La Protección de Datos de Carácter Personal como Derecho Humano

The protection of personal data as a human right

Marcelo Richter [1]

Resumen

La protección de datos de carácter personal representa el reconocimiento de un derecho humano que se desarrolla a partir de la evolución de la tecnología. La dignidad del individuo, al igual que su intimidad y su honor deben ser resguardados de los usos indebidos que se pueden hacer de los datos de carácter personal que se encuentran en bancos de datos, tanto de carácter público como privado. Los distintos Estados, en la búsqueda de consolidar las libertades públicas, han diseñado distintos mecanismos para proteger a sus ciudadanos, y la legislación de protección de datos de carácter personal es uno de los instrumentos para que el individuo tenga garantizada su intimidad y su dignidad personal. La promoción y defensa de este derecho humano (protección de datos de carácter personal) consolida las libertades que son necesarias en un Estado Constitucional y Democrático de Derecho.

Palabras claves

Derechos humanos. Protección de datos de carácter personal. Tecnología. Datos de carácter personal. Habeas data. Principios para protección de datos de carácter personal. Honor. Intimidad. Dignidad Personal. Red Iberoamericana de protección de datos.

Abstract

[1] MARCELO PABLO ERNESTO RICHTER. Profesor, destacándose en el dictado de diversas cátedras vinculadas al Derecho Constitucional y al Derecho del Trabajo y de la Seguridad Social en las siguientes entidades: Centro Interamericano de Estudios de Seguridad Social (CIESS), San Carlos de Guatemala, Rafael Landívar, Galileo, Mariano Gálvez y del Istmo. Es conferencista habitual para entidades públicas y privadas y en foros nacionales e internacionales en temas referidos al Derecho del Trabajo y la Seguridad Social, al Derecho Constitucional y Derechos Humanos. Abogado Asesor de Magistratura en la Corte de Constitucionalidad. Ex Director Ejecutivo del Instituto de Justicia Constitucional. Autor de textos y artículos especializados en las materias de las que también es conferencista.

The protection of personal data represents the recognition of a human right that is developed from the evolution of technology. The human dignity, like the people's privacy and honor must be protected from misuse that can be made of the personal data found in databases, both public and private. Some States, seeking to consolidate public freedoms have designed different mechanisms to protect its citizens, and legislation for the protection of personal data is one of the instruments for which the individual has guaranteed their privacy and personal dignity. The advocacy of this human right (protection of personal data) consolidates the freedoms that are necessary in a constitutional and democratic state of law.

Key words

Human rights. Protection of personal data . Technology . Personal data . Habeas data. Principles for protection of personal data . Honor. Privacy . Personal dignity. Iberoamerican network of data protection .

Sumario

1. Generalidades.

Para el Derecho, como para otras ciencias, el mundo cambió, -aunque sólo una pequeña parte de la humanidad goce del privilegio de contar- con las nuevas tecnologías de la comunicación para fomentar el desarrollo de su vida.

La inmediatez en el traspaso de la información demuestra en la práctica la inexistencia de

las fronteras en los términos políticos que conocíamos hasta ahora. Los seres humanos realizan o confeccionan y, además, se incorporan a cientos de registros. La individualización y anotación con nombre y apellido, su estado civil, su residencia o domicilio, se expide una acta de nacimiento, se produce el otorgamiento de un documento de identidad numerado, la extracción de fichas dactiloscópicas, la obtención del pasaporte, la confección de la ficha de ingreso laboral, la apertura de cuentas corrientes o cajas de ahorro bancarias, las fichas de ingreso a un club social o deportivo, se establece un récord escolar o universitario, y tantas otras más, que implican la existencia de una serie de datos personales que, merced al avance tecnológico, se encuentran interconectados. Es por ello que dichas informaciones implican una serie de datos que sin previa autorización de su titular podrían ser mal utilizados.

El avance de la tecnología, la acumulación de datos y lo que se conoce como la cibercarretera, transmiten, casi necesariamente, un exceso de información. Este proceso incontrolable de producción, acceso, distribución y acumulación de datos ha dejado a las personas desprotegidas y a merced del uso que le quiera dar el poseedor de éstos, por lo tanto se ha creado la necesidad de regularlos.

El poder informático se ha desarrollado de tal manera que ha producido consecuencias negativas. Nuestra hoja de vida puede ser manejada por intereses malintencionados o impúdicos que solicitan datos de personas para fines indebidos con el objeto de dañar la conducta, la carrera profesional, el honor y la moral. Como consecuencia de las acciones referidas, en varios países de la comunidad internacional se creó la institución del hábeas data para proteger la información de personas que están en manos de otros. Es una acción iniciada por los particulares para que se preserve su derecho humano a la intimidad. Tiene, como intención principal, proteger de los abusos, excesos y arbitrariedades que con el mal uso de la información pudieran lesionar los derechos de la personalidad, como otros derechos constitucionales motivados por una información tergiversada, falsa o discriminatoria que conste en un registro o banco de datos. Es la respuesta jurídica para proteger la información personal tomando conocimiento de datos propios en poder de otros.

Toda persona tiene derecho a la información, a acceder a cualquier registro de datos, sea público o privado. Pero para tomar conocimiento de estos y en caso de existir falsedad,

manipulación o discriminación, es necesario contar con un medio legal expedito y urgente que le permitirá detener, suprimir, rectificar, modificar, actualizar, en todo o en parte, el dato en cuestión, para que se detenga la manipulación, se subsane la falsedad o el menoscabo que pudiera implicar. Esta acción no tiene por objeto limitar los avances de la ciencia sino que se vincula con el control del uso abusivo y excesivo que se le pudiera dar a esa información que puede producirle perjuicios a las personas.

La informática no ha agregado nada original a la tarea de acopiar la historia personal y patrimonial de cada uno. Pero brinda un instrumento perfeccionado, pasándose del soporte cartón, papel, fichas, libros, cuadernos y hojas, películas, fotocopiado y cintas, a la memoria de los ordenadores computarizados en donde se incorporan, relacionan y duermen ahora los datos, o bien reviven instantáneamente a voluntad de quien opera con ellos.

En los archivos en soporte papel, se acumuló toda la información atinente a la persona, desde su nacimiento a más allá de la muerte. Pero estos archivos, tenían el inconveniente de la lentitud de su confección, falta de comunicación entre sí, tardanza en la búsqueda y encuentro de lo anotado, posibilidad de reaccionar a tiempo para evitar que se comuniquen errores, etc., estas circunstancias evitaron que fuera notorio el riesgo que para el ser humano entrañaban estos registros. Es con la informática al servicio de estos repertorios donde se intensifica la potencial amenaza a la privacidad, puesto que se descubre la posibilidad de compilar información en cantidades inimaginables, pudiéndose procesar y difundir en cuestión de segundos. La máxima expresión de esta amenaza la configura Internet, que es un medio eficaz para entrelazar los datos, de manera de obtener casi instantáneamente una radiografía del individuo. Por este y otros motivos, la necesidad actual de proteger el ámbito de la privacidad.

El avance de la tecnología generó la aparición de los bancos de datos. No existe definición jurídica de banco de datos, técnicamente es un “conjunto organizado de bases de datos junto con el soporte físico y el soporte lógico para su explotación, tal como los programas de mantenimiento y actualización y los programas de gestión, administración y aplicación”.[2]

[2] Saroka, Raúl Horacio, Tesoro, José Luis, “Glosario de Informática”, Ediciones Contabilidad Moderna, Buenos Aires, República Argentina, 1984. Pág. 25.

La informática ha abierto una gama de posibilidades: a) la rapidez en el archivo y formación de datos; b) la casi instantánea transmisión de datos; c) la simultánea comunicación de todos en un acto; d) el almacenamiento completo y abarcador en poco espacio; e) la posibilidad, por lo tanto de conformar a la persona humana; f) construir una proyección del porvenir; g) comunicar al mundo de dicha realidad virtual; h) rapidez en la búsqueda y encuentro de los resultados. Estas posibilidades tienen como contracara peligros tales como: 1) recopilación de datos sensibles en instituciones no autorizadas para recabar estos datos; 2) cesión a terceros de la información, vulnerando los fines para los cuales fue recogida; 3) impedir que la persona interesada tome conocimiento de los datos que se manejan sobre ella; 4) mantener eternamente la información, sin dar lugar al llamado “derecho al olvido”.

Por todo lo mencionado, es necesario dispensarle a los datos de carácter personal una protección distinta al derecho a la intimidad en su concepción tradicional, que de una adecuada protección a la privacidad permitiendo la posibilidad del uso de los sistemas automatizados. Porque ante las situaciones descritas podríamos decir que la esfera privada no escapa a la llamada “globalización” que abarca la transmisión de informaciones y de datos, muchos de los cuales son de personas, sus cualidades sus proyectos de vida, y también de su patrimonio, esto desnuda un aspecto del ser en el que se ponen en veremos la dignidad como valor sustancial y los derechos que de ella provienen.

Constituye a esta altura de la civilización una verdad de perogrullo que quien cuenta con buena información[3], cuenta con una cuota importante de poder, y que si además tiene a su disposición tecnología apta para procesarla, multiplicarla en cantidad y calidad y transmitirla ágilmente, ese poder aumenta considerablemente.

Los pilares de este novísimo fenómeno -el “poder informático”, consecuencia palmaria de los recientes avances en materia de tecnología informática y de telecomunicaciones que provocaron la “revolución informática”- se encuentran en las libertades informativa e

[3] Valga aclarar que el vocablo "dato" alude a un elemento circunscrito y aislado (por ejemplo, nombre o nacionalidad), que no alcanza a tener el carácter de información, pues para que se trasforme en ella se requiere la interconexión de esos datos de manera que, vinculados, se conviertan en una referencia concreta (v.gr., nombre y nacionalidad). Los actuales sistemas permiten, por ejemplo, entrelazar datos seleccionados y obtener las referencias solicitadas en pocos segundos, e incluso transferir lo deseado a la computadora de quien consulta.

informática. Al realizar un análisis de los aspectos relativos a las consecuencias de la "revolución informática", es posible advertir que en el caso en que la actividad de recolección, tratamiento y transmisión de datos se dirige a información de índole personal, puede ocasionar graves perjuicios a los registrados, con lo cual, si no existe coto alguno a la actividad informática, las consecuencias para las personas incluidas en las "bases" y "bancos" de datos pueden ser catastróficas, en especial porque por medio de simples operaciones asociativas de datos es factible no sólo establecer los perfiles, sino incluso hasta desnudar aspectos íntimos de las personas registradas.

El fenómeno predescrito (como se dijo originado a partir de los efectos provocados por el almacenamiento, entrecruzamiento y transferencia de datos personales mediante tecnología informática, dado que, obviamente, el registro de antecedentes, referencias o datos relativos a las personas no constituye un fenómeno nuevo, porque archivos manuales o mecanográficos hubo siempre, pero no generaron demasiados conflictos sino hasta el advenimiento de la denominada "era de las computadoras"), comenzó a preocupar a las sociedades desarrolladas a partir de la década de los años 70 y consecuentemente dio origen a ciertas normas tendientes a regular el tratamiento de datos personales, en tren de oponer a la "libertad informática" de los registradores un haz de derechos y libertades de los registrados (o sólo uno, que pretende englobarlos, denominado "derecho a la autodeterminación informativa".), potencialmente amenazados por el uso abusivo de aquella libertad[4].

Paralelamente, la preocupación de aquellas sociedades por las restricciones indebidas al acceso a información pública, llevó a que también se establecieran ciertos principios tendientes a garantizarlo. Así ocurrió con la Freedom of Information Act norteamericana, dictada en 1966, en la cual básicamente se estableció que la información que tiene la Administración- pertenece al pueblo.

Así las cosas, se formaron dos frentes de batalla que no siempre fueron tratados de manera independiente: uno, ocupado de los avances informáticos sobre los derechos

[4] En especial, los derechos a la intimidad, al honor, a la imagen, a la identidad; de propiedad potencialmente amenazados, por ejemplo, si se dieran a conocer datos legítimamente almacenados pero que deben permanecer en reserva, como la fórmula química de un producto, la composición patrimonial o los detalles relativos a los negocios de una empresa, etc.

personales cuya meta se centraba especialmente en la limitación de la actividad de los operadores de las bases y bancos de datos en el tratamiento de datos personales, y otro, preocupado por la eliminación de límites abusivos al derecho a informarse y permitir el libre acceso y tratamiento de datos vacantes. Ambos, curiosa pero no casualmente, confluyeron a la hora del dictado de las normas sobre tratamiento de datos personales, e incluso en algunas versiones del hábeas data.

2. Concepto.

Los datos de carácter personal están definidos legalmente como cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables. También se los ha definido como toda aquella información relativa al individuo que lo identifica o lo hace identificable; estos datos le dan al individuo: identidad, lo describen, establecen su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional, entre otros. Además, también describen los aspectos más sensibles o delicados del individuo, como su forma de pensar, estado de salud, características físicas, ideología y vida sexual, entre otros aspectos distintivos.

De acuerdo a las distintas legislaciones que han atendido el tema, y también a la evolución de la materia, se puede afirmar que existen diferentes categorías de datos, como por ejemplo, los conocidos como **de identificación** (nombre, domicilio, teléfono, correo electrónico, firma, fecha de nacimiento, edad, nacionalidad, estado civil, etc.); los **laborales** (puesto, categoría o escalafón, domicilio, correo electrónico y teléfono del trabajo); los **patrimoniales** (información fiscal, historial crediticio, tarjetas de crédito y de debito, cuentas bancarias, ingresos y egresos, etc.); los **académicos** (trayectoria educativa, títulos, certificados, etc.); los **ideológicos y filosóficos** (creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas); los **de salud** (estado de salud, historial clínico, enfermedades padecidas, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, etc.); aquellos que definen **características personales** (tipo de sangre, ADN, huella digital, etc.); los que representan **características físicas** (color de piel, iris y cabellos, señales particulares, etc.); y, finalmente, los que configuran vida y hábitos

sexuales, origen (étnico y racial.); entre otros.

3. ¿Cuáles son los principios que rigen la protección de datos de carácter personal?

Los principios relativos a la protección de datos de carácter personal, se pueden definir como aquellas reglas mínimas que deben observar, tanto las entidades gubernamentales como las empresas o entes privados que utilizan datos personales (sea de personas físicas o morales), por medio de los que se garantiza un uso adecuado de la información personal. Los principios de la materia más reconocidos son los siguientes: licitud, consentimiento, calidad, información, proporcionalidad y responsabilidad.

Principio de la Justificación Social. Esto implica que la recolección de datos deberá tener un propósito general y usos específicos socialmente aceptables.

Principio de Licitud. Se refiere al compromiso que deben asumir tanto las entidades gubernamentales como los entes privados que accedan y manejen información personal cuando un individuo solicita la prestación de un bien o servicio, obligándose a respetar, en todo momento, la confianza que el propietario de la información deposita en las entidades a quien se las cede, para su buen uso, dentro de lo que establece el orden jurídico del Estado.

Principio de la Limitación de la Recolección. Esto significa que existe una serie de datos cuya recolección debe prohibirse, salvo excepciones justificadas, como por ejemplo datos referentes a la raza, religión, salud, costumbres sexuales, opiniones políticas, usos de estupefacientes, etc. Fuera de estos datos sensibles, la recolección de otros datos debe ser con autorización, conocimiento y consentimiento del interesado, y deberá limitarse al mínimo necesario para alcanzar el fin perseguido con la recolección de cualquier tipo de datos personales.

Principio de la Especificación del Propósito o la Finalidad. Esto implica que al recolectarse los datos, debe especificarse la razón o finalidad de aquélla, impidiendo que los datos puedan usarse con fines distintos para los cuales se señaló como razón para la recolección.

Principio de Consentimiento. Debido a que todos los individuos son propietarios de los datos de carácter personal, este principio les permite decidir de manera informada, libre,

inequívoca y específica si quiere compartir su información con otras personas. Para las entidades públicas o privadas que la posean, implica el deber de solicitar tu autorización o consentimiento para que pueda disponer de la información que te concierne, sobre todo cuando se trata de datos sensibles que afectan la esfera más íntima del ser humano. En algunas legislaciones se exige que quienes van a utilizar los datos personales almacenados, le soliciten a su propietario su consentimiento de manera expresa y por escrito. Adicionalmente, deberán implementar medidas de seguridad muy estrictas que eviten quebrantar la confidencialidad, integridad y disponibilidad de esos datos.

Principio de Calidad o Fidelidad de la información. Conforme a este principio, los datos recolectados deben ser verdaderos, de tal suerte que no produzcan una falsa imagen de la persona. Por ello es que las legislaciones deben permitir el acceso para su verificación, y poder rectificar, anular o actualizarse cualquier dato que no corresponda a la realidad. Los datos de carácter personal que se encuentren en posesión de entes gubernamentales o empresas privadas deben estar actualizados y reflejar con veracidad la realidad de la información, esto con el objeto de que la existencia de cualquier inexactitud no afecte a su propietario. Asimismo, implica que el tiempo que las entidades referidas conserven los datos de uno o varios individuos, no debe exceder más allá de lo necesario para el cumplimiento de los fines que justificaron su recolección y utilización. Si se produce la circunstancia de que se ha cumplido íntegramente la finalidad para la que se proporcionaron, recolectaron y usaron los datos, su tratamiento deja de ser necesario y, por lo tanto, aquellas que los poseen deben cancelarlos.

Principio de Información. Se refiere a la potestad que se le otorga al propietario de los datos para conocer previamente las características esenciales respecto de la utilización que se le efectuará a los datos personales que aquel proporcione a un ente privado o gubernamental. Esto significa que, las empresas y las oficinas públicas deben dar a conocer esas características por medio de lo que se conoce como “aviso de privacidad”.

Principio de Proporcionalidad. Las entidades mencionadas sólo podrán recabar los datos estrictamente necesarios e indispensables para la finalidad que se persigue y que justifica su tratamiento.

Principio de Responsabilidad. Quienes traten datos personales deben asegurar que sea dentro o fuera del país, se cumpla con los principios esenciales de protección de datos

personales, y se deben comprometer a velar siempre por el cumplimiento de estos principios y a rendir cuentas en caso de incumplimiento.

Principio de Confidencialidad. Esto significa que el acceso a la información por parte de terceros, sólo será posible si lo consiente el propio sujeto de la información, o por mandato judicial. Indudablemente puede distinguirse cuando los datos se proporcionen sin especificar, ni identificar al sujeto, y ello puede ocurrir cuando se realiza un estudio de carácter estadístico, en cuyo caso no acarreará sanción alguna.

Principio de Salvaguardia de Seguridad. A través de este principio se establece la obligación, por parte del responsable del registro, de adoptar las seguridades adecuadas para proteger la información contra posibles pérdidas, destrucciones o acceso no autorizado. Inclusive puede disponerse la posibilidad de destruir la información en circunstancias especiales, como en los casos de guerra, por ejemplo.

Principio de Política de Apertura. Se garantiza a través de este principio la transparencia de la acción de la administración pública o privada respecto de los procedimientos y prácticas concernientes al procesamiento de datos personales. Por ello deben ser de conocimiento público la existencia, fines, usos y métodos de operación de los registros de datos personales.

Principio de Limitación en el Tiempo. Los datos deben conservarse sólo hasta el cumplimiento de la finalidad para la cual fueron recolectados. Cumplida la finalidad, la información debe ser cancelada, salvo casos excepcionales.

Principio de Control. Se debe prever un organismo de control, responsable de la efectividad de los principios enunciados. Tanto la ley danesa, como la francesa, prevén organismos especiales. La primera crea una inspección de registros, y la segunda la Comisión Nacional de la Informática y las Libertades.

Principio de Participación Individual. Consagra el derecho de acceso de las personas al registro de datos donde se haya recolectada información sobre su vida personal o familiar.

4. Evolución, características y categorías de las acciones reconocidas para la tutela de datos personales

Al iniciar este trabajo, se aseveró que los Estados han adoptado diversas formas para encarar la problemática que representa el uso de datos de carácter personal por quienes

no son sus propietarios. Una de las formas más conocidas, fue la creación del instituto conocido como hábeas data, en sus diferentes facetas y con sus características distintivas. En este pasaje se pretende destacar las tres grandes etapas por las que este ha atravesado, si se considera la rápida evolución que ha experimentado:

A) Etapa de Origen: Corresponde al Parlamento del Land de Hesse, en la República Federal de Alemania, el mérito de haber promulgado el primer texto legal de protección de datos: la Datenshutz del 7 de octubre de 1970. Esta ley pionera, marcó el comienzo de un recorrido que culminaría en la Datenshutz federal alemana, promulgada el 27 de febrero de 1977. El objeto y ámbito de esta última norma se centran en la protección de datos, que tienen como fin impedir la lesión de bienes dignos de tutela de las personas interesadas, garantizando los datos relativos a su persona, de abusos cometidos con ocasión de su almacenamiento, transmisión, modificación o cancelación (elaboración de datos). El eje de la ley federal, al igual que su antecesora de Hesse, viene constituido por la figura del comisario federal para la protección de datos (Bundesbeauftragter fur den Datenshutz), a quien le corresponde velar por el cumplimiento de la norma y recibir las quejas de los eventuales perjudicados. También corresponde a esta primera etapa, la Data Lag sueca, del 11 de mayo de 1973. En esta norma se establece el principio de la publicidad de los bancos de datos personales informatizados, mediante un registro abierto a la consulta de las personas en él incluidas.

B) Etapa de desarrollo legal: Con la promulgación de la Privacy Act, estadounidense, del 31 de diciembre de 1974, se inicia un nuevo ciclo en el desarrollo de las leyes de protección de datos. La adopción de la Privacy Act debe ser relacionada con la preocupación que se creó en el Congreso de los Estados Unidos con el escándalo del Watergate, y el temor sobre el uso que el gobierno puede hacer de los ordenadores y sistemas informatizados. La existencia de esta ley federal no prohíbe a los Estados federados adoptar otros casos normativos sobre el tema, siempre que no sean contrarios a las disposiciones de la Privacy Act, o que supongan una carga comercial a los otros Estados de la Unión. Así, entonces, diez Estados federados han adoptado disposiciones normativas sobre protección de datos, sin que ninguno de ellos tenga disposiciones legales que cubran el sector público y al privado. El núcleo de la ley federal reside en la protección de los individuos frente al asalto a su intimidad (assault on privacy) por los

sistemas de acopio y almacenamientos de datos derivados del uso de la tecnología informática por las agencias federales, es decir, los bancos de datos de la administración federal. Para defender a los ciudadanos ante estas posibles injerencias en su intimidad, la Privacy Act garantiza el derecho de información y acceso que tiene toda persona respecto a aquellos datos que le conciernen, así como las facultades para rectificar las informaciones erróneas y cancelar las indebidamente procesadas. En este ciclo, se ubica también la ley francesa del 6 de enero de 1978, relativa a la *Informatique aux fichers et aux libertés*. Uno de los aspectos centrales de esta norma reside en definir los datos personales como "informaciones que permiten, directa o indirectamente identificar a la persona física a que se refieren, con independencia de que su procesamiento haya sido por una persona física o moral". Al igual que el sistema germano, la ley francesa prevé un órgano público para ejercer el poder de policía específico. Sin embargo, a diferencia del sistema de los comisarios para la protección de datos de las leyes alemanas, en Francia se ha optado por una institución de estructura colegiada: La *Comisión Nationale de l'Informatique et des Libertés*. Gran Bretaña promulgó su Data Protection Act. La orientación medular del texto británico se cifra en su carácter realista. Se trata de una norma que ha optado deliberadamente por una solución de compromiso entre su finalidad de garantía de las libertades y su objeto concurrente de no obstaculizar el desarrollo del sector informático. El conjunto de facultades y derechos que configuran la libertad informática se hallan diseminados en el articulado del texto y responden a los postulados del Convenio 108 del Consejo de Europa, lealtad y legitimidad de los procedimientos de obtención de datos, determinación de su finalidad y uso conforme a ella, actualización, seguridad de su conversación y reconocimiento del derecho de acceso a las personas concernidas. La ley británica no prevé, en principio, la posibilidad de extender sus garantías a las personas jurídicas. "Su artículo 1 señala, de forma expresa, que a los efectos de la tutela prevista en las disposiciones de la ley, se entenderá por dato personal el conjunto de informaciones referentes a un "individuo vivo". La Data Protection Act excluye también de su ámbito a los ficheros manuales al circunscribirse a los sistemas automatizados".[5]

[5] Ekmekdjián, Miguel Ángel y Pizzolo, Caloggero, "Hábeas Data: El Derecho a la Intimidad frente a la Revolución Informática", Editorial Depalma, Buenos Aires, República Argentina, 1998. Pág. 115.

C) Etapa de expansión: Es la etapa actual, en la cual un creciente número de Estados e instituciones la asumen como una nueva libertad, tan importante como los derechos procedentes. La globalización de la información y la informática han exigido que se busquen formas más eficientes para proteger la libertad de información pero a su vez se garantiza el derecho a la privacidad e intimidad en una sociedad interconectada. Esta etapa está marcada por los acuerdos multilaterales para proteger estas libertades, en el caso de la Unión Europea y los propios organismos internacionales como la ONU y la UNESCO.

Existe una clasificación formulada por Néstor Pedro Sagüés, que es citada recurrentemente por distintos autores, fallos y por la doctrina especializada y comparada. Conforme lo explica el autor mencionado[6], el instituto de hábeas data admite ciertas variables enunciadas. Conviene clasificarlas, dice, teniendo en cuenta también, otras modalidades que pueden surgir de la experiencia jurídica contemporánea.

Oscar Raúl Pucinelli[7], manifiesta que la clasificación de los diversos tipos y subtipos de hábeas data (los que coexisten la mayoría de las veces en una misma norma), se relacionan directamente con el objetivo que cada uno persigue, y con el derecho que el sujeto activo pretende esgrimir a través de él. Desde ya, dice Pucinelli, que el hábeas data ha sido concebido principalmente para tutelar a los derechos de los particulares frente a quienes colectan, tratan o distribuyen (ya sea otros particulares o el Estado), y que se encuentra más perfeccionado para aquel fin que para su otra versión, que pretende brindar una herramienta efectiva, tanto a quienes colectan información, ante la negativa injustificada de acceso a las fuentes de información pública, como a la sociedad, que también cuenta con el derecho a informarse a través de quienes, luego de recabada la información, la proyectarán hacia ella.

Afirma Pucinelli, refiriéndose al caso argentino, el tema relativo a los datos personales y al acceso a la información pública, ha tenido regulaciones diversas: Mientras algunas de las provincias consideraron en sus constituciones sólo un aspecto de la protección de aquellos datos, ocupándose de los antecedentes policiales y penales (La Rioja, Salta y San Juan), o de establecer el derecho de acceso a las fuentes de información (Catamarca

[6] Sagüés, Néstor Pedro, “Subtipos de Hábeas Data”, Jurisprudencia Argentina, 1995 -IV-. Págs. 352 a 354.
[7] Pucinelli, Oscar Raúl, “Tipos y subtipos de hábeas data”, La Ley, 1997 -D- República Argentina. Pág. 222.

y Formosa; además de Río Negro y San Luis, que por otra parte, también regularon el hábeas data); otras fueron más allá, consagrando al hábeas data como una acción específica de garantía (Ciudad Autónoma de Buenos Aires, provincia de Buenos Aires, Córdoba, Chaco, Chubut, La Rioja, Jujuy, Río Negro, San Luis, San Juan y Tierra del Fuego, aunque con diseños bien diversos). Además de la regulación constitucional, o en lugar de ella, algunas provincias asumieron el tema de la legislación subconstitucional (Tucumán, Neuquén y Jujuy).

Volviendo a la opinión de Néstor Sagüés, las categorías por él establecidas son las siguientes:

A) Informativo: Sagüés llama hábeas data informativo, al que respondiendo al objeto originario de este proceso constitucional, procura solamente recabar información obrante en registros o bancos de datos públicos o privados destinados a proveer informes.[8] Del hábeas data informativo existen tres subtipos: el exhibitorio, el finalista y el autoral.

A.1) Exhibitorio: Esta forma responde a la pregunta ¿qué se registró? Tiene por fin, evidentemente, y en palabra de los doctrinarios, "tomar conocimiento de los datos" referidos a la persona que articula el hábeas data.

A.2) Finalista: Su meta es saber ¿para qué? y ¿para quién? Se registran los datos. Emerge, además de para qué tomar conocimiento de los datos, para conocer la finalidad de ellos.

A.3) Autoral: Este subtipo, dice Sagüés, no es tan habitual ni en la doctrina ni en el derecho comparado. Su propósito es inquirir acerca del productor, del gestor y del distribuidor de datos. Si la norma declara que "no podrá afectar el secreto de las fuentes de información periodística" mediante un hábeas data, parecería que si es factible a través de esta acción preguntar por las fuentes de información no periodística y sobre las que no pese jurídicamente otro tipo razonable de secretos de fuentes. Abonando esta postura, la Constitución de la provincia de San Luis enuncia el derecho de los habitantes para averiguar la fuente de información en que se obtienen los datos respectivos.

Pucinelli indica que este subtipo de hábeas data se encuentra regulado expresamente en las siguientes constituciones: Argentina, Brasil, Colombia, Paraguay y Perú. También lo

[8] Artículo 43 de la Constitución de la República Argentina. Artículo 2 inciso 5 de la Constitución de la República de Perú.

prevé expresamente la Constitución de Portugal, y en el plano de las autonomías locales argentinas, se encuentra regulado por las constituciones de Buenos Aires (Ciudad Autónoma y provincia), Córdoba, Chaco, Chubut, Jujuy, Río Negro, San Juan, San Luis y Tierra del Fuego.

B) Por Omisión: En este subtipo, el propósito es agregar más datos a los que debería constar en el respectivo banco o base. El caso más común es de poner al día información atrasada (por ejemplo, si alguien aparece como deudor habiendo satisfecho su obligación, o aparece como encausado habiendo sido en definitiva sobreseído).

En tal sentido está previsto en el artículo 43 de la Constitución de la Nación Argentina, como mecanismo para actualizar información. Pero también existe otra hipótesis de inclusión por hábeas data que no significa necesariamente actualización. Sagüés cita a Oscar Pucinelli, quien habla de un objetivo de inclusión de datos de un hotel omitido en la guía turística oficial. Añadimos, dice Sagüés, la no inserción de antecedentes pertinentes en el legajo de un docente o funcionario. El hábeas data aditivo, conforme lo sintetiza Sagüés, es un hábeas data por omisión.

C) Rectificador: Apunta a corregir errores en los registros del caso, esto es, a sanar datos falsos. Corregir el dato que manifiestamente contradice una evidencia y mal informa sobre la naturaleza o cualidades de una persona.

D) Reservador: Este subtipo busca asegurar la confidencialidad de ciertos datos. En tal caso, el dato es cierto y no hay obstáculos para su conservación por parte del registro respectivo, pero sí puede causar daños su divulgación, y por ende se ordena al titular del registro que lo mantenga en sigilo, para su uso personal exclusivo o para su empleo específico para los fines legales pertinentes. No obstante, si media un interés público relevante en la transmisión de esos datos, tal interés puede vencer la valla que significa el perjuicio por la difusión (por ejemplo, la comunicación de antecedentes penales).

E) Cancelatorio o Exclutorio: Se refiere a la denominada información sensible, concerniente a ideas políticas, religiosas o gremiales, al comportamiento sexual, a ciertas enfermedades o actos de contenido racial, todos ellos potencialmente discriminatorios o lesivos del honor o privacidad del afectado.

No existe una regla fija acerca de cuándo es procedente un hábeas data para reservar y cuándo el contenido peligroso de esa información es tan grande que corresponde borrarla.

Dice Sagüés que el criterio delimitador al respecto es cambiante de pueblo en pueblo y de momento a momento. Datos que otrora no eran vistos como nocivos (los referidos a la identificación étnica de una persona), asumen hoy, en ciertas sociedades, rasgos tan negativos, que parece indispensable eliminarlos en los bancos de datos. En última instancia, será la judicatura la que deberá precisar el concepto indeterminado de información sensible.

Pucinelli, en cambio, no comparte que se trate solamente de datos sensibles, y manifiesta: "Nosotros preferimos incluir en este tipo a otra clase de información, que no entrando en el catálogo de sensible, de todas formas no puede ser almacenada por cualquier registro (como ocurre con las fórmulas de determinadas sustancias), pues si bien alguno las podrá contener de manera reservada, en los casos en que no se trata de un registro habilitado para ello, no bastará con confidencializarla, sino que es imprescindible su eliminación".[9]

Este tipo, dice Pucinelli, se encuentra regulado expresamente en las constituciones de Argentina y Paraguay. También lo prevé expresamente la Constitución de Portugal, aunque limitado al caso de la informática.

Para concluir con todo el panorama de clasificación del hábeas data, indica Sagüés, que desde luego un hábeas data puede ser mixto, en el sentido de comprender un objetivo simplemente exhibitorio o pretender, también, actualizar, rectificar, reservar o excluir datos concernientes a la información que obre en un registro.

5. Objetivos de la protección de datos de carácter personal.

El objetivo que se persigue con el resguardo de datos es brindar una protección especial al derecho a la intimidad, el cual consideramos una derivación del derecho a la dignidad.[10]

En definitiva, evitar que el uso incorrecto de la información pueda lesionar el honor, el buen nombre y el ámbito de privacidad de la persona, como consecuencia de la difusión de datos erróneos, incompletos o inexactos. Es necesario destacar, además, que para este cometido se requiere la existencia de cinco objetivos principales:

A) Que una persona pueda acceder a la información que sobre ella conste en un registro o

[9] Op. Cit., 11, Pág. 222.

[10] Ekmekdjián, Miguel Ángel, "Manual de la Constitución Argentina", Editorial Depalma, Buenos Aires, República Argentina, 1996. Pág. 42

banco de datos;

B) Que se actualicen los datos atrasados;

C) Que se rectifiquen los inexactos;

D) Que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros; y

E) Supresión en los procesos de obtención de información del requisito de la llamada información sensible, entre la que cabe mencionar la vida íntima, ideas políticas, religiosas o gremiales, entre otras.

Los objetivos más importantes son el reconocimiento de los derechos de acceso y control de datos, y derecho a accionar en los casos en que la ley lo prescribe.

6. El bien jurídico tutelado.

El objeto tutelado coincide con la intimidad y la privacidad de la persona, debido a que todos los datos referidos a esta que no tienen como destino la publicidad o la información innecesaria a terceros necesitan preservarse.

La intención al proteger los datos personales es que se pueda accionar contra los bancos de datos que posean aquellos que sean total o parcialmente inexactos o discriminatorios, y también contra los datos obsoletos o los que deban permanecer reservados.

La aludida finalidad protectiva se dispone para fines específicos: la garantía del derecho al honor y a la intimidad de las personas y el acceso a la información que sobre estas se registre. La declarada garantía de estos derechos conlleva asumir la estrecha relación entre los datos de carácter personal y los derechos al honor y a la intimidad y, en especial, muy estrechamente con este último (sin desconocerse las indudables relaciones con el derecho de la dignidad personal, de mayor espectro y alcance). La referencia al derecho a la dignidad que se formula se encuentra justificada, si este resulta un concepto relativamente nuevo que opera como eje del cual dimanan otros derechos fundamentales, y que incluso se ubica en una dimensión superadora de esos derechos. “La tutela encuentra también sus raíces en el reconocimiento de la dignidad humana, que exige el

respeto del ser humano más allá de sus manifestaciones corpóreas, a través del reconocimiento de su intimidad, honor, etc.”.[11]

7. La Red Iberoamericana de Protección de Datos

La Red Iberoamericana de Protección de Datos (RIPD), surge como motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en la ciudad de Antigua, República de Guatemala, que se desarrolló del uno al seis de junio de dos mil tres, con la asistencia de representantes de catorce países de Iberoamérica. Esta iniciativa, referida a la protección de datos de carácter personal, contó desde sus inicios con un apoyo político reflejado en la Declaración Final de la XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos celebrada en Santa Cruz de la Sierra, Estado Plurinacional de Bolivia, los días catorce y quince de noviembre del año dos mil tres, estando conscientes los representantes políticos del carácter de la protección de datos personales como derecho fundamental, así como de la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos.

