Responsabilidad derivada de informes crediticios

Doctorando: EDUARDO MOLINA QUIROGA

Directora de Tesis: Dra. AÍDA R. KEMELMAJER de CARLUCCI

Introducción

Las bases de datos con información sobre el cumplimiento de las obligaciones, sobre todo comerciales, existen desde hace largo tiempo. Por lo menos eran conocidas ya en épocas de nuestra infancia, con el nombre de “clearing de morosos”. En esa época, su difusión estaba limitada a un pequeño círculo de comerciantes, y era sencillo superar las consecuencias de integrar estos listados. Bastaba con cancelar la deuda u obtener una renegociación de plazos, para obtener una certificación del “clearing” y recuperar la capacidad de obtener crédito.

La irrupción de las modernas tecnologías de la informática y las comunicaciones ha impactado en varios ámbitos del Derecho, y obliga a reflexionar de modo especial sobre cómo responder eficazmente a la demanda permanente de hacer justicia.

Pensemos en los documentos en soporte electrónico o digital, y en dicho contexto, el fenómeno de la llamada “firma digital”, o el correo electrónico, que nos replantean el concepto de “documento”, tanto desde el punto de vista de la forma de los actos jurídicos, como desde la perspectiva de la eficacia probatoria de dichos medios.

Los programas de computación y las bases de datos han exigido, luego de un debate largo y profundo, resolver el tema de su protección legal, por ahora atendido en la ley de derechos de autor.

La contratación de bienes y servicios informáticos genera nuevos institutos, como la noción de sistema, una nueva visión de la entrega, entendida como un

conjunto complejo de actividades que excede largamente la clásica tradición, e incorpora novedades como el “test de aceptación”. A ello debe sumarse la relevancia de la etapa precontractual, con nuevos paradigmas de la buena fe, que incluyen el deber de definir las necesidades del usuario y el deber de asesoramiento y consejo por parte del proveedor. También una actualización del error esencial como vicio de la voluntad, las garantías de compatibilidad, modularidad, escalabilidad y migrabilidad de datos, entre otras novedades.

Los contratos entre ausentes han adquirido una dimensión muy específica con el llamado “comercio electrónico”, y por supuesto que la gran red conocida como “Internet” ha trastocado muchos de nuestros conceptos tradicionales, sobre ámbito de aplicación de la norma, territorialidad, competencia, entre otros interrogantes aún abiertos.

Las agresiones a los sistemas de información, ya sea por medio de archivos autoejecutables con aptitud para provocar desde insignificantes molestias hasta la inutilización absoluta de la información y sus soportes (virus, gusanos, etc), así como las intrusiones en los servidores y redes, tanto públicas como privadas, que llevan a cabo “hackers”, “crackers”, etc., para no mencionar al correo no deseado (”spam”) nos revelan otros aspectos del impacto de la informática y las nuevas tecnologías.

Los informes crediticios

En ese contexto, la protección de los datos personales es sin duda una institución hija de dicho impacto y el tema que abordamos está inserto en esa problemática general, aunque con algunos perfiles propios.

El tratamiento de datos personales ha evolucionado desde una visión que lo considera un aspecto del derecho a la intimidad hasta la noción de autodeterminación informativa, o el derecho autónomo a la protección de los datos personales. En este devenir, la actividad de tratamiento de datos personales, género en el que la especie “informes crediticios” presenta caracteres distintivos, ha motivado que se elaboren una serie de principios rectores que apuntan a establecer cuando es lícita esta actividad.

Uno de los mencionados principios es la exigencia de “calidad” en el tratamiento de datos personales, consagrado en normas internacionales, legislaciones

nacionales extranjeras y en nuestra propia ley 25.326.

La difusión de datos que informan erróneamente sobre el cumplimiento de obligaciones dinerarias, por parte de entidades bancarias y empresas de informes crediticios tiene consecuencias en el terreno de la responsabilidad civil.

Nuestro trabajo apunta a establecer que los informes crediticios están sometidos, en general –como todo tratamiento de datos personales- al principio de calidad (art. 4, Ley 25.326) y que la no observancia de esta pauta convierte en ilícita a la conducta del responsable de la base de datos.

Pero además, la ley argentina ha regulado especialmente a los informes crediticios en el artículo 26 de la mencionada Ley 25.326, con exigencias particulares, que deben ser interpretadas en el contexto del principio de calidad antes citado.

En este trabajo se ha relevado la legislación nacional y gran parte de la internacional y de otros países, que se ha ocupado en forma directa o indirecta de este problema, así como jurisprudencia nacional y extranjera considerada relevante y la opinión de la doctrina especializada, que por cierto es abundante en la materia.

La hipótesis de trabajo que nos ha guiado es la existencia de responsabilidad por los daños y perjuicios derivados no solo los informes crediticios erróneos, sino también de un manejo inadecuado de los datos de carácter personal referidos al cumplimiento o incumplimiento de las obligaciones dinerarias, y los informes sobre solvencia patrimonial y riesgo crediticio. Al hablar de un manejo inadecuado estamos refiriendonos a la no observancia del principio de calidad (art.4, Ley 25.326)

Ubicación del tema en el Derecho

El tema resulta difícil de encasillar en alguna de las áreas de la dogmática jurídica con exclusividad, aunque hemos señalado al Derecho Civil como la más aproximada.

La cuestión tiene puntos de contacto con el Derecho Constitucional, por la incorporación en la Constitución Nacional y en varias constituciones provinciales del llamado “habeas data”, garantía que se encuentra en cartas fundamentales de otros países. También se vincula con el Derecho Comercial, sobre todo en materia de

informes de cumplimiento de obligaciones dinerarias y solvencia crediticia. Asimismo, el moderno Derecho del Consumidor aparece cada día más implicado, y lo mismo cabe señalar con respecto al Derecho Bancario.

Denominamos “Protección de datos personales” a un conjunto de reglas que apuntan a establecer cómo debe actuarse en el tratamiento de información referida a personas individualizadas o individualizables. Una especie de este género lo constituyen los informes que contienen datos sobre el cumplimiento o incumplimiento de obligaciones dinerarias, así como otros factores en base a los cuales se determina la viabilidad de otorgar crédito a un sujeto.

Los problemas derivados del tratamiento automatizado de información de carácter personal se vincularon en un inicio con el derecho a la intimidad, o en su versión más amplia, con el derecho a la privacidad, para ir evolucionando hacia un concepto diferente, pero no excluyente, más ligado a la libertad personal, que ha recibido la denominación de “autodeterminación informativa”.

El almacenamiento y recopilación de datos de carácter personal no es una actividad que haya surgido con la irrupción de la informática. Por el contrario, desde antaño, la existencia de los ficheros manuales con datos de carácter personal auguraba los riesgos de datos incompletos, falsos o utilizados para un propósito diferente para el cual se habían recogido. Sin embargo, la preocupación ha crecido a partir del tratamiento automatizado de esta información personal, como consecuencia de la aplicación de tecnologías informáticas.

La reforma de 1994 estableció en el artículo 43, párrafo tercero de la Constitución Nacional que “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 aquellos. No podrá afectarse el secreto de las fuentes de información periodística.”

Protección de datos personales

La información es un concepto complejo, que se integra con “datos”. El dