vía de ejemplo, ya que dice la norma: "u otros medios similares autorizados".

Estos registros pueden estar tanto en la órbita pública como privada.

En el **artículo 2** se establecen las excepciones de esta ley. También vemos que la enumeración que realiza es a vía de ejemplo, ya que el mismo artículo así lo establece.

Asimismo podemos ver que para la obtención y tratamiento de los datos que no sean comerciales se necesitará la "expresa y previa conformidad de los titulares, luego de informados del fin y alcance del registro en cuestión", lo que no es necesario para la obtención y tratamiento de datos que sean de carácter comercial, consagrando así el apartamiento del régimen de la protección de datos personales, ya que se debería de necesitar, sea cual sea el carácter de estos, el

consentimiento y conformidad de los titulares de esos datos personales.

Nuestro país se ha caracterizado por no tener una legislación específica sobre esta materia hasta el 7 de octubre de 2004, día en que se promulga la Ley No. 17838 sobre "Protección de Datos Personales para ser utilizados en Informes Comerciales y Acción de Habeas Data"

En el Capítulo II del Título I se consagran los principios generales que rigen el tratamiento de los datos personales con carácter comercial.

El primer principio consagrado es el de legalidad, principio que se hace efectivo en el artículo 3 cuando se establece que: " se deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley reconoce".

En el artículo 4 volvemos a tener excepciones, en este caso es en cuanto sólo a la necesidad del consentimiento del titular de los datos, se enumeran en cuatro incisos cuales son los datos personales que no requieren previo y especial consentimiento:

a) los que deriven de fuentes públicas de información, mencionando los registros, archivos y publicaciones en medios masivos de comunicación;

b) los recabados para el ejercicio de funciones o cometidos constitucional y legalmente regulados propios de las instituciones del Estado o en virtud de una obligación específica legal;

c) cuando se trate de listados cuyos datos se limiten a nombres y apellidos, documento de identidad o registro único de contribuyente, nacionalidad, estado civil, nombre del cónyuge, régimen patrimonial del matrimonio, fecha de nacimiento, domicilio y teléfono, ocupación o profesión y domicilio.

En este inciso vemos que se establece que no es necesario previo y especial consentimiento para obtener datos que estarían dentro de la categoría de "datos sensibles" de las personas, como por ejemplo: régimen patrimonial del matrimonio, ocupación o profesión, nombre del cónyuge, su estado civil, el domicilio laboral.

d) los que deriven de una relación contractual del titular de los datos y sean necesarios para su desarrollo y cumplimiento:

e) se realice por personas física o jurídicas, privadas o públicas, para su uso exclusivo o el de sus asociados o usuarios.

Otros principios consagrados en esta Ley son los de: veracidad, adecuación, ecuanimidad, y no exceso.

El **artículo 5** se encarga de enumerarlos, así como de proteger a estos datos, estableciendo que "el titular del registro es responsable de la violación de esta disposición, así como de la obtención ilegítima de sus datos". Menciona aquí por primera vez quién es el responsable por esos registros, a su vez la obtención de esos datos no pueden ser mediante medios ilícitos, como el fraude, abuso, extorsión y toda otra forma que sea contraria a la ley.

En su inciso final consagra otra de las responsabilidades de quien es responsable del tratamiento de ese archivo: el deber de suprimir, sustituir y completar los datos, cuando sean total o parcialmente inexactos o incompletos, completándolos con datos veraces y actualizados, pero esa responsabilidad se vuelve tal siempre y cuando éste conociere la circunstancia.

Otra circunstancia que encontramos en este artículo es que remite al artículo 9, en lo que se refiere el plazo de caducidad de los datos, los cuales deben ser eliminados al llegar al mismo.

Se regulan las obligaciones de las personas físicas o jurídicas encargadas de obtener la información, estableciendo en su **artículo 6**, que deben "utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros". Se consagra aquí el principio de finalidad, así como el deber de confidencialidad, la no difusión de la información.

El deber de secreto se extiende no sólo a quien es el titular del archivo o registro, o base de datos, sino también a las personas que tienen relación con éste, ya sea en forma laboral u otra forma de relación, y ese secreto va a perdurar durante y después de finalizada la relación entre ambos (**artículo 7**).

Si no se cumple con este requisito se aplicará lo establecido en el artículo 302 del Código Penal que establece que: "El que, sin justa causa, revelare secretos que hubieran llegado a su conocimiento, en virtud de su profesión, empleo o comisión, será castigado, cuando el hecho causare perjuicio, con multa ..."

Al final de su inciso segundo se establece la excepción de guardar secreto, cuando éste sea relevado por juez competente o por consentimiento del titular.

A partir del artículo 8 comienza el Capítulo III del Título I, denominado "Del tratamiento de datos personales relativos a obligaciones de carácter comercial", finalizando en el artículo 11.

En el **artículo 8** podemos encontrar una clasificación de cuáles son los datos que pueden ser tratados de acuerdo a la Ley, así tenemos:

a) datos personales relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial;

b) datos personales que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos;

c) datos que provienen de fuentes de acceso público, o de informaciones facilitadas por el acreedor o de acuerdo al artículo 5, anteriormente mencionado.

Habíamos mencionado brevemente el artículo 9, cuando hablamos del artículo 5, referente al plazo en que podrían estar registrado los datos personales relativos a obligaciones de carácter comercial. Este artículo establece que "sólo" podrán estar registrados por cinco años a partir de su incorporación en el registro. A continuación se establece un plazo para solicitar su nuevo registro por "única vez", al acreedor, siempre y cuando el titular de esos datos no hubiera cumplido con su obligación.

El nuevo registro se debe solicitar antes de los treinta días del vencimiento del plazo, si se hace después no tendría andamiento la solicitud y caducaría la inscripción.

Se establece en el inciso final un plazo para el mantenimiento de los datos en el archivo, una vez cancelada o extinguida la obligación por cualquier medio de cumplimiento, por un plazo "máximo" de cinco años contados desde la fecha de la cancelación o extinción.

Ese plazo no es renovable, esto se debe a la aplicación nuevamente, del principio de finalidad en el que se asegura que el período de conservación de los datos personales no excede el necesario para alcanzar la finalidad con que se ha registrado.[61]

Vuelve a establecer otra obligación para los responsables de las bases de datos, en su **artículo 10**, limitándolo a efectuar valoraciones subjetivas respecto a la información, lo que hace que esta información sea veraz y sin ninguna implicancia valorativa.

Si la obligación es cumplida por el deudor se debe realizar la comunicación al responsable de la base de datos. Este **artículo 11** establece obligaciones tanto para el acreedor como para el responsable de la base de datos, el deber de comunicación de la modificación de la situación al responsable del registro, estableciéndole como máximo un plazo de diez días hábiles para efectuar dicha comunicación, y de tres días hábiles para el responsable de la base para realizar la actualización de la misma.

[61] Alberto PEREZ PEREZ y otros. " La situación en Uruguay". ¿Seguridad, Privacidad, Confidencialidad? El desafío de la protección de datos personales. Goethe – Institut, Montevideo, 2004. Página 115

En el Titulo II el tema es el Habeas Data y Organo de Control, en su Capítulo I comenzamos con la regulación del Habeas Data.

El **artículo 12** regula el derecho que tiene toda persona a entablar una acción para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso. Como vemos en toda la ley se repiten los principios de finalidad, veracidad, así como el derecho de acceso a la información por el titular, sin importar si esos registros tienen el carácter de públicos o privados.

También se regula el derecho de rectificación, de supresión de los datos personales incluidos en la base de datos, si existe error, falsedad o discriminación en la información.

En el **artículo 13** se menciona que habrá un registro actualizado de consulta, que será gratuito y público, teniendo acceso a él cualquier persona que lo requiera al órgano de control que se menciona más adelante.

Se consagra el derecho de acceso a la información por todo titular en el **artículo 14**. El titular como requisito debe presentar su documento de identidad para certificar que es quien dice ser.

Como característica este derecho de acceso es gratuito, puede hacerse a cualquier clase de registro, ya sea público o privado, y se debe realizar por intervalos no inferiores a seis meses, con la excepción de un interés legítimo de acuerdo al ordenamiento jurídico.