La Red aludida, se configura desde sus orígenes como un foro integrador de los diversos actores, tanto del sector público como privado, que desarrollen iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos, así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, considerando la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho. La actividad de la Red, de acuerdo a la opinión de sus representantes, ha sido intensa y fructífera, promoviendo el desarrollo de diez encuentros, uno por año, y de otros tantos seminarios sobre los más variados temas de interés: protección de datos de los menores; datos de salud; sector financiero (fraude); sector comercial y marketing, en especial la lucha contra el Spam; las nuevas tecnologías y su impacto sobre la privacidad;

[11] Peyrano. Guillermo F., “Régimen Legal de los Datos Personales y Hábeas Data. Comentario a la ley 25326 y a la reglamentación aprobada por Decreto 1558/2001”, Editorial Lexis Nexis - Depalma, Buenos Aires, República Argentina, 2002. Págs. 21 y 22.

transferencias internacionales, etc. Esta trayectoria ha llevado a que la Red se haya consolidado como principal promotor del diálogo e impulsor de iniciativas y políticas en la región, que ha significado que más de ciento cincuenta millones de ciudadanos de Iberoamérica dispongan en la actualidad, junto al tradicional amparo de habeas data, de normas que permitan garantizar eficazmente el uso de su información personal y de autoridades especializadas con competencias para tutelar esas garantías. Ejemplos significativos del avance normativo producido en la región durante el funcionamiento de la Red, se encuentran en países como Argentina (Ley 25326/2008), Uruguay (Ley 18331/2008), Perú (Ley 29733/2011), Costa Rica (Ley 8968/2011), Nicaragua (Ley 787/2012), y Colombia (Ley 1581/2012), que ha sido la última en incorporarse al grupo de países que disponen de una normativa específica en esta materia.

En definitiva, es interés primordial de las instituciones que en la actualidad constituyen la Red Iberoamericana de Protección de Datos, seguir impulsando el desarrollo del Derecho Fundamental a la Protección de Datos de Carácter Personal por medio de las entidades con capacidad y competencias para instar a los gobiernos nacionales a que elaboren una regulación normativa en esta materia, a efectos de lograr la obtención de la Declaración de Adecuación por parte de la Comisión Europea.

Los miembros de la Red son los siguientes: Principado de Andorra, República Argentina, Estado Plurinacional de Bolivia, República Federativa de Brasil, República de Chile, República de Colombia, República de Costa Rica, República de Ecuador, República de El Salvador, Reino de España, República de Guatemala, República de Haití, República de Honduras, Estados Unidos Mexicanos, República de Nicaragua, República de Panamá, República de Paraguay, República de Perú, República de Portugal, República Dominicana, República Oriental del Uruguay, y República Bolivariana de Venezuela.

8. La protección de datos de carácter personal en Guatemala

Por las características particulares de la sociedad guatemalteca, la necesidad que se consideró primordial fue la de tener acceso a la información, aunque este derecho siempre genera tensión con el de protección de datos personales. Por ese motivo, se consideró que el sistema constitucional guatemalteco, le reconoce a los habitantes del país, en forma expresa e implícita, una serie de derechos fundamentales, entre los que se encuentra el

acceso a la información pública. Este último es considerado como un derecho vinculado en forma muy estrecha con el ejercicio de la libertad de expresión de ideas, al que las autoridades públicas le deben prestar una atención y protección especial. El derecho de acceso a la información está consagrado en los artículos 19 de la Declaración Universal de Derechos Humanos; 19, inciso 2), del Pacto Internacional de Derechos Civiles y Políticos; 13, inciso 1), de la Convención Americana sobre Derechos Humanos; 30, 31 y 35, párrafo quinto, de la Constitución Política de la República; y 5 de la Ley de Emisión del Pensamiento. Sin embargo, el reconocimiento mencionado no ha significado el ejercicio efectivo de este derecho, debido a que un gran número de funcionarios y empleados públicos se resisten o se oponen a que los ciudadanos accedan libremente a los archivos, registros y expedientes públicos.

El veintitrés de septiembre del año dos mil ocho, el Congreso de la República de Guatemala, sancionó el Decreto 57-2008, Ley de Acceso a la Información Pública, norma que fue publicada en el Diario de Centro América (Diario Oficial) el veintitrés de octubre, también de dos mil ocho. De conformidad con el artículo 72 de la Ley referida, esta entró en vigencia ciento ochenta días después de su publicación en el Diario Oficial.

La entrada en vigencia del Decreto mencionado, constituyó un gran avance para fomentar y fortalecer la búsqueda de transparencia en la función pública, el combate a la cultura de opacidad, la necesidad de participación ciudadana en la vida y en los asuntos públicos, la responsabilidad de la administración pública, y en términos generales, una importante herramienta con miras a la consolidación de la vida democrática y republicana del país.

Ese cuerpo normativo atribuye al Procurador de los Derechos Humanos la calidad de autoridad reguladora en esta materia. Además, por su naturaleza de derecho fundamental, este tema corresponde al mandato constitucionalmente establecido al reconocido como Comisionado del Congreso de la República. El derecho humano de libre acceso a la información o el derecho a saber, parte del principio de que la información pertenece a los ciudadanos, es pública por principio y le corresponde al Estado por medio de sus instituciones el adecuado manejo para su disponibilidad y transparencia. Este derecho le permite a la población un mejor nivel de toma de decisiones, al contar con información accesible, certera y oportuna.

En el artículo 1 de la ley que se analiza, establece que su objeto, entre otros, es:

1) garantizar a toda persona interesada, sin discriminación alguna, el derecho a solicitar y a tener acceso a la información pública en posesión de las autoridades y sujetos obligados por la ley;

2) garantizar a toda persona individual el derecho a conocer y proteger los datos personales de lo que de ella conste en archivos estatales, así como de sus actualizaciones; y

3) garantizar la transparencia en la administración pública y de los sujetos obligados y el derecho de toda persona a tener acceso libre a la información pública. Como se advierte, de los tres objetivos señalados, el segundo está íntimamente relacionado con la protección de datos de carácter personal, en lo que se considera como desarrollo de una sociedad democrática.

En el artículo 3 de la Ley de Acceso a la Información Pública, se reconocen los principios que la inspiran, destacándose los siguientes:

1) máxima publicidad;

2) transparencia en el manejo y ejecución de los recursos públicos y actos de la administración pública;

3) gratuidad en el acceso a la información pública; y

4) sencillez y celeridad de procedimiento.

La ley analizada, con el fin de unificar su interpretación, en su artículo 9 ha establecido una serie de definiciones, de las que se transcribirán las que están relacionadas con el instituto del hábeas data. Las más relevantes son:

A) Datos personales: los relativos a cualquier información concerniente a personas naturales identificadas o identificables.

B) Datos sensibles o datos personales sensibles: aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o actividad, tales como los hábitos personales, el origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza.

C) Derecho de acceso a la información pública: el derecho que tiene toda persona para tener acceso a la información generada, administrada o en poder de los sujetos obligados

descritos en la presente ley, en los términos y condiciones de la misma.

D) Información pública: es la información en poder de los sujetos obligados contenida en los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico y que no sea confidencial ni estar clasificado como temporalmente reservado.

E) Hábeas data: es la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización. Los datos impersonales no identificables, como aquellos de carácter demográfico recolectados para mantener estadísticas, no se sujetan al régimen de hábeas data o protección de datos personales de la presente ley.

La regulación concreta respecto al habeas data se inicia en el artículo 30 de la Ley de Acceso a la Información Pública. En el artículo mencionado se indica que los sujetos obligados[12] de estas normas son responsables de los datos personales que contengan los registros que manejan y que no podrán usar la información obtenida para fines comerciales, salvo que hayan obtenido autorización expresa del titular de la información; y por ello deberán:

1) adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos que sean presentados por los titulares de los mismos o sus representantes legales, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos;

2) administrar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos, en relación con los propósitos para los cuales se hayan obtenido;

3) poner a disposición de la persona individual, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su

[12] Son todas las autoridades públicas que están enumeradas en la Ley de Acceso a la Información Pública y las que administren bancos de datos de carácter público.

tratamiento;

4) procurar que los datos personales sean exactos y actualizados;

5) adoptar las medidas necesarias que garanticen la seguridad, y en su caso confidencia o reserva de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

El artículo 32 de la Ley de Acceso a la Información Pública, indica que no se requiere el consentimiento del titular de la información para proporcionar datos personales en los siguientes casos:

1) Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

2) Cuando se transmitan entre sujetos obligados o entre dependencias y entidades del Estado, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

3) Cuando exista una orden judicial;

4) Los establecidos en la propia ley;

5) Los contenidos en los registros públicos;

6) En los demás casos que establezcan las leyes.

El artículo referido, también establece, pero como cuestión prohibitiva, que no se podrán crear bancos de datos o archivos con datos sensibles o datos personales sensibles, salvo que sean utilizados para el servicio y atención propia de la institución que lo hubiese creado.

El artículo 33 de la Ley analizada establece, que solamente los titulares de la información o sus representantes legales, previa acreditación de ambas circunstancias, podrán solicitar que se les proporcione los datos personales que estén contenidos en sus archivos o sistema de información. La información requerida, debe ser entregada por el sujeto obligado dentro de los diez días siguientes, contados a partir de la presentación de la solicitud, en formato o de manera que el solicitante comprenda lo que se le remita, o de la misma forma y por escrito, se le debe comunicar, que el sistema de datos personales no contiene la información que fue requerida.

De acuerdo a lo normado en el artículo 34 de la Ley referida, los particulares podrán

solicitar, de la misma forma en que se mencionó en el párrafo anterior, que se modifiquen sus datos personales contenidos en cualquier sistema de información. Para ello, el interesado debe entregar una solicitud de modificaciones, en la que deberá indicar el sistema de datos personales al que va dirigido, los cambios que desea realizar, y adjuntará los documentos que motive su petición. El sujeto obligado -la autoridad-, debe entregarle al solicitante, en un plazo no mayor de treinta días hábiles, contados a partir de la entrega de la solicitud, la resolución en la que consten las modificaciones o, un informe fundamentado, las razones o motivos por los que no procedieron los cambios requeridos.

Cuando se produzca la negativa por parte del sujeto obligado de entregar o corregir datos personales, el artículo 35 de la Ley de Acceso a la Información Pública establece, que se podrá interponer recurso de revisión, que es definido como un medio de defensa jurídica, que tiene por objeto garantizar que en los actos y resoluciones de los sujetos obligados -autoridad pública-, se respeten las garantías de legalidad y seguridad jurídica (artículo 52 de la Ley de Acceso a la Información Pública).

La norma indica en forma expresa que el recurso de revisión lo debe presentar, el interesado por sí mismo o a través de su representante legal, ante la autoridad máxima del sujeto obligado, la que será competente para resolverlo. La interposición se debe efectuar dentro de los quince días siguientes a la fecha de la notificación de la resolución que contiene la negativa del sujeto obligado de entregar o corregir datos personales. También es procedente el recurso de revisión, de acuerdo a lo normado en el artículo 55 de la Ley de Acceso a la Información Pública, en los mismos términos y plazos cuando:

1) el sujeto obligado no entregue al solicitante los datos personales solicitados, o lo haga en un formato incomprensible;

2) el sujeto obligado se niegue a efectuar modificaciones, correcciones o supresiones a los datos personales;

3) el solicitante considere que la información entregada es incompleta o no corresponda a la información requerida en la solicitud;

4) en caso de falta de respuesta en los términos de la presente ley;

5) por vencimiento del plazo establecido para la entrega de la información solicitada;

6) en los casos específicamente estipulados en la propia ley.

Es obligación de la máxima autoridad de los sujetos obligados, subsanar, en forma

inmediata, dice la ley, las deficiencias que existan en los recursos interpuestos, debido a que se debe respetar el principio de sencillez en materia administrativa (artículo 56 de la Ley de Acceso a la Información Pública).

De conformidad con lo establecido en el artículo 57 de la Ley analizada, son requisitos que debe contener el recurso de revisión:

1) la dependencia o la entidad ante la que se presentó la solicitud;

2) el nombre del recurrente y del tercero interesado si lo hay, así como el domicilio, lugar o medio que señale para recibir notificaciones;

3) la fecha en que se le notificó o tuvo conocimiento del acto reclamado;

4) el acto que se recurre y los puntos petitorios;

5) los demás elementos que considere procedentes someter a juicio de la máxima autoridad.

Es obligación de la máxima autoridad del sujeto obligado, de acuerdo a lo establecido en el artículo 58 de la Ley que se está analizando, sustanciar el recurso de revisión de acuerdo con las siguientes directivas:

1) interpuesto el recurso mencionado, la máxima autoridad deberá resolver la cuestión planteada en forma definitiva, dentro de los cinco días siguientes de su planteamiento;

2) las resoluciones emitidas por la autoridad obligada, son de carácter público.

Las resoluciones de la máxima autoridad del sujeto obligado, deben constar por escrito y establecer el plazo para su cumplimiento y los procedimientos para asegurar su ejecución; y pueden confirmar la decisión de la Unidad de Información, o también pueden revocar o modificar aquéllas decisiones y, por consiguiente, ordenar a la dependencia o entidad que permita al particular o a su representante legal, el acceso a la información solicitada, la entrega de esta o las modificaciones, correcciones o supresiones a los datos sensibles solicitados. (Artículo 59 de la Ley de Acceso a la Información).

Emitida la resolución de la máxima autoridad del sujeto obligado, en la que se declaró la procedencia o improcedencia de las pretensiones del recurrente, aquélla conminará al obligado para que dé exacto cumplimiento a lo resuelto, dentro del plazo de cinco días, bajo apercibimiento, de que en caso de incumplimiento, certificará lo conducente ante el órgano jurisdiccional competente; sin perjuicio de dictarse todas aquellas medidas de carácter administrativo y las que conduzcan a la inmediata ejecución de lo resuelto. Una

vez concluido el procedimiento de revisión, se considerará agotada la fase administrativa, por lo que contra esa resolución, el interesado, podrá interponer la acción constitucional de amparo, con el objeto de que prevalezca su derecho constitucional, sin perjuicio de que pueda iniciar otro tipo de acciones legales vinculadas con la normativa específica. La última circunstancia descrita, confirma que para el legislador guatemalteco, el hábeas data constituye un derecho que puede ser ejercido por los ciudadanos, pero no una garantía como la reconocen otras legislaciones nacionales, circunstancia que se considera negativa, en virtud de que el instituto jurídico analizado, es de mayor amplitud e importancia que el que le asignó el legislador guatemalteco.

Aunque la Ley de Acceso a la Información Pública, le reconoce al hábeas data la condición de garantía –artículo 9 de la norma mencionada-, su regulación final corresponde a la de un derecho, debido a que ante la vulneración que pueda producir un sujeto obligado –funcionario público y las entidades privadas que perciban, invierta o administren fondos públicos, incluyendo fideicomisos constituidos con fondos públicos, obras o servicios públicos sujetos a concesión o administración-, la forma de defensa ante la violación consumada es mediante el ejercicio de la acción constitucional de amparo, después de haber agotado la vía administrativa.

La legislación guatemalteca le concede legitimación para ejercer los derechos vinculados con el hábeas data a toda persona que necesite conocer o pretenda la protección de datos personales que se encuentren en archivos estatales.

La legislación nacional faculta al Procurador de los Derechos Humanos para controlar la debida aplicación de la Ley de Acceso a la Información Pública, sin embargo, en legislaciones comparadas se crean autoridades de aplicación y de control efectivo del cumplimiento de la ley que regula el hábeas data, y en algunos casos les reconoce potestades para representar a los individuos frente a los bancos de datos, públicos o privados, contra los que se inicie la acción de hábeas data. En este aspecto se advierte una diferencia que puede ser salvada o corregida mediante una futura modificación legislativa en Guatemala.

La falta de un proceso judicial para la protección de datos personales impide la revisión judicial de las decisiones adoptadas en sede administrativa, lo que en definitiva atenta

contra la posibilidad que tiene el Organismo Judicial de controlar las decisiones adoptadas por el poder administrador.

Debido a que la legislación guatemalteca –Ley de Acceso a la Información Pública-, no estableció una etapa judicial con una acción efectiva para el ejercicio de los derechos involucrados en esta materia, es poco probable que los objetivos que tiene la norma referida se cristalicen, debido a que se depende de la decisión de funcionarios públicos, que cuando se pretende fiscalizar su actuación, ejercen el poder con arbitrariedad y vedan toda posibilidad de garantizar la transparencia en la administración pública. Esta circunstancia, ha sido advertida por el Procurador de los Derechos Humanos, el que ha expresado que, entre otras circunstancias, recurrir siempre al plazo máximo establecido por la normativa –diez días- para proporcionar la información solicitada o para responder a los requerimientos del peticionante en el caso de una actualización o modificación, contraviene el espíritu de la ley; e incluso se ha afirmado, que algunas instituciones públicas utilizan el plazo de diez días para no entregar la información requerida, para solicitar y establecer prórrogas para retrasar el proceso de entrega de datos o para que aquella se proporcione en forma incompleta; circunstancias que atentan contra los principios de máxima publicidad, transparencia en el manejo y ejecución de los recursos públicos y sencillez y celeridad en el procedimiento.

En conclusión, se impone una pronta revisión de la Ley de Acceso a la Información Pública, con el objeto de introducirle modificaciones que incorporen un proceso judicial que tienda a hacer efectivo el ejercicio de los derechos que la norma mencionada pretende proteger y para que exista la posibilidad de que el Organismo Judicial controle las decisiones que adopte la administración pública y aquellos que constituyan o manejen archivos de carácter público. También es imprescindible el control sobre archivos de carácter privado, porque es en ese ámbito en el que se producen las mayores violaciones a los derechos humanos, particularmente, el relacionado con la protección de datos personales vinculados a la intimidad y honra del individuo.

Bibliografía consultada

Altmark, Daniel R. – Molina Quiroga, Eduardo. “Régimen Jurídico de los Bancos de

Datos", en Informática y Derecho, volumen 6, editorial Depalma, Buenos Aires, 2.000.
Bazán, Víctor. "El Hábeas Data y sus particularidades frente al Amparo", en Revista de Derecho Procesal nº 4, editorial Rubinzal Culzoni, Buenos Aires, 2.000.
Bianchi, Alberto B. "Hábeas Data y Derecho a la Privacidad", publicado en El Derecho, tomo 161 Págs. 866 y ss.
Bidart Campos, Germán J. "Tratado elemental de Derecho Constitucional Argentino", tomo VI, editorial Ediar, Buenos Aires, 1995.
Bidart Campos, Germán J. "¿Habeas data o qué? ¿Derecho a la verdad o qué?", en suplemento de Derecho Constitucional, Revista La Ley, del 15 de febrero de 1999, Págs. 21 y ss.
Cifuentes, Santos. "Protección Inmediata de los Datos Privados de la Persona. Hábeas Data Operativo". Revista La Ley del 15/11/95.
Dalla Vía, Alberto R., - Basterra, Marcela I. "Hábeas Data y otras Garantías Constitucionales", editorial Némesis, Buenos Aires, 1999.
Ekmekdjian, Miguel Ángel – Pizzolo, Calogero. "Habeas Data. El Derecho a la Intimidad frente a la Revolución Informática", editorial Depalma, Buenos Aires, 1996.
Estadella Yuste, Olga. "La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales", editorial Tecnos, Madrid, 1995.
Falcón, Enrique M. "Hábeas Data", editorial Abeledo Perrot, Buenos Aires, 1996.
García Belaúnde, Domingo. "El Hábeas Data y su Configuración Normativa" (con algunas referencias a la Constitución peruana de 1993), en Liber Amicorun Héctor Fix Zamudio, volumen I, editorial Secretaría de la Corte Interamericana de Derechos Humanos, San José de Costa Rica, 1998.
Gozaíni, Osvaldo Alfredo, "Derecho de Amparo", 2º edición, editorial Depalma, Buenos Aires, 1998.
Gozaíni, Osvaldo Alfredo. "La legitimación en el Proceso Civil", editorial Ediar, Buenos Aires, 1996.
Palazzi, Pablo. "El Hábeas Data en la Constitución Nacional" (La protección de la privacidad en la "era de la información"), en Jurisprudencia Argentina del 20 de diciembre de 1995.
Puccinelli, Oscar Raúl, "El Hábeas Data en Indoiberoamérica", en El Amparo

Constitucional, perspectivas y modalidades, editorial Depalma, Buenos Aires, 1999.
Quiroga Lavié, Humberto. “El Amparo Colectivo”, editorial Rubinzal Culzoni, Buenos Aires, 1998.
Romero Coloma, Aurelia María. “Los Derechos al Honor y a la Intimidad frente a la Libertad de Expresión e Información”. Problemática procesal, editorial Serlipost, Barcelona, 1991.
Velázquez Bautista, Rafael. “Protección jurídica de datos personales automatizados”, editorial Colex, Madrid, 1993.
http://www.colima-estado.gob.mx/transparencia/pagina_preview.php?idPagina=NDM= (consulta realizada el 11/10/2014)
http://cuidatusdatos.com/infodatospersonales.html (consulta realizada el 11/10/2014)
http://blog.derecho-informatico.org/faqs/datos-personales-2/datos-personales/#sthash.CdDISAvW.dpbs (consulta realizada el 11/10/2014)