LA PROTECCIÓN DE DATOS PERSONALES EN IBEROAMÉRICA

Paola Rosario Cano Revilla (Coord.)
Leonel Caraballo Leal / Xenia Soledad Díaz Martínez / Héctor Scaianschi Díaz / Beatriz Eugenia Suárez López / Arianna Marisol Rivera Pérez / Simón Joaquín Rodríguez Wilches
Alumnos del Máster Oficial en Derecho. Segunda y Tercera Edición
Universidad de Alcalá

Resumen: La Protección de datos personales es un derecho fundamental del ser humano y en la actualidad, los Países Iberoamericanos de Colombia, Perú, República Dominicana, Venezuela y Uruguay han adoptado preceptos legislativos para proteger los derechos relacionados a la intimidad de la persona. Asimismo tienen prevista la acción de Habeas Data como mecanismo de protección a estos derechos. No obstante, aunque algunos países han adoptado leyes especiales para la protección de datos personales, como Argentina, Colombia y Uruguay, y otros cuentan con una protección específica de los datos personales en sus Textos Constitucionales, tal es el caso de Colombia, Argentina y Venezuela, el resto de los países mencionados en este artículo Perú y República Dominicana podrían proveer de protección al "Derecho a la Protección de Datos Personales", como tal, a través de una inclusión constitucional y/o de una legislación especial, donde se establezca este derecho del sujeto titular de los datos personales.

Palabras clave: Protección de Datos Personales, Iberoamérica, habeas data

Abstract: The Protection of personal data is a fundamental human right being and at present, acknowledged as so in the new regulations adopted by the Latin-American Countries of Argentina, Colombia, Peru, Dominican Republic, Venezuela and Uruguay. Likewise they have established the Habeas Data as the specific legal action to claim violations to the rights of personal data protection and intimacy. Nevertheless, though some countries as Argentina, Colombia and Uruguay

count with an specific law to protect Habeas Data, and even others contempt the protection in their Constitutions, as Colombia, Argentina and Venezuela, the rest of the mentioned countries, meaning Peru and Dominican Republic, could provide protection to this right by means of incorporation of constitutional provisions and by approving special rules recognizing the right to personal data protection.

Keywords: Personal data protection, Latin America, habeas data

SUMARIO: I. INTRODUCCIÓN. II. LA PROTECCIÓN DE DATOS EN ALGUNOS PAÍSES DE IBEROAMÉRICA: 1. En Argentina: 1.1. Reconocimiento constitucional del derecho a la protección de datos; 1.2. La ley de Protección de Datos Personales: a) La formación de archivos de datos; b) Derechos de los titulares en relación a sus datos personales; 1.3. Acción de protección de los datos personales. 2. En Colombia: 2.1 Jurisprudencia Constitucional anterior a la entrada en vigencia de la Ley 1266 de 2008 (Ley de Habeas Data); 2.2 Ley 1266 de 2008, por la cual se dictan disposiciones generales sobre el habeas data. 3. En Perú: 3.1. Precepto Constitucional; 3.2. Normas o Leyes que protegen los datos personales; 3.3. Jurisprudencia Comentada y la acción de Habeas Data. 4. En República Dominicana: 4.1. Precepto Constitucional; 4.2. Normas o Leyes que protegen los datos personales; 4.3. Resolución 055-06 del Instituto Dominicano de Telecomunicaciones (INDOTEL). 5. En Venezuela: 5.1. Habeas Data como un amparo especializado; 5.2. El Habeas Data como una acción autónoma; 5.3. De la competencia para conocer de la acción autónoma de Habeas Data; 5.4. Los sujetos en el ejercicio de la acción de Habeas Data. 6. En Uruguay: 6.1. Régimen legal: a) Principios generales de la ley; b) Principales derechos de las personas; c) Datos con régimen especial: sensibles y especialmente protegidos; 6.2. Control y vigilancia del sistema de protección; 6.3. Habeas data. III. CONCLUSIONES.

I. Introducción

El presente trabajo tiene su origen en el Seminario que se celebró en la sede de la Agencia Española de Protección de Datos (AEPD) el 13 de mayo de 2009, y en el que intervinieron los alumnos del Máster Oficial

en Derecho de la Facultad de Derecho de la Universidad de Alcalá.[1] La finalidad del Seminario no era otra que dar a conocer cuál era la situación en la que el derecho fundamental a la protección de datos personales se encontraba reconocido en diferentes países latinoamericanos. Gracias al esfuerzo de ponentes invitados y de la investigación llevada a cabo por los alumnos del Máster, se evidenció el avance que el tema había experimentado en estos países.

El conocimiento y -especialmente- reconocimiento del derecho a la protección de datos personales supone un paso decisivo en toda sociedad democrática, un paso más en la garantía de libre desarrollo de las personas. Si un ciudadano no sabe qué informaciones sobre su persona se han recogido y almacenado, ni qué uso se les va a dar, no puede actuar con la misma libertad, tanto en su vida privada como en su vida en sociedad, que si supiera qué datos se han recogido, y pudiera disponer y controlar el uso que se les va a dar. Y esta idea está calando cada vez más en la sociedad iberoamericana. En los últimos años, países latinoamericanos como Argentina, Chile, Paraguay, Perú y, recientemente, Uruguay han aprobado Leyes de protección de datos personales, y otros Estados como México y Brasil están trabajando en su desarrollo.

No obstante, el reconocimiento y garantía de este derecho no siempre es fácil, pues hay que tratar de buscar un equilibrio entre los derechos de los ciudadanos y la necesidad que tienen los Estados de tener información sobre sus ciudadanos para ofrecerles sus servicios. Y aquí es donde vamos a encontrar la diferencia entre los Estados Europeos y los situados al otro lado del charco, influenciados por el ordenamiento americano. En Estados Unidos, la dispersa normativa sectorial y el poder del mercado y la seguridad ciudadana, han dejado al derecho a la protección de datos personales algo relegado. De esta forma, mientras que en los ordenamientos jurídicos europeos, como el español, la obligación de transponer normativa europea (en concreto, la Directiva 95/46/CE, sobre Protección de Datos Personales) ha contribuido a garantizar el derecho a la protección de datos personales de manera uniforme en todos los estados europeos, la situación en Iberoamérica no es la misma, pues no existe una obligación semejante.

[1] El Seminario fue abierto por el Decano de la Facultad de Derecho, D. Alfonso García Moncó, y por el Director de la Agencia, D. Artemi Rallo, y participaron como Ponentes invitados, además de los autores del presente artículo, D. Ricard Martínez Martínez (AEPD), Dña. Teresa Pereyra Caramé (de la Agencia de Protección de Datos de la Comunidad de Madrid) y D. Javier Rodríguez Navarro (de la empresa *Arentia Consultores*). El presente trabajo ha sido coordinado por la becaria del Máster Oficial en Derecho, Dña. Paola Cano Revilla.

En Iberoamérica, a diferencia de Europa, la regulación del derecho a la protección de datos personales, así como de las facultades que lo componen se encuentra dispersa en las distintas Constituciones latinoamericanas, lo que hace más complicado su reconocimiento en cada uno de sus países. Como veremos, la mayoría de ellos ha reconocido la protección a los datos personales en una normativa sectorial, pero no lo han hecho dentro de su Ley Fundamental, y menos aún, como un derecho fundamental; por otro lado, otros países lo han ido reconociendo de forma jurisprudencial; y, también, encontraremos aquéllos países que lo reconocen expresamente en su Constitución y lo desarrollan vía legislativa.

El tema es realmente relevante, sobre todo si tenemos en cuenta que vivimos en un mundo globalizado y que la informática y las telecomunicaciones rompen con las tradicionales barreras de espacio y tiempo. Todo ello influye en el comercio internacional, donde la diferente regulación de las leyes de protección de datos puede llegar a convertirse en un serio obstáculo para el movimiento de bienes, servicios y personas entre nuestro Estado e Iberoamérica. Gracias pues al trabajo y dedicación de los alumnos del Máster Oficial en Derecho.

II. La Protección de datos en algunos países de iberoamérica

1. En Argentina

1.1. Reconocimiento constitucional del derecho a la protección de datos

El derecho a la protección de datos personales (*"Habeas Data"*) se incorporó en la sección dogmática de la Constitución argentina en la reforma de 1994 como un apartado al artículo que regula la acción de amparo general.[2] De esta forma, en el esquema constitucional, la acción de *habeas data* es una subespecie o modalidad de la acción de amparo. Sin embargo, en la doctrina y jurisprudencia se pueden encontrar crite-

[2] Art. 43- Ap. 1. [Acción de amparo general]
Ap. 2. [Legitimación en defensa de intereses difusos]
Ap. 3. [Habeas data] *"Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística"*.
Ap. 4. [Habeas Corpus]

rios distintos sobre la naturaleza del derecho a la protección de los datos personales.

Un sector considera que el *habeas data* es una garantía procesal de los derechos a la intimidad y privacidad, consagrados en los artículos 18 y 19 de la Constitución, respectivamente.[3] Según esta concepción, la acción de amparo sería una garantía procesal, con tres modalidades, que apuntan a defender distintos derechos fundamentales. Por un lado, estaría el habeas corpus, como amparo contra la lesión del derecho a la libertad ambulatoria y contra las condiciones indignas de reclusión. Por otro lado, aparecería el *habeas data* protegiendo el derecho a la intimidad. Y finalmente, todos los demás derechos fundamentales, entrarían en la protección de la *acción de amparo* general.[4]

Por su parte, otra posición considera que el derecho tutelado va más allá del derecho a la intimidad y prefieren ubicarlo en la esfera más amplia de los derechos de la personalidad. Quienes mantienen esta postura han comenzada a manejar el concepto de *autodeterminación informática*.[5] Con estas tendencias se empieza a reconocer que la Constitución consagra un derecho autónomo, distinto a la intimidad; un derecho que se relaciona con la capacidad para disponer de los datos personales. En este sentido, la jurisprudencia ha considerado que el *habeas data* no protege solamente la intimidad o la privacidad con el alcance clásico de tales conceptos concluyendo que: *"habría que hacer una reformulación a la luz de la realidad y encuadrarla en el derecho a la autodeterminación informática"*.[6]

La polémica referida pude tener consecuencias prácticas de importancia. En este sentido, la caracterización del *habeas data* como una sub-

[3] Las disposiciones citadas consagran el derecho a la *intimidad*; también entendido como derecho a la privacidad o la reserva de la autonomía individual (*Vid:* BIDART CAMPOS; German; *Tratado Elemental de Derecho Constitucional Argentino*; Ediar; 2002; Bs.As.; 442). El art. 18 señala que: *"El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en que casos y con que justificativos podrá procederse a su allanamiento y ocupación"*. Por su parte, el artículo 19 establece: *"Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe"*.

[4] Al respecto; *vid.* SAFADI; Carlos; "El Hábeas Data y los estándares de privacidad en los datos médicos"; en *Derecho Procesal Constitucional*; RIVAS, A. (Dir.); Ad-Hoc; Bs.As.; 2003, pág. 242.

[5] *Vid:* Juzgado en lo Civil Nº 39 de la Ciudad Autónoma de Buenos Aires; "Cañada Pérez c/ Bank Boston; Habeas Data"; octubre de 2008 y las posiciones allí citadas de BIDART CAMPOS y VANNOSI.

[6] Juzgado en lo Civil Nº 39 de la Ciudad Autónoma de Buenos Aires; "Cañada Pérez c/ Bank Boston; Habeas Data"; octubre de 2008

especie de la acción de amparo implica la extensión de los presupuestos que se exigen para su procedencia, en particular, la ilegitimidad manifiesta.[7] Por el contrario, si se parte de la existencia de un derecho autónomo, calificable como *"derecho a la autodeterminación informática"*, su tutela por medio de la acción de habeas data puede independizarse de los requisitos de procedencia del amparo y operar de modo automático frente a cualquier utilización inexacta de los datos objeto de la tutela.

Ahora bien, aunque no existe un acuerdo sobre los caracteres del derecho tutelado por el *habeas data* (aspecto del derecho a la intimidad o derecho autónomo), en cualquier caso, su rango constitucional sí impone ciertos límites al legislador en sus facultades de reglamentación. El alcance de estos límites fue discutido en el caso: *"Halabi v. Estado Nacional"*.[8] En esa oportunidad se pidió la declaración de inconstitucionalidad de la ley 25.873 que establecía que los prestadores de servicios de telecomunicaciones debían poder captar y derivar las comunicaciones que transmiten para que pudieran ser observadas a pedido del Poder Judicial o el Ministerio Público. A su vez, también imponía a los prestadores de servicios que brindaran la identificación completa de sus usuarios y los registros de tráfico de comunicaciones cursadas por ellos. La declaración de inconstitucionalidad de la ley se basó en su falta de justificación y proporcionalidad. La ley impugnada autorizaba la intromisión sin determinar casos, ni justificativos, sin garantizar la debida intervención judicial y creaba un "*... archivo viviente del contenido de las telecomunicaciones...*". Para llegar a esta conclusión, el juez se fundó no sólo en la absoluta generalidad del texto de la ley, sino en las carencias de su trámite parlamentario. Se entendió que una ley que limite esta clase de derechos debe estar "singularmente fundada" exigencia que no cumplía la ley impugnada.[9]

[7] Al respecto, *vid:* Corte Suprema de Justicia de la Nación. Sentencia del 6 de marzo de 2001, caso: "Lascano Quintana, Guillermo c/ Veraz S.A.". La CSJN consideró que el *habeas data* como subespecie de amparo requiere que el acto lesivo sea manifiestamente ilegítimo. Señaló al respecto: *"...la resolución de la instancia anterior por la cual se condenaba con costas a la demandada a suprimir de su registro personal la información correspondiente a la sociedad, implicó una interpretación que como bien lo destaca el señor Procurador Fiscal exorbita el texto constitucional que prevé una medida de tal naturaleza, ante actos de ilegalidad o arbitrariedad manifiesta...."*

[8] Tramitado ante el Juzgado Nacional de Primera Instancia en lo Contencioso Administrativo Federal Nro. 10 de Buenos Aires, con sentencia del 14 de junio de 2005.

[9] En este sentido, el art. 18 de la Constitución obliga al Congreso a determinar en qué casos y con qué justificativos podrá procederse al allanamiento de la correspondencia (norma que se consideró extensible a las comunicaciones telefónicas). El tribunal entendió que la ley impugnada carecía de toda justificación de la limitación de estos derechos. Incluso, analizó los antecedentes parlamentarios, en los que corroboró que no existió un proyecto, ni exposición de motivos y que finalmente la ley se aprobó sin discusión. Por ello, destacó la falta de razonabilidad de la norma y declaró la inconsti-

1.2. La Ley de Protección de Datos Personales

El 4 de octubre de 2000 se sancionó la Ley 25.326 denominada "Ley de Protección de Datos Personales" que desarrolló el instituto reconocido en el artículo 43 de la Constitución. Según se declara en su artículo primero, el objeto de la ley es proteger los datos personales, definidos como *"información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"*. Se estructura en 6 capítulos: 1) condiciones para la obtención y tratamiento de datos personales; 2) derechos de las personas en relación a sus datos personales almacenados en algún archivo; 3) regulación del funcionamiento de las bases de datos; 4) autoridad de control; 5) delitos relacionados a la utilización indebida de los datos protegidos y; 6) acción de *habeas data*.

a) La formación de archivos de datos

El artículo 3 de la ley establece el principio de que la formación de archivos de datos es lícita si se cumplen con las disposiciones de la ley (Principio de *licitud*). El artículo 4 establece que los datos deben ser ciertos (Principio de *fidelidad*), adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido (Principio de *proporcionalidad*)[10] y que no pueden ser utilizados para

---

tucionalidad de la ley concluyendo: *"[l]a importancia del derecho protegido conmina pues, a la sanción de una norma motivada y fundada, lo que, insisto, en la ley 25.873 estuvo ausente. Es más, la Corte* [refiere a la Corte Suprema de Justicia] *requiere que la ley se encuentre, por exigencia constitucional, "... singularmente fundada" La ley no motivó ni fundó sus prescripciones, menos aún, "singularmente" (como lo exige la CSJ). Tampoco distingue casos, oportunidades o situaciones. No impone límites (a supuestos delictuales), ni garantiza la confidencialidad o secreto de la información."*

[10] Al respecto, *vid:* Corte Suprema de Justicia de la Nación. Sentencia del 6 de marzo de 2001; caso: "Lascano Quintana, Guillermo c/ Veraz S.A." En esa oportunidad se planteó la legalidad de incluir en la base de datos de información crediticia la circunstancia de que existían juicios pendientes contra una sociedad de la que el afectado era administrador. En primera y segunda instancia se hizo lugar a la acción condenándose al demandado a suprimir esa información. Sin embargo, la CSJN revocó esta decisión. En el voto conforme de una de los ministros se señaló que la información impugnada no aparecía como desmesurada en relación al fin perseguido con el registro de datos. En concretó, manifestó que: *"...la información asentada en el registro de la demandada no es falsa -ni tampoco desactualizada-, ya que está fuera de discusión que el actor era presidente de la sociedad. Tampoco puede predicarse que sea discriminatoria, por cuanto sólo refleja una circunstancia objetiva que guarda estrecha relación con la seguridad del crédito. Es decir, que se trata de una materia que hace al interés del tráfico jurídico, por lo que no se observa que el asiento cuya supresión se persigue configure de suyo una indebida intrusión en una zona de reserva o un menoscabo al ejercicio de derechos de raigambre constitucional sobre bases igualitarias".* Sin embargo, la decisión no fue unánime. Tres ministros votaron en discordia con los siguientes argumentos: *"Que en cuanto a la legitimidad del modo de registro y suministro de los datos, no puede dudarse que los correspondientes a dos personas distintas -el actor y la empresa- se han relacionado de tal forma que al informarse los del primero se menciona que el segundo tiene observaciones. Esta correlación parece inadecuada en la medida en que, al menos, es susceptible de*

fines distintos o incompatibles con los que motivaron su obtención (Principio de *finalidad*).

El principio general es que el tratamiento de datos personales sólo se puede realizar con el "consentimiento" del titular (art.5 inc.1).[11] Sin embargo, este principio está bastante limitado por el inc. 2, que contempla los casos en que este consentimiento no es necesario, como, por ejemplo, cuando se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, o cuando los datos refieran al incumplimiento de obligaciones patrimoniales y sean suministradas por los acreedores.

Luego, se establece un régimen general para un tipo concreto de datos, los datos sensibles. Estos se definen como: *"datos personales que relevan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o política e información referente a la salud o a la vida sexual"*. La ley expresamente prohíbe su registro, evitando todo criterio de comercialización sobre ellos.[12] Sin embargo, como excepción, habilita su tratamiento si median razones de interés general autorizadas por ley (art.7 inc.2) o si son tratados con finalidades estadísticas o científicas y se disocian de sus titulares. Además, se establece que los datos sensibles sólo pueden cederse entre dependencias de los órganos del Estado para el cumplimiento de sus respectivas competencias.

---

producir confusión en el ámbito de las relaciones jurídicas, en las que el conocimiento del derecho -más allá de presunciones legales- no parece alcanzar necesariamente para distinguir entre la responsabilidad de las personas de existencia ideal y la de sus directivos. Que a ello se agrega que las quejas de la recurrente parten de la base por cierto más que discutible, de limitar la ilegalidad al caso del dato falso o discriminatorio, extremo que no se compadece ni siquiera con las mismas normas que la empresa señala respetar pues si omite suministrar listados o información general, debiera con similares fundamentos abstenerse de brindar información "cruzada". La información de ese modo suministrada aparece - tal como lo sostiene el a quo- no ya discriminatoria sino susceptible de producir discriminación, lo que es suficiente en los términos de un remedio de neto corte preventivo como el hábeas data, para entenderlo procedente".

[11] Dispone el art. 5 que cuando el consentimiento se preste con otras declaraciones deberá figurar en forma expresa, destacada y en forma previa se deberá informar al requerido de: 1) la finalidad para la que serán tratados los datos; 2) quiénes pueden ser sus destinatarios; 3) identidad y domicilio del responsable del archivo; 4) las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos y 5) la posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

[12] La ley exceptúa expresamente de la prohibición a los registros que mantenga la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales de sus miembros. A su vez, también se dispone que los datos relativos a la salud y antecedentes penales pueden ser tratados por los profesionales u autoridades competentes.

b) Derechos de los titulares en relación a sus datos personales

La ley consagra cinco derechos fundamentales: 1) acceder al registro de datos (Derecho de acceso, art. 14)[13]; 2) actualizar aquellos datos que pudieran estar atrasados; 3) corregir la información inexacta; 4) asegurar la confidencialidad de cierta información para que no trascienda a terceros; y 5) cancelar datos vinculados con la denominada información sensible.[14] Estos cuatro últimos derechos se regulan en el artículo 16 bajo el título: *"derecho de rectificación, actualización o supresión"*.[15]

En definitiva, estas son las cinco concreciones del derecho a la personalidad informativa o a la autonomía informativa. A su vez, se impone un deber correlativo a los responsables de las bases de datos de habilitar el acceso a las solicitudes en los plazos establecidos y estructurar sus archivos de forma que no obstaculicen su cumplimiento.[16] Por su parte, el capítulo IV, que crea un registro de archivos de datos, impone a los responsables la obligación de inscribir los archivos que administren.

[13] La información se debe proporcionar en el plazo de diez días corridos de haber sido intimado fehacientemente. Además, se establece que este derecho sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.

[14] *Vid:* Juzgado Civil y Comercial Federal Nº 8, sentencia del 30 de septiembre de 2002; Cámara Nacional en lo Contencioso Administrativo Federal; Sala 4, sentencia del 5 de septiembre de 1995;

[15] El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, en un plazo máximo de cinco días hábiles contados a partir del día de recepción del reclamo o del momento en que se advierte el error o falsedad.

[16] La ley 25.326 establece que el actor antes de iniciar acciones judiciales debe ejercer su derecho de acceso, rectificación o supresión. En consecuencia, los responsables de las bases de datos siempre tienen oportunidad de enmendar los errores en una instancia extrajudicial. Por ello, los tribunales mantienen una firme tendencia en condenar a las entidades demandadas al pago de los gastos judiciales, considerando que ellas son las responsables de la existencia del litigio. A su vez, los daños producidos por los errores en la información que suministran estas entidades pueden reclamarse por la vía del juicio ordinario a través de una típica acción de daños y perjuicios. Al respecto, recientemente se registró un antecedente donde el tribunal se basó en la actitud negligente del demandado (tanto antes del proceso cuando se negó irrazonablemente a suprimir la información errónea como durante el proceso al negarse a suministrar la información exacta de sus fuentes) para sumar a la condena a resarcir los daños y perjuicios una condena al pago de daños punitivos basada en el art. 52 bis de la ley de defensa del consumidor, Nº 24.240 (Caso: "Cañada Pérez c/ Bank Boston; Habeas Data"; octubre de 2008. Juzgado en lo Civil Nº 39 de la Ciudad Autónoma de Buenos Aires). En el caso, el tribunal resolvió lo siguiente: *"Como vemos la norma sólo exige el incumplimiento por parte de éste [el proveedor] de sus obligaciones legales o contractuales para con el consumidor. En consecuencia el daño punitivo resulta aplicable en todos los casos (...), es decir, a todo vínculo jurídico. Entiendo, entonces que allí donde haya un reclamo por un derecho violado como el de la actora, existirá a la par la aplicación de los daños punitivos. (...) Por lo expuesto entiendo que conforme lo establecido en el art. 52 bis de la ley N° 24.240. –de Defensa del Consumidor- incorporado por el art. 25 de la Ley 26.361 corresponde aplicar a la entidad financiera demandada una multa civil a favor del consumidor –actora en estas actuaciones- (...), equivalente al importe por el que prosperará la demanda con más sus intereses al momento de practicarse la liquidación; todo ello a modo de sanción ejemplificadora para que la entidad financiera no viole derechos de terceros ni afecte derechos personalísimos de sus clientes"*.

1.3. Acción de protección de los datos personales

La acción de protección de los datos personales (calificada por primera vez como: *acción de hábeas data*) procede para reclamar los derechos establecidos en los artículos 14 a 16 de la ley (derechos de *acceso, rectificación*, *actualización* o *supresión*).

Pueden ejercerla el afectado sea persona física o jurídica contra los responsables y usuarios de los bancos de datos destinados a proveer informes.

En la demanda se debe individualizar el banco de datos y su responsable o usuario. Se deben exponer las razones por las cuales se entiende que en el archivo individualizado se encuentra información referida al actor y los motivos por los que esta información sería discriminatoria, falsa o inexacta. También se debe justificar que se ha solicitado mediante intimación su corrección previamente.

Mientas dura el proceso se puede solicitar que el registro o banco de datos asiente que la información está sometida a un proceso judicial. Asimismo, el Juez podrá bloquear provisionalmente el dato motivo del juicio si es manifiesto su carácter discriminatorio, falso o inexacto.

Si se admite la acción se da traslado de la demanda por 5 días hábiles, plazo que podrá ser ampliado a criterio del juez. En dicha oportunidad el juez requerirá la remisión de la información sobre el accionante contenida en el archivo individualizado. Con la contestación se deberán expresar las razones por las cuales se incluyó la información cuestionada y aquellas por las que no se cumplió con el pedido efectuado por el interesado. Tras la contestación, el actor puede ampliar la demanda en el caso que conozca -por la información presentada por el demandado- que hay más datos inexactos o que de cualquier modo vulneran las prescripciones de la ley.

Finalmente, se dictará sentencia que, en el caso de estimar la acción, especificará la información que debe ser suprimida, rectificada, actualizada o declarada confidencial, fijando un plazo para su cumplimiento.[17]

[17] Vid: Juzgado Civil y Comercial Federal Nº 8. Sent. 30 de septiembre de 2002.En el caso: "Vidou; María Cristina c/ Banco Central de la República Argentina y otros", se solicitó—además de que se eliminara un dato erróneo sobre la existencia de una deuda con una banco—que los demandados: *"informen y asienten en sus registros que la deuda y situación de riesgo patrimonial, financiero y comercial que informaron de ella durante todo el lapso de publicación obedecieron a un error del Lloyd Bank, siendo falsos los datos oportunamente suministrados"*. El tribunal rechazó esta segunda petición considerando que ni en el art. 43 de la Constitución ni en la ley 25.326 se contempla el deber de los propietarios de registros o bancos de datos de comunicar las modificaciones o rectificaciones que están obligados a hacer en virtud de sentencias condenatorias. Por ello, consideró que la condena se debe limitar a ordenar la supresión, rectificación, confidencialidad o actualización de los datos.

2. En Colombia

La protección de datos personales en Colombia no es un tema ajeno y extraño en nuestro ordenamiento jurídico, ya que la Constitución Política dedica un artículo específico que establece el derecho al Habeas Data[18]. Esto nos llevaría a pensar que en nuestro país existe una adecuada legislación al respecto, ya que si tenemos en cuenta que la Constitución fue expedida en el año 1991, podríamos decir que tenemos un gran experiencia en este tipo de protección, sin embargo, contrario a esto, debemos indicar que tan sólo en el año 2008 fue expedida por el Congreso una ley que regula esta protección, a pesar de que la Corte Constitucional ya por el año de 1992 había indicado en sus fallos de revisión de acciones de tutela, la necesidad de la expedición de una ley que regulara el alcance de este derecho fundamental.

Pero antes de detenernos en el contenido de la ley, nos parece oportuno echar un vistazo a la línea jurisprudencial de la Corte Constitucional al respecto.

2.1. Jurisprudencia Constitucional anterior a la entrada en vigencia de la Ley 1266 de 2008 (Ley de Habeas Data)

Los antecedentes jurisprudenciales sobre la protección del Habeas Data en Colombia, sin los cuales no es posible entender el desarrollo de la figura, son imprescindibles por cuanto a pesar de que esta figura está consagrada constitucionalmente en el artículo 15 de la Carta desde 1991, no es hasta el 31 de diciembre de 2008, es decir, hace tan sólo pocos meses, que entró en vigor la primera ley de Habeas Data que le corresponderá regular todas las minucias relacionadas con el tema en cuestión.

Con el fin de no extendernos más de la cuenta por no ser la finalidad de este trabajo, nos referiremos exclusivamente a la sentencia T-414/92 de 16 de junio de 1992[19], que sentó doctrina constitucional para el manejo

[18] El artículo 15 de la Constitución colombiana señala: "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 los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. 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". Este artículo se encuentra en el Capítulo I De los derechos fundamentales, de tal manera que son amparadas por vía de tutela o recurso de amparo.

[19] Sentencia de Tutela T-414 de 1992. Magistrado Ponente: Ciro Angarita Barón

del Habeas Data hasta que se produjese la promulgación de la respectiva ley que regulara el tema.

La sentencia aclarara que la Constitución garantiza tanto el derecho a la intimidad como el derecho a la información *"cuyo rango constitucional es equivalente"*, por lo cual es preciso *"establecer un equilibrio entre ambos derechos"* que permita respetar la libertad y la dignidad de las personas tanto como el derecho a la información veraz e imparcial.

Con la consagración expresa que se ha hecho de la dignidad humana como el valor supremo del Estado Social de Derecho, (Artículo 1o. de la Carta de 1991), la intimidad, que es una de las manifestaciones más concretas y directas de dicha dignidad, adquirió una posición privilegiada en el conjunto de los derechos constitucionales fundamentales. Esto implica, una vez más, que ante un eventual conflicto insuperable entre el derecho a la información y el derecho a la intimidad en donde no pueda ser posible un equilibrio o coexistencia, la intimidad deberá prevalecer.

En los casos en que se haya vulnerado la intimidad, la libertad personal y la dignidad de los ciudadanos mediante el abuso de la tecnología informática y del derecho de y a la información, se ordena que prevalezcan estos derechos sobres los demás en todos los casos.

Por último, debo agregar que la sentencia de tutela T-414/92, de 16 de junio de 1992, ordenó que *"en todos aquellos casos similares al presente por sus hechos o circunstancias, siempre que hayan ocurrido abusos o intromisiones arbitrarias o ilegales en la recolección, almacenamiento, tratamiento, uso y divulgación no autorizada expresamente de datos personales, por cualquier medio o tecnología, que amenacen vulnerar la intimidad y libertad informática de la persona, la doctrina constitucional enunciada en esta sentencia tendrá CARACTER OBLIGATORIO para las autoridades".*

2.2. Ley 1266 de 2008, por la cual se dictan disposiciones generales sobre el Habeas data

Tenemos que destacar, en primer lugar, que el objeto de la ley es el de desarrollar el derecho constitucional de las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos. También tiene por objeto desarrollar los demás derechos, libertades y garantías constitucionales relacionados con la recolección de información.

Esta ley se aplica a todos los datos de información personal registrados en un Banco de datos[20], administrados por entidades de naturaleza pública o privada, y se aplica sin perjuicio de las normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en Bancos de datos de naturaleza pública para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público.

Es importante aclarar cuáles son los sujetos que pueden intervenir en el manejo de los datos personales. En primer lugar tenemos al titular de la información, que puede ser una persona natural o jurídica a quien se refiere la información que reposa en un Banco de datos, y sujeto del derecho de Habeas data; en segundo lugar, la fuente de información es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio, y que en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará a un usuario final. Este sujeto puede llegar a tener el doble carácter de fuente y de operador de la información; Y por otro lado, el operador de la información es la persona, entidad u organización que recibe de la fuente datos personales, los administra y los pone en conocimiento de los usuarios; por último el usuario es la persona ya sea natural o jurídica que puede acceder la información personal de uno o varios titulares de la información,

La ley consagra una serie de principios de la administración de datos, cuales son:

Principio de veracidad o de calidad de los registros o datos: según el cual los datos consignados en los Bancos de datos deben ser veraces, completos, actualizables, exactos, comprobables y comprensibles, de tal manera que no se permite la divulgación de datos parciales, incompletos, fraccionados o que puedan llegar a inducir a error.

Principio de finalidad: la administración de datos debe obedecer a una finalidad, la cual debe ser comunicada al titular de la información de manera previa o concomitante con el otorgamiento de la información.

Principio de circulación restringida: Según el cual la administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, así como de las disposiciones de la Ley de Habeas data y de los principios de la administración de datos. Igualmente se señala que

[20] No se hace referencia a si los datos allí consignados son sólo de carácter informático o no, lo que implica que pueden no ser sólo de esta naturaleza.

los datos personales, salvo los que sean de información pública, como por ejemplo, sentencias judiciales debidamente ejecutoriadas, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, a menos que el acceso sea controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados por la ley.

Principio de temporalidad de la información: Se indica que la información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del Banco de datos[21].

Principio de interpretación integral de derechos constitucionales: Según el cual, la ley de la que estamos hablando, será interpretada siempre en el sentido de que se amparen los derechos constitucionales, como el habeas data, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Además se indica que los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el art. 20 de la Constitución[22] y con los demás derechos aplicables.

Principio de seguridad: La información de los registros individuales de los bancos de datos y los que resulten de las consultas que de ella hagan los usuarios, deben ser manejados con las medidas técnicas necesarias para garantizar la seguridad de los registros, con el fin de evitar su adulteración, pérdida, consulta o uso no autorizado.

Principio de confidencialidad: Según el cual toda persona natural o jurídica que intervenga en la administración de datos personales, que no tengan la naturaleza de públicos, están obligadas a garantizar la reserva de la información, en todo tiempo, incluso después de finalizar su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la ley.

[21] En ese sentido, la ley hace referencia al tiempo de permanencia de la información en los Bancos de datos de los operadores, si es de carácter positivo, la información permanecerá de manera indefinida; sin embargo, cuando haya mora los datos sí están sometidos a un tiempo de permanencia, vencido el cual la información deberá ser retirada de los Bancos de datos, este tiempo es de cuatro (4) años contados a partir de la fecha en que se extinga la obligación por cualquier modo. Sobre este punto, es preciso indicar que la Corte Constitucional en la sentencia C-1011 de 2008, por la que declaró la exequibilidad de la ley de habeas data, manifestó que en caso de que la mora sea inferior a dos años, el tiempo de permanencia de los datos no podrá exceder el doble de la mora.

[22] Artículo 20 Constitución de Colombia: "Se garantiza a toda persona la libertad de expresar y 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".

Por último, para cerrar estos comentarios que se han hecho a la Ley de Habeas data en Colombia, se debe indicar que existen dos entidades que ejercen vigilancia, por un lado la Superintendencia de Industria y Comercio[23], que ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información de que trata esta ley, en cuanto se refiere a la actividad de administración de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países; y por otro, la Superintendencia Financiera de Colombia ejercerá vigilancia e impondrá sanciones en los casos en que la fuente, el usuario o el operador de la información sea una entidad sometida a su vigilancia.

3. En Perú

3.1. Precepto Constitucional

En Perú el "Derecho a la Protección de Datos personales" en la actualidad no existe como tal estructura normativa autónoma. No obstante, el derecho a la intimidad personal y familiar del ciudadano, en íntima conexión con el derecho de Protección de Datos, es un derecho personalísimo que se encuentra protegido por la Constitución Política de 1993[24].

3.2. Normas o Leyes que protegen los datos personales

A partir de tal protección constitucional, y en relación con el derecho a la salud reconocido en la Norma fundamental peruana[25] desarrollado por la Ley General de la Salud[26], se tutela el derecho de toda persona usuaria de los servicios de salud al respeto de su personalidad, dignidad e intimidad y a exigir reserva de la información relacionada con el acto médico, y de su historia clínica, con las excepciones que la Ley establece. A pesar de lo indicado, según prevé dicha legislación, el médico que haya brindado atención médica a una persona herida por arma blanca, herida de bala, por accidente de tránsito, o por causa de otro tipo de violencia que constituya delito perseguible de oficio, o cuando existan indicios de

[23] Las Superintendencias son organismos técnicos, con personería jurídica y autonomía administrativa y patrimonio propio que realiza la inspección, vigilancia y control de determinados organismos dependiendo del tipo de actividad al que se dedican.

[24] La intimidad personal es tutelada en el apartado 7º, artículo 2 de la Constitución Política del Perú de 1993, que establece: "Toda persona tiene derecho al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propia".

[25] Constitución Política del Perú de 1993, en su artículo7.

[26] Ley General de la Salud Nº 26842, de fecha 27 de julio de 1997, en su artículo 15.

aborto criminal, tiene la obligación de poner el hecho en conocimiento de la autoridad competente[27].

Asimismo, sin dejar el ámbito sanitario, los datos de las personas que padecen el síndrome de inmunodeficiencia adquirida (SIDA) se encuentran igualmente protegidos. De la misma forma, la específica Ley contra el síndrome de inmunodeficiencia adquirida[28] protege los derechos a la autonomía y a la prueba para el diagnóstico, el derecho a la confidencialidad, el derecho al trabajo a partir de esa coyuntura, así como a la atención integral de salud.

En el ámbito financiero, en referencia a los datos bancarios, los sujetos tienen derecho al secreto bancario y la reserva tributaria, los cuales sólo pueden levantarse a petición del juez, del Fiscal de la Nación, o de una Comisión investigadora del Congreso, con arreglo a Ley y siempre que se refieran al caso investigado[29]. De esta manera, el secreto bancario también forma parte del contenido constitucionalmente protegido del derecho a la intimidad. De este modo se prohíbe a las empresas del sistema financiero, así como a sus directivos y trabajadores, suministrar cualquier información sobre las operaciones pasivas con sus clientes, a menos que medie autorización escrita de éstos o se trate de los supuestos consignados en la Ley[30].

Sobre el particular, el Tribunal Constitucional en su Sentencia de 21 de enero de 2004. Expediente Nº 1219-2003-HD/TC, caso Nuevo Mundo Holdong S.A, precisaba que la protección constitucional, que se dispensa en relación con el secreto bancario, busca asegurar la reserva o confidencialidad de una esfera de la vida privada de los individuos o de las personas jurídicas de derecho privado. En concreto, la necesaria confidencialidad de las operaciones bancarias de cualquiera de los sujetos descritos que pudieran realizar con cualquier ente, público o privado, perteneciente al sistema bancario o financiero.

En el ámbito informático, en materia de protección de la intimidad personal y familiar del sujeto, se prohíbe a los servicios informáticos, computerizados o no, públicos o privados, suministrar informaciones

[27] Ley General de la Salud Nº 26842...cit., en artículo 30.

[28] Ley contra el síndrome de inmunodeficiencia adquirida Nº 26626, de fecha 20 de junio de 1996.

[29] Constitución Política del Perú de 1993, en su artículo 2 apartado 7º.

[30] Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros Nº 26702, en sus artículos 140, 142 y 143.

que afecten a tales bienes jurídicos[31]. Del mismo modo, la Ley que regula las centrales privadas de información de riesgos (CEPIRS[32]), y de protección al titular de la información[33], concede protección específica al respecto. Dicha información deberá ser confidencial, no difundida y conservada durante el plazo legal establecido o, en su defecto, durante el tiempo necesario para los fines para los que fue recolectada.

De modo genérico, los datos de carácter personal incluidos en las bases de datos de las empresas del sector privado, en el tráfico comercial y en las negociaciones realizadas por Internet, son cedidos por parte de sus titulares para una finalidad determinada. En tal sentido, la Ley que regula el uso del correo electrónico comercial no solicitado (SPAM)[34] otorga protección a los datos de carácter personal obtenidos a través de la red. La responsabilidad y competencia de esta protección queda delegada al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)[35], el cual, a través de la Comisión de Protección al Consumidor y de la Comisión de Represión de la Competencia Desleal, conocerá de las infracciones a la presente Ley e impondrá las multas fijadas de acuerdo a lo establecido en la Ley de Protección al Consumidor[36], o en las Normas de la Publicidad en Defensa del Consumidor[37], según corresponda.

En materia de comunicaciones, los datos e información de los sujetos contenida en las mismas, se encuentran bajo el amparo del derecho al secreto y a la inviolabilidad de las comunicaciones y documentos privados de toda persona[38]. Al respecto, sólo en caso de mandato motivado del Juez, las comunicaciones, telecomunicaciones o sus instrumentos podrán ser abiertos, incautados, interceptados o intervenidos con las garantías previstas en la ley. En consecuencia, se guardará secreto de los asuntos ajenos al hecho que motiva su examen.

[31] Constitución Política del Perú de 1993, en su artículo 2 apartado 6º.

[32] Empresas que en locales abiertos al público y de modo habitual, recolectan y tratan información de riesgos relacionada con personas naturales o jurídicas, con el propósito de difundir por cualquier medio mecánico o electrónico, de manera gratuita u onerosa, reportes de crédito acerca de éstas.

[33] Ley Nº 27489 promulgada el 27/6/2001, publicada el 28/6/2001 y reglamentada por Decreto Supremo Nº 031-2005MTC.

[34] Ley Nº 28493, anti spam, de Perú, de fecha 12 de abril de 2005.

[35] Regulado por el Decreto Legislativo del 16 de abril de 1996 (publicado el 18 de abril de 1996).

[36] Decreto Legislativo Nº 716, de fecha 7 de noviembre de 1991.

[37] Decreto Legislativo Nº 691, de 5 de noviembre de 1991, acompañado de su reglamento, el Decreto Supremo 20-94-ITINCI.

[38] Constitución Política del Perú de 1993, en su artículo 2 apartado 10º.

Del mismo modo, se condena la violación del secreto profesional por parte del sujeto que, teniendo información por razón de su estado, oficio, empleo, profesión ministerio, de secretos cuya publicación pueda ser lesiva, los revela sin consentimiento del interesado[39].

Por todo lo expuesto, la República del Perú cuenta con preceptos constitucionales, normas de carácter estrictamente sectorial y un proyecto de Ley de Protección de Datos Personales aprobado por Resolución Ministerial 331-2004 JUS, que persigue, como finalidad regular, garantizar el derecho a la protección de datos personales, cautelando los derechos a la intimidad, identidad, honor y propia imagen. Al respecto, los datos a proteger por la futura Ley son aquellos que se encuentran en soporte técnico, informático o similar, u otros que se creen, susceptibles de tratamiento y uso público y/o privado. Igualmente, se dispone, en el mismo cuerpo legal, la creación de la Autoridad Nacional de Protección de Datos Personales (APDAP), como organismo público descentralizado, con personalidad jurídica de derecho público interno, adscrito a la Presidencia del Consejo de Ministros.

3.3. Jurisprudencia Comentada y la acción de Habeas Data

Como principal mecanismo de defensa de los datos personales en el Perú, está prevista la Garantía Constitucional del *Habeas Data*[40], regulada por Ley expresa[41], la cual procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o de cualquier otra persona, que vulnere o amenace el derecho a la intimidad personal y familiar del sujeto titular del mismo.

En consecuencia, mediante el *Habeas Data* toda persona puede acudir a dicho proceso en primer lugar para acceder a información que obre en poder de cualquier entidad pública, así como para conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. En segundo término, faculta para exigir la supresión o para

[39] Código Penal Peruano aprobado por Decreto Legislativo Nº 635 fecha 8 de abril de 1991, en su artículo 165.

[40] Constitución Política del Perú de 1993, en su artículo 200 apartado 3º.

[41] Ley sobre el Habeas Data Nº 26301, de fecha 3 de mayo de 1994.

impedir que se suministren datos o informaciones de carácter sensible o privado que afecten a derechos constitucionales[42].

En relación a lo expuesto destaca la Sentencia de 20 de diciembre de 2006, Expediente Nº 04627-2006-PHD/TC, emitida por el Tribunal Constitucional del Perú, que resuelve el recurso de agravio constitucional interpuesto contra la Sentencia emitida por la Primera Sala Civil de la Corte Superior de Lambayeque declarando improcedente la demanda de Habeas Data presentada en el caso en concreto por X, quien como árbitro de fútbol, arbitró un partido entre dos equipos determinando la sanción al equipo Y. Posteriormente, el Presidente del equipo Y, publicó en el diario Z el informe médico practicado al árbitro X, haciendo pública la enfermedad que éste padecía. Por esta razón, X presentó demanda de Habeas Data contra el Seguro Social donde lo atendieron y diagnosticaron su enfermedad, por facilitar el informe médico, documento que constaba en su historia clínica; asimismo, demandó al Presidente del equipo de fútbol Y y al diario Z. El fallo, emitido por el Tribunal Constitucional, declaró infundada la demanda, al no haber encontrado responsabilidad en el Seguro Social, pues el documento que se publicó en el diario no contenía ningún sello o signo identificativo que lo vinculara con esa institución. Además de ello, el Seguro Social exhibió la historia clínica de X, donde no figuraba el documento en mención. Finalmente, declaró improcedente la demanda en cuanto a las responsabilidades de Y y Z, al considerar que el hecho había ocurrido con anterioridad a que se presentara la demanda, afirmando que sólo procedería, la rectificación en el proceso ordinario.

Respecto a este fallo, el Código Procesal Constitucional establece que el proceso de *habeas data* tiene por finalidad proteger los derechos constitucionales, reponiendo las cosas al estado anterior a la violación[43]; no obstante, no proceden los procesos constitucionales cuando existan vías procedimentales específicas, igualmente satisfactorias, para la protección del derecho constitucional amenazado[44]. Igualmente y dado que el procedimiento de Habeas Data será el mismo que el previsto por dicho Código para el proceso de amparo[45], se podrá rechazar una demanda de Habeas Data si se ha interpuesto en defensa del derecho de rectificación

[42] Constitución Política del Perú de 1993, en su artículo 2 apartados 5º y 6º

[43] Código Procesal Constitucional aprobado por Ley Nº 28237 de fecha 31 de mayo de 2004,en artículo 1.

[44] Código Procesal Constitucional... cit., en artículo 5.

[45] Código Procesal Constitucional... cit., en artículo 65.

y no se acredita la remisión de una solicitud cursada por conducto notarial u otro fehaciente al director del órgano de comunicación[46]. Además de lo indicado, para que proceda el Habeas Data se requiere que el demandante previamente haya reclamado, por documento de fecha cierta, el respeto de los derechos a que se refiere el artículo anterior, y que el demandado se haya ratificado en su incumplimiento o no haya contestado dentro del plazo establecido por esta Ley[47].

4. En República Dominicana

4.1. Precepto Constitucional

La utilización masiva de las herramientas electrónicas, es lo que caracteriza a la sociedad de hoy. Aquellas que permiten capturar, almacenar, tratar y usar nuestros datos personales. Todo esto unido al reconocimiento del derecho fundamental de acceso a la información pública, nos plantea la necesidad de garantizar a través de una legislación general la protección de los datos personales.

Es el artículo 8 de la Constitución de la República Dominicana, que reconoce como finalidad principal del Estado la protección efectiva de los derechos de la persona y el mantenimiento de los medios que le permitan perfeccionarse progresivamente dentro de un orden de libertad individual y de justicia social. Establece constitucionalmente normas para la consecución de estos fines entre las que están la inviolabilidad de la correspondencia y demás documentos privados, la inviolabilidad del secreto de comunicación telegráfica, telefónica y cablegrafía.

A pesar de que no cita textualmente la protección a los datos personales, el artículo 10 plantea que, la enunciación del artículo 8 no es limitativa y por consiguiente, no excluye otros derechos y deberes de igual naturaleza. En ese mismo sentido, es interesante señalar que nuestra Constitución en su artículo 3 establece que la República Dominicana reconoce y aplica las normas del Derecho Internacional general y americano en la medida en que sus poderes públicos las hayan adoptado.

En este sentido, cabe señalar algunos articulados de instrumentos internacionales adoptados por la República Dominicana que se refieren a:

[46] Código Procesal Constitucional... cit., en artículo 47.
[47] Código Procesal Constitucional... cit., en artículo 62.

a) el artículo 12 de la Declaración Universal de los Derechos Humanos,
b) el artículo 17 del Pacto Internacional sobre Derechos Civiles y Políticos,
c) el artículo 11 de la Convención Americana sobre Derechos Humanos.

Todos utilizan términos casi idénticos cuando hablan de la protección de la ley contra "injerencia y ataques" a la vida privada, a la correspondencia, la honra y la reputación.

4.2. Normas o Leyes que protegen los datos personales

De igual forma, el Acuerdo General sobre Comercio en Servicios (GATS) que forma parte del marco de los Tratados de la Organización Mundial del Comercio, establece en su artículo XIV-C-II que ninguna de las disposiciones de ese Acuerdo, será interpretada como límite para que un Estado adopte y aplique medidas para la protección de la privacidad de los particulares en relación con el tratamiento y la difusión de datos personales y la protección del carácter confidencial de los registros y cuentas individuales.

La normativa vigente en República Dominicana para la protección de datos es:

a) La Ley general 200-02 sobre acceso a la información pública y su reglamento de aplicación Decreto 130-05. El principio es que toda la información pública, es de libre acceso. Existen dos excepciones: las limitaciones en virtud de intereses públicos preponderantes y las limitaciones en virtud de intereses privados preponderantes. Dentro de las limitaciones al acceso a la información pública en virtud de intereses privados preponderantes se hace mención de los datos personales.

b) La Ley 288-05 que regula las sociedades de intermediación crediticia y protección al titular de la información. Esta es una legislación sectorial que contempla la protección de datos personales. El objeto de esta ley es regular la prestación de los servicios de referencias crediticias y el suministro de información en el mercado, garantizando el respeto a la privacidad y los derechos de los titulares de la misma. Sus disposiciones son de orden público y de aplicación general. Los principios rectores de esta Ley son: El Acceso de la Persona Interesada, La Exactitud, La Finalidad, La Seguridad de Datos.

4.3. Resolución 055-06 del Instituto Dominicano de Telecomunicaciones (INDOTEL)

Por último la Resolución 055-06 del Instituto Dominicano de Telecomunicaciones (INDOTEL) sobre protección de datos de carácter personal por los sujetos regulados.

En materia de telecomunicaciones la necesidad de protección de los datos personales, vino dada, porque la inexistencia de un marco normativo general en materia de datos personales podría ir en detrimento de la capacidad de este país para poder realizar transacciones electrónicas con países que si cuentan con tal normativa.

Esta resolución consta de XI títulos. Su objeto es garantizar la protección, confidencialidad y debido uso de la información suministrada a los sujetos regulados.

De tal suerte que lo dispuesto en esta norma es aplicable a los tratamientos de datos personales de los interesados que realicen los sujetos regulados por el INDOTEL, independientemente de si el tratamiento se lleva en archivos digitales o en papel.

A los fines de esta norma se entenderá como datos personales cualquier información concerniente a personas naturales identificadas o identificables.

Los datos relativos a personas jurídicas no serán considerados Datos de Carácter Personal, sin perjuicio de aquellos datos relativos a personas naturales que se encuentren vinculadas a dichas personas jurídicas que si podrán ser considerados como Datos de Carácter Personal, comprendiendo, entre otros, los datos de sus representantes, apoderados o trabajadores.

La propia resolución en uno de sus articulados establece que para los casos en que exista algún vacío normativo, se deberá buscar su interpretación atendiendo a la importancia que tiene la protección de la intimidad y el honor de los interesados en el tratamiento de sus datos de carácter Personal por parte de los entes regulados.

La normativa regula la recogida de los datos de carácter personal, distinguiendo en si la información fue recibida directamente de los propios interesados o si fue de un tercero.

Así mismo establece como regla el consentimiento para el tratamiento de los datos de carácter personal, describiendo como debe ser este consentimiento.

Establece los derechos de los interesados normandos los derechos de acceso, rectificación y cancelación de datos personales.

Por último, otorga facultades de inspección y sanción, estas últimas pueden ser muy graves, graves y leves atendiendo a su naturaleza y gravedad.

Son sanciones administrativas a las que se hacen pasibles los entes regulados, independientemente de la responsabilidad civil o penal en que pudiesen incurrir los infractores.

Finalmente, otras leyes y normas referentes a la protección de datos son: la Ley 42-01. Ley General de Salud. y su Reglamento de Hospitales (Regulación de la historia clínica), Ley de SIDA, Ley Monetaria y Financiera, el Código Tributario y el Código de Niños, Niñas y Adolescentes.

5. En Venezuela

Fundamentalmente se ha trabajado en el concepto de Habeas Data y a nivel constitucional. La Protección de Datos Personales no está supervisada por una organización específica.

En la Constitución de la República Bolivariana de Venezuela[48] el Habeas Data está contemplado en el artículo 28 que reza: "*toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes que consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto a las fuentes de información periodística y de otras profesiones que determine la Ley*".

Se reconoce un conjunto de derechos de la persona respecto a la información que sobre sí misma o sus bienes se encuentran bajo dominio de instituciones públicas o privadas, protege la intimidad y el libre desarrollo de la personalidad. Se establece como un derecho de toda persona a acceder a documentos de cualquier naturaleza que contengan información suya cuyo conocimiento sea de interés para comunidades o grupos de personas. La figura del habeas data queda en "amparo constitucional,

[48] Publicada en Gaceta Oficial Nº 36.860 de fecha 30 de diciembre de 1999.

mediante un trámite oral, público, breve, gratuito, y no sujeto a formalidad; y la autoridad judicial competente tendrá potestad para restablecer inmediatamente la situación jurídica infringida o la situación que más se asemeje a ella, y con tratamiento preferencial", tal como lo dispone el segundo aparte del artículo 27 de la Constitución.

Por otro el artículo 60, consagra "*toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos*"[49]. El legislador quiso dar un paso por delante de la tecnología y prever que fuera el Estado quien controle la influencia de ésta sobre la sociedad, para así evitar que se violen o lesionen derechos de las personas.

Además del texto constitucional la Ley Orgánica de la Defensoría del Pueblo[50], en su artículo 15 parte 2, establece la posibilidad de "*interponer, adherirse o de cualquier modo intervenir en las acciones de inconstitucionalidad, interpretación, amparo, hábeas corpus, Habeas Data (...)"*.

Y la Ley Especial contra Delitos Informáticos[51], en su artículo 20, establece como delito la violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personal de otro o sobre la cual tenga interés legítimo, que esté incorporada en un computador o sistema que utilice tecnologías de información, será penado con prisión de 2 a 6 años y multa de 200 a 600 U.T.[52]

El Tribunal Supremo de Justicia[53] ha sido el órgano encargado de establecer los procedimientos mediante los cuales serán garantizados los derechos consagrados en el artículo 28 de la Constitución Nacional referidos a Protección de Datos o Habeas Data. Señala la Sala Constitucional que existiendo en el país una Sala Constitucional específica para

[49] Es idéntico al artículo 18.4 de la Constitución Española de 1978.

[50] Publicada en Gaceta Oficial Nº 37.995 de fecha 5 de agosto de 2004.

[51] Publicada en Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2001.

[52] Unidad Tributaria, es la medida de valor creada a los efectos tributarios como una medida que permite equiparar y actualizar a la realidad inflacionaria, los montos de las bases de imposición, exenciones y sanciones, entre otros, con fundamento en la variación del Índice de Precios al Consumidor. SERVICIO NACIONAL INTEGRADO DE ADMINISTRACIÓN ADUANERA Y TRIBUTARIA (SENIAT).

[53] http://www.tsj.gov.ve

conocer lo relativo a las infracciones de la Carta Fundamental, no parece lógico, ante el silencio de la Ley, atribuir el conocimiento de estas causas a tribunales distintos.

Dentro de las Sentencias vinculadas al tema, encontramos las siguientes que hemos clasificado en un amparo especializado, como una acción autónoma, de la competencia para conocer de la acción autónoma, y por último los sujetos en el ejercicio de la acción:

5.1. El Habeas Data como un amparo especializado. Sentencia 00659, Exp. Nº 04-0338, del 16/06/2004. Partes: Elías Pernía vs. Luis Toscón

Se interpuso recurso de habeas data contra la página Web creada por el Diputado Luis Toscón[54], la cual contenía los datos personales de los ciudadanos que participaron en la jornada de recolección de firmas para un proceso revocador. El Tribunal consideró que al ser el recurso de habeas data, era una modalidad especial de la acción de amparo constitucional dirigido a proteger el derecho constitucional al honor y la reputación de las personas, siendo la Sala Constitucional la que contaba con la facultad y el deber de velar por la correcta interpretación y aplicación de las normas constitucionales.

5.2. El Habeas Data como una acción autónoma. Sentencias 1004, Exp. Nº 07-2145, del 26/05/2007, partes: Franca Alfano Tantino; y Sentencia 1012, Exp. Nº 00-2812, del 12/06/2001, partes: María Inmaculada Pérez Dupuy

En el primer supuesto, el Tribunal mantuvo que el mandamiento de habeas data constituye una eficaz herramienta para hacer realidad el contenido del derecho a protección del honor, vida privada y reputación consagrado en el artículo 60 antes descrito, puesto que si se establece el "derecho de toda persona a ser protegido" en su honor y reputación es tarea del intérprete determinar el camino procesal más adecuado acorde con esa necesidad de protección.

En la segunda de las Sentencias, se mantiene que la acción de habeas data es autónoma, diferente a la de amparo constitucional, y tiene lugar cuando alguien en una base de datos, donde recopila información de las personas en forma general, guarda datos sobre otro (el accionante), el cual tiene derecho a acceder a la recopilación, a que se le informe con que finalidad el recopilador guarda la información, y además -según los

[54] http://www.luistascon.com/

casos- tiene derecho a que los datos se pongan al día, se rectifiquen o se destruyan.

5.3. De la competencia para conocer de la acción autónoma de Habeas Data. Sentencia 332, Exp. Nº 00-1797, del 14/03/2001. Partes: Isaca C.A.

Cuando las leyes no han desarrollado su ejercicio y se requiere acudir a los tribunales de justicia, debido a la aplicación directa de dichas normas, es la jurisdicción constitucional, representada por la Sala Constitucional, la que conocerá las controversias que surjan con motivo de las normas constitucionales aun no desarrolladas legislativamente, hasta que las leyes que regulan la jurisdicción constitucional, decidan lo contrario.

5.4. Los sujetos en el ejercicio de la acción de Habeas Data. Sentencia 1050, Exp. Nº 00-2378, del 23/08/2000. Partes: Ruth Capriles Méndez y otros; Y Sentencia 2452, Exp. Nº 02-2108, del 01/09/2003. Partes: Antonio José Varela. Exp: 02-2108

En el primero de los supuestos, el Tribunal mantiene que quien no alega que el habeas data se solicita para obtener información sobre sus datos registrados, carece de interés legítimo en tal acción, ya que no hace uso del derecho que otorga dicha norma, con los otros derechos que nacen de la misma, los cuales giran alrededor de las informaciones personales.

Y en el segundo supuesto, el Tribunal consideró que cuando los registros no son del acceso del colectivo, sino que, en razón de su especialidad, guardan determinados tipos de información, entonces el interés para solicitar su acceso y consecuente modificación, actualización o destrucción, se reduce al ámbito del derecho subjetivo de la persona o representante, cuyos datos repercuten de manera directa. Respecto del interés de la persona para acceder, actualizar, modificar, e inclusive, eliminar información, la Sala lo ha circunscrito dentro del ámbito de que los datos de interés contengan aspectos relacionados directamente en la esfera jurídico-subjetiva del afectado.

Se concluye tras estas sentencias, y después de una consulta pública realizada por la UCV,[55] que es necesario que la Asamblea Nacional decrete una Ley de Protección de Datos[56], porque se considera que la

[55] Universidad Central de Venezuela. Caracas-Venezuela. http://www.ucv.ve/
[56] http://www.asambleanacional.gob.ve/

información personal y la vida privada de los ciudadanos debe ser resguardada y protegida por una Ley.

6. En Uruguay

La Constitución no menciona expresamente el derecho de la persona a la protección de sus datos personales o su intimidad como tal. Sin embargo, su artículo 72 declara que la enunciación de derechos individuales de la Carta no es taxativa y que en él caben todos los derechos inherentes a la persona o derivados de la forma republicana de gobierno.

Por ello, este derecho puede considerarse allí comprendido. En este sentido, de forma expresa la Ley de protección de datos personales de 2008, expresamente declara que "*es un derecho humano porque está comprendido en el artículo 72*".[57] Interesa destacar que con anterioridad a la nueva Ley se habían planteado acciones judiciales de amparo por lesión al derecho a la intimidad y la jurisprudencia no había negado la calidad de derecho constitucional protegido de la protección de los datos.[58]

6.1. Régimen legal

La primera Ley que Uruguay tuvo al respecto se aprobó en 2004, pero refería únicamente a bases de datos de carácter comercial y su regulación era bastante sintética. Por otro lado, estaban vigentes—como siguen hoy—el régimen del secreto bancario (recogido en la Ley de Intermediación Financiera), el secreto tributario y algunas leyes de bases de datos públicos con fines estadísticos.

Recién con la Ley 18331 Uruguay pasa a tener un régimen general de protección de datos personales. La Ley comprende los datos relativos a personas físicas y jurídicas (en este último caso en cuanto les fuere aplicable el régimen legal) registrados en cualquier soporte que los haga

[57] Artículo 1º de la ley 18331.

[58] Además, antes de la nueva Ley, se plantearon acciones judiciales para obtener datos que autoridades estatales no querían brindar. Por ejemplo, en 2005 la Liga de Defensa Comercial (entidad privada encargada de difundir en la plaza comercial la información sobre el incumplimiento de obligaciones comerciales) demandó al Banco Central por no entregarle la lista de de personas con cuenta suspendida por falta de pago de cheques, invocando su deber de mantener el secreto bancario. La acción fue amparada porque se entendió que el derecho a la protección de los datos del titular de la cuenta debía ceder frente a la necesidad del comercio, de conocer la conducta crediticia de sus agentes (*vid*. Sentencia de 2005 del Tribunal de lo Contencioso Administrativo, en el caso Liga de Defensa Comercial c/ Banco Central del Uruguay).

susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos, en el ámbito público y privado.[59]

Sin embargo, la nueva Ley aclara que su régimen no se aplica a las bases de datos mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales ni a las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.[60]

a) Principios generales de la ley

El capítulo II de la Ley sienta una serie de principios generales, interpretativos y rectores de la actuación de los titulares de bases de datos (públicas y privadas). Son los principios de: a) Legalidad[61]; b) Veracidad[62]; c) Finalidad[63], d) Previo consentimiento informado[64], e) Seguridad de los datos y reserva; f) Responsabilidad. Estos principios se van desarro-

[59] Artículo 3 de la ley 18331.

[60] Se considera una base de datos al "*conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso*". Es "*dato personal*" la "*información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables*".

[61] El artículo 6 establece el principio de legalidad, expresando que la formación de bases de datos es lícita cuando se encuentren debidamente inscritas y observan en su operación los principios que establece la ley y la reglamentación. También se dice que las bases de datos no pueden tener finalidades violatorias de derechos humanos o ser contrarias a las leyes o a la moral pública.

[62] El artículo 7 regula el principio de veracidad, que implica que los datos recogidos para su tratamiento deben ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. Además, se establece que su recolección no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones de la ley. Finalmente, también en dicho artículo se dispone que los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario.

[63] Este principio, establecido en el artículo 8, determina que los datos no pueden utilizarse para fines distintos a los que motivaron su obtención. Además, los datos se deben eliminar cuando dejen de ser necesarios o pertinentes a los fines para los que se recolectaron. La reglamentación—aún no dictada—podrá determinar casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y según la legislación específica, se conserven datos personales aun cuando haya perimido tal necesidad. Tampoco se pueden comunicar datos entre bases, sin que medie ley o previo consentimiento informado del titular.

[64] Artículo 9. La ley excluye en ciertos casos la necesidad de previo consentimiento informado: a) datos provenientes de fuentes públicas de información (como registros o publicaciones en medios masivos de comunicación); b) los recabados para el ejercicio de funciones de los poderes del Estado o en base a una obligación legal; c) los listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, su razón social, nombre de fantasía, registro de contribuyentes, domicilio, teléfono e identidad de las personas a su cargo; d) los derivados de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su cumplimiento; y e) los recolectados por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico.

llando luego a lo largo del articulado, principalmente al enunciarse los derechos de las personas. No obstante, en cierta medida estos principios generales se restringen en la regulación legal concreta de la Ley.

b) Principales derechos de las personas

La Ley establece una serie de derechos de las personas. En esencia, son el de obtener información respecto a la finalidad de la obtención de sus datos y su utilización[65] y el derecho a acceder a esta información. El acceso a la información de las bases de datos es gratuito cada seis meses, acreditando el solicitante su identidad.[66] Sin embargo, este derecho se limita si la información afecta a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales.[67]

La Ley también recoge el derecho de las personas a la *rectificación, actualización, inclusión o supresión de los datos,* por error o falsedad, en no más de 5 días.[68] Asimismo, se reconoce el derecho a impugnar las valoraciones personales, sean hechas por personas públicas o privadas.[69] Además, se establece que la valoración sobre el comportamiento basada en un tratamiento de datos, sólo tiene valor probatorio a pedido del afectado.

[65] El artículo 13 de la Ley establece que las personas tienen derecho a la información "*expresa, precisa e inequívoca*" sobre: a) la finalidad del tratamiento de sus datos y quiénes pueden ser sus destinatarios; b) la existencia de la base de datos y la identidad y domicilio del responsable; c) el carácter obligatorio o facultativo de las respuestas al cuestionario, especialmente sobre los datos "sensibles"; d) las consecuencias de dar los datos y de la negativa a hacerlo o su inexactitud; e) posibilidad de ejercer los derechos de acceso, rectificación y supresión.

[66] La información debe brindarse en no más de 5 días y de forma clara, sin uso de codificaciones y en su caso, acompañada de una explicación que la haga accesible a la "*media de la población*". La información debe ser amplia, versar sobre todo el registro sin abarcar a terceras personas aunque se vinculen con el interesado. Puede brindarse por cualquier medio a solicitud del titular.

[67] Artículo 27 de la Ley. No obstante, interesa destacar que en el poco tiempo de vigencia de la Ley esta previsión ha sido aplicada de manera mesurada por la justicia. La sentencia 12 del 14 de noviembre de 2008, el Tribunal de Apelaciones en lo Civil de 5º Turno, rechazó la interpretación extensiva de la seguridad pública efectuada por el Ejército, que pretendía negar el acceso a investigaciones realizadas sobre la conducta sexual de un militar, sometido a Tribunal de Honor por esas presuntas conductas.

[68] Artículo 15 de la Ley. El artículo 16 establece taxativamente cuando corresponderá la eliminación o supresión de los datos (si generan perjuicios a los derechos e intereses legítimos de terceros; si existe notorio error o falsedad; o se contraviene lo establecido por una obligación legal).

[69] Así, se establece también que el afectado podrá impugnar los actos administrativos o decisiones privadas que valoren su comportamiento y tengan por único fundamento un tratamiento de datos personales que ofrezca una definición de sus características o personalidad. Tendrá también derecho a obtener información sobre los criterios de valoración y el programa utilizado en el tratamiento que sirvió para adoptar la decisión.

Por otra parte, en el esquema legal los datos personales, de regla, no pueden comunicarse sin previo consentimiento (siempre revocable) del titular y para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario.[70] Se debe informar previamente al titular sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo. No obstante, no se exige el previo consentimiento en algunos casos como cuando se involucra la "*seguridad o defensa nacional*"; existe necesidad de comunicar los datos por motivo de salud pública (de emergencia o para la realización de estudios epidemiológicos) pero se debe preservar la identidad de sus titulares con mecanismos de disociación adecuados.

c) Datos con régimen especial: sensibles y especialmente protegidos

Los datos sensibles son los que "*revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual*".[71] Sólo pueden recolectarse por razones de interés general autorizadas por ley.

Como principio, nadie puede ser obligado a proporcionarlos y sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular. También pueden tratarse con fines estadísticos o científicos, pero disociados de su titular. Asimismo, la ley prohíbe crear bases de datos con información que directa o indirectamente revele datos sensibles. Se exceptúan de la prohibición las que posean los partidos políticos, sindicatos, iglesias, asociaciones, fundaciones y entidades sin fines de lucro, respecto de sus asociados o miembros, pero la comunicación de estos datos precisará previo consentimiento del titular.

Por otro lado, los datos personales relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por las autoridades públicas competentes. Sin embargo, se dispone que nada de lo establecido en la Ley impedirá a dichas autoridades comunicar o hacer pública la identidad de las personas (físicas o jurídicas) que estén siendo investigadas por, o hayan cometido, infracciones a la normativa, si hay norma que así lo impone o lo creen conveniente.

También se admite la licitud de la recolección de datos relativos a la salud, datos comerciales y crediticios, así como otros datos para fines de promoción y publicidad. En el primer caso, se permite la recolección de

[70] Artículo 17 de la Ley.
[71] Literal E del Artículo 4 de la Ley.

datos por centros sanitarios y profesionales de la salud, cumpliendo las normas de la ley y respetando el secreto profesional.[72]

Respecto a los datos aptos para fijar perfiles con fines promociónales, comerciales o publicitarios (o que permitan establecer hábitos de consumo), sólo se pueden recolectar si figuran en documentos accesibles al público o han sido facilitados por los titulares u obtenidos con su consentimiento. El titular de los datos además de su derecho de acceso sin cargo alguno, podrá siempre solicitar el retiro o bloqueo de sus datos de los bancos de datos.[73]

Asimismo se autoriza el tratamiento de datos para "*brindar informes objetivos*" de carácter comercial. Esto incluye los informes sobre el incumplimiento de obligaciones crediticias, que permitan evaluar la conducta comercial o capacidad de pago. Los datos deben obtenerse de fuentes de acceso público o informaciones facilitadas por el acreedor. Estos datos solo pueden quedar registrados por 5 años, prorrogables una vez.[74] En caso de pago de la deuda, la información debe adecuarse a la nueva realidad un plazo de 3 días desde que el acreedor comunique la cancelación y sólo puede quedar registrada por 5 años.

Por último, en materia de telecomunicaciones, se establece la obligación de los prestadores de servicios de comunicaciones electrónicas de garantizar la protección de los datos personales conforme a la Ley. También deben comunicar al titular de los datos cualquier riesgo particular de seguridad de la red y las medidas a adoptar en su caso.[75]

6.2. Control y vigilancia del sistema de protección

La ley dedica dos capítulos a regular la creación y funcionamiento de las bases de datos (públicas y privadas). Para el control de su cumplimiento se crea la *Unidad Reguladora y de Control de Datos Personales*, organismo desconcentrado del Poder ejecutivo, con amplia autonomía técnica.[76] Sus principales competencias son—además de una enunciación genérica de "*todas las acciones necesarias para el cumplimiento de los*

[72] Artículo 19 de la Ley.
[73] Artículo 21 de la Ley.
[74] Artículo 22 de la Ley.
[75] Artículo 20 de la Ley.
[76] Artículo 31 de la Ley. Este órgano es dirigido por un Consejo de tres miembros y asesorado por un Consejo Consultivo de cinco miembros, integrado por representante de distintos sectores públicos y sociales relevantes (como el Poder Judicial, el Ministerio Público, el Poder Legislativo y un representante del "área académica").

objetivos de la ley"—dictar las normas reglamentarias, registrar y supervisar las bases de datos y eventualmente sancionar los incumplimientos con apercibimientos, multas y suspensiones.

6.3. Habeas data

La tutela del derecho a la protección de datos personales, en concreto los derechos de acceso, rectificación y supresión se efectúa en vía jurisdiccional. Así, la Ley reconoce el derecho de toda persona a "*entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y—en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización—a exigir su rectificación, inclusión, supresión o lo que entienda corresponder*" contra el responsable de una base de datos pública o privada.

La estructura procesal es idéntica a la acción de amparo que existe hace veinte años y que permite tutelar "*cualquier derecho constitucional*" amenazado.[77] Es una estructura sumaria y en la que la pretensión queda resuelta en un breve lapso.[78] No obstante, importa señalar que pese a la semejanza entre la acción de habeas data y el amparo, la jurisprudencia ha señalado que la "identidad del trámite" procesal, no debía confundirse con identidad sustancial de las acciones ya que esta acción era autónoma e independiente del amparo.[79]

De hecho, se resalta en la sentencia que en la Ley de protección de datos personales—a diferencia de lo que hacía la anterior de 2004—no hay siquiera remisión al proceso de amparo, de forma principal ni secundaria. Esto es relevante pues en el derecho uruguayo, la acción de amparo tiene carácter excepcional, residual y supeditado siempre a la existencia de un acto "manifiestamente ilegítimo" de parte del de-

[77] Así, la Sentencia Nº 12, del 14 de noviembre de 2008 del Tribunal de Apelaciones en lo Civil de 5to. Turno reconoció que antes de la previsión expresa del habeas data, la acción de amparo era la vía procesal idónea para proteger el derecho a la intimidad y a la protección de los datos personales.

[78] Artículo 44 de la Ley. Se presenta la demanda y el juez—salvo que fuera manifiestamente improcedente—convoca a la vista pública en un máximo de tres días. En la vista el demandado contesta la demanda y también allí se producirá la prueba ofrecida y alegarán verbalmente las partes. La sentencia se dicta también en la audiencia o a más tardar, a las veinticuatro horas. Igualmente, se prevé que en casos excepcionales se prorrogue la vista por hasta tres días. En cualquier caso, si se extendiera en el tiempo podrían teóricamente adoptarse sin demora medidas provisionales.

[79] Sentencia Nº 12, del 14 de noviembre de 2008 del Tribunal de Apelaciones en lo Civil de 5to. Turno. En este caso, el actor había pretendido el acceso a ciertos datos—antes de la vigencia de la nueva Ley—mediante acción de amparo, que fue desestimada. Más tarde replanteó la acción enmarcándola como habeas data específicamente previsto y se acogió su pretensión.

mandado, que hace bastante difícil obtener una sentencia acogiendo la pretensión. Por ello, su consideración autónoma, tanto legal como jurisprudencial, decididamente contribuyen a la eficacia del habeas data como medio de tutela.

III. Conclusiones

La agrupación y tratamiento automatizado de datos gracias a técnicas informáticas (bases de datos) y la transmisión de datos personales a través de Internet (correos electrónicos, transferencia electrónica de fondos bancarios, comercio electrónico, entre otros) debe suponer la inclusión de mecanismos de defensa para la protección de datos en cada uno de nuestros ordenamientos jurídicos nacionales.

Remitiéndonos a la experiencia europea, la protección de datos personales constituye hoy en día una de las ramas más importantes del Derecho, habiendo alcanzado dentro del escenario jurídico internacional un importante desarrollo, gracias a las iniciativas legislativas europeas. Por ende, se debe tener en cuenta la urgente necesidad que tienen algunos países de América Latina en aprobar una norma de carácter específico en materia de protección de datos; una norma que unifique el marco normativo en esta materia; una norma que no deje vacíos en el derecho interno y que evite ese clima de inseguridad jurídica.

Tras constatar la experiencia europea como raíz legislativa de posteriores desarrollos normativos en Iberoamérica, como es el caso de la República de Argentina, Uruguay y Colombia, consideramos necesaria la inclusión de los preceptos legislativos que regulan derechos relacionados al Derecho de protección de datos personales en aquellos países que carecen de tal regulación, además, esto no implica sólo que se adopte una ley sobre esta materia sino que la misma debe darse en un marco normativo adecuado que incluya aspectos que se remitan directamente a la citada experiencia legislativa, lo que no ha de suponer una mera traslación de la norma española o argentina en la materia, sino una adecuación de tal regulación a las especificidades y la problemática de cada país. Lo que supondría definitivamente la tutela efectiva del derecho a la protección de datos personales, reconociéndolo constitucionalmente e integrándolo en el derecho a la intimidad personal y familiar.

Con relación a la Garantía Constitucional de Habeas Data, reconocida en los diversos ordenamientos jurídicos analizados en este artículo, precisar que el término *Habeas Data* significa "tengas, traigas y conser-

ves los datos" o información personal contenida en los registros. En ese sentido, lo que se persigue es la protección a la información contenida en los registros personales, es decir, en las bases de datos almacenadas en Instituciones Públicas o Privadas. El Habeas Data constituye así un instituto de Tercera Generación, que complementa los derechos de la Primera y Segunda Generación, polarizándose en los derechos personales que protegen la dignidad, la no discriminación, la intimidad, los derechos relativos a la preservación del medio ambiente, defensa del consumidor y los derechos surgidos por la degradación que sufren las personas por los avances de la revolución tecnológica. Estos nuevos derechos surgieron como consecuencia del "poder informático", cuyo uso abusivo afecta y pone en peligro los derechos personales, especialmente el derecho a la intimidad, pues los registros contienen datos sensibles de la persona, relativos a sus creencias religiosas, afiliación política, militancia gremial, antecedentes de salud, laborales o académicos a los que se puede acceder y divulgar fácilmente.

Específicamente en Venezuela, debemos señalar que el proceso constitucional de Habeas Data, se encuentra en un estado incipiente, dado que la ciudadanía no tiene cabal conocimiento del ámbito de aplicación y los derechos tutelados por las instituciones, pese a las jurisprudencias esgrimidas por el Tribunal Constitucional en ocasión de diversos procesos entablados a con el objeto de lograr el acceso a la información tanto pública como privada. Por lo que resultan de capital importancia que el máximo interprete de la constitución aclare el concepto de autodeterminación informativa, como presupuesto de tutela por el proceso de Habeas Data, toda vez que mediante ella se puede solicitar la rectificación y/o actualización de datos contenidos en un banco de registro ya sea de índole público como privado cuando exista un interés valido de por medio por parte del recurrente.

En caso de la legislación Colombiana, queremos señalar que pese a las diferentes críticas que se han realizado a la nueva ley de Habeas Data, lo cierto es que ésta era una ley muy esperada y que aunque regula de manera concreta la protección de datos comerciales y financieros es un paso importante, sobre todo porque en Colombia existía una gran preocupación en cuanto al manejo y los límites que tenían los operadores de la información financiera y crediticia, siendo este el aspecto que más preocupaba a la generalidad. Sin embargo, confiamos en que paso a paso podamos tener una completa protección del Habeas Data en Colombia, acorde con los estándares internacionales y que pueda posicionar a

Colombia en los primeros lugares en cuanto al manejo adecuado de la información.

En Uruguay, la Ley es aún muy reciente para evaluarla adecuadamente. No obstante, como se ve, sigue los lineamientos generales en los principales temas de la Ley española y las legislaciones europeas y brinda una regulación completa del tema. La vía procesal establecida para tutelar estos derechos también parece funcionar adecuadamente como muestra la jurisprudencia de este último año.

Finalmente, indicar que en Perú el "Derecho a la Protección de Datos personales" no existe como tal estructura normativa autónoma. No obstante, el derecho a la intimidad personal y familiar del ciudadano, en íntima conexión con el derecho de Protección de Datos, es un derecho personalísimo que se encuentra protegido por la Constitución Política de 1993 y existen una serie de Leyes que protegen la intimidad de las personas, en el ámbito de sus derechos constitucionalmente reconocidos.