Si los datos personales son de personas que ya han fallecido, el derecho de acceso se puede ejercer por quien tenga derecho a hacerlo, o sea por sus herederos universales, siempre y cuando justifiquen tal calidad presentando la sentencia de declaratoria de herederos.

Se le establece un plazo al responsable de la base de datos para otorgar la información solicitada, lo debe hacer "dentro de los veinte días hábiles de solicitada". Si así no lo hiciera o si lo negara sin justificación, quien haya solicitado la información tiene habilitada la acción de habeas data.

En el **artículo 15** se establece el procedimiento para dar cumplimiento a los derechos de rectificación, actualización, eliminación o supresión de los datos, si así correspondiera en caso de error o falsedad de la información.

Habilita, este artículo en su inciso tercero, si no se cumple con el procedimiento, al interesado a promover la acción de habeas data, como garantía de su accionar.
Asimismo menciona las razones por las cuales se debe eliminar o suprimir los datos personales del titular:

a) en casos de notorio error o falsedad

b) en casos en que se pueda causar perjuicio a los derechos o intereses legítimos de terceros

c) en casos en que contravengan lo establecido por una obligación legal.

Mientras se encuentre el proceso en marcha, el responsable del registro debe dejar constancia de que la información está siendo revisada, si es solicitada por terceros.

Todas las acciones que se realicen, ya sean de rectificación, actualización, eliminación o supresión de datos personales cuando sea necesario realizarlas, serán hechas gratuitamente, esto es para que cualquier interesado pueda acceder a ese beneficio. (**artículo 16**)

Con el artículo 17 hasta el 19 se configura el Capítulo II, del Título II, el cual se denomina "Acción de protección de los datos personales".

La acción de habeas data procede cuando se cumplen los supuestos establecidos en el **artículo 17**. Con ella se trata de dar seguridad al titular de los datos, siendo el sujeto activo de la misma, contra el responsable de la base de datos o registro (sujeto pasivo), que se van a cumplir con todos los principios de derecho que han sido mencionados a lo largo de toda la Ley.

Se menciona quienes son las personas que van a tener la legitimación activa de esta acción, en algunos casos ya sea por si o mediante apoderado como es el caso de los herederos y los representantes de las personas jurídicas. (**artículo 18**).

En el **artículo 19** se establece que las acciones que se promuevan va a regirse en lo general por las normas del Código General del Proceso, y en lo especial por lo establecido en los artículos 6, 7, 10, 12 y 13 de la Ley No. 16011, de fecha 19 de diciembre de 1988, conocida como la "Ley de Acción de Amparo".

El órgano de control está regulado en el Capítulo III del Título II, artículos 20 a 21.

Quien será el órgano de control es el Ministerio de Economía y Finanzas asistido por una Comisión Consultiva integrada por: tres integrantes de ese Ministerio, dos del Ministerio de Educación y Cultura, un representante de la Cámara Nacional de Comercio y de Servicios y uno de la Liga de Defensa Comercial. Estará presidida por uno de los representantes del Ministerio de Economía y Finanzas.

A su vez el **artículo 20** consagra los cometidos de la Comisión Consultiva y el **artículo 21** la aplicación de medidas sancionatorias a las firmas de tratamiento de datos en caso que se violen las normas de esta Ley, que van desde el apercibimiento hasta la clausura del archivo o registro o base de datos.

Para hacer cumplir estas sanciones se establece el procedimiento que se llevará a cabo, así

como qué sucederá en caso de interposición de recursos contra la resolución judicial que hiciere lugar a la clausura, el uso de la fuerza pública si fuera necesaria para la clausura en caso de incumplimiento de la resolución.

El juez competente será de acuerdo a las normas de la Ley Orgánica de la Judicatura No. 15750, de fecha 24 de junio de 1985.

Así llegamos al Título III "Disposiciones finales y transitorias".

Se establece un plazo de transición para los archivos, registro y bases de datos existentes con anterioridad a la presente Ley de noventa días a partir del momento de la promulgación de ésta para ponerse al día con la normativa e inscribirse en el registro (**artículo 23**).

El mismo plazo anterior se le otorga por el **artículo 24**, a los responsables de las bases para actualizar los registros de acuerdo a la normativa vigente, así como a los acreedores para actualizar los datos que tengan incorporados a las bases desde hace más de cinco años.

Si estos últimos no comunicaron al responsable de la base las cancelaciones que se realizaron, tendrán un plazo de diez días hábiles para hacerlo, y el responsable tres días hábiles par actualizar los registros (**artículo 25**).

Como mencionamos up supra, en nuestro régimen jurídico las normas generales están mencionadas en la Constitución, en las Leyes Nos. 16011, 16616, Decreto 396/95 y en la Ley No. 17838 específica de datos personales.

En la Constitución no se menciona, como en otras, un recurso judicial especial llamado habeas data, que si se menciona en la Ley No. 17838, además de los principios generales de protección de datos, pero tiene una limitante que es: el objeto protegido, ya que son sólo el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, así como el tratamiento de datos personales, que se encuentren en archivos, registros, bases de datos, u otros medios similares autorizados, sean públicos o privados en la esfera comercial, dejando de lados los demás campos de información.

De acuerdo a lo establecido anteriormente y en el artículo 25, apartado 2 de la Directiva No. 95/46/CE el carácter de adecuado del nivel de protección que puede ofrecer nuestro país no se adecua totalmente a los requisitos necesarios para eso.

Con fecha 19/12/06 se promulgó la Ley No. 17.930 de Presupuesto Nacional, la que en su artículo 261, prohíbe la cesión, venta, reproducción o entrega a terceros de la información relativa al estado civil de las personas por quienes reciben la misma en virtud de convenios celebrados con la Dirección

General del Registro de Estado Civil, sean personas físicas o jurídicas, públicas o privadas, y se realice en forma onerosa o gratuita.

Establece además que La Dirección General del Registro de Estado Civil será la encargada de fiscalizar el cumplimiento de lo establecido en este artículo, y que el Ministerio de Educación y Cultura reglamentará las sanciones económicas a aplicar ante el incumplimiento de la prohibición establecida.

En el plano judicial se promulgó la Acordada No. 7564 de fecha 1/2/06, sobre el tratamiento de datos en el Poder Judicial, teniendo por objeto la protección integral de los datos personales - incluidos los datos sensibles -, asentados en bancos o bases de datos de carácter documental o jurisprudencial en todos los ámbitos del Poder Judicial y cualquiera sea el soporte que los contenga papel o magnético.

Conclusiones

Hemos dado un paso adelante en lo que se refiere a la materia de protección de datos personales, pero no alcanza a cubrir todo el espectro de la misma, ya que sólo se ha legislado en materia de carácter comercial.

Se han incluido en nuestro régimen jurídico nuevos conceptos como el de Habeas Data, y el de acción de habeas data, que también se ven limitados en su alcance, por el carácter de los datos personales que se mencionan en la Ley.

Mediante esta normativa los titulares de los datos personales tienen procedimientos que le aseguran la protección de sus derechos fundamentales referentes a la información que se encuentra en las bases de datos, registros o archivos.

Se puede decir que en lo que se refiere a los datos personales con carácter comercial, las personas tanto físicas como jurídicas, pueden decir: "no tengan información sobre mi si no la necesitan",

Debemos completar la legislación para estar dentro de un sistema de nivel adecuado garantizando la protección total de los datos personales.

A pesar de existir información en los organismos públicos como el Poder Judicial, que es pública por su ubicación, también es privada por pertenecer al ámbito del derecho a la intimidad y de la privacidad de las personas ✧

**** La Dra. Esc. Beatriz Rodríguez Acosta es Directora de Jurisprudencia de la Suprema Corte de Justicia***

El Comité de Redacción de la Revista Iberius agradece la generosa y desinteresada colaboración de todos aquellos que han hecho posible esta nueva edición.

Por mas información sobre la Revista:

Red Iberius:
www.iberius.org

gestión.iberius@cgpj.es

Comité de Redacción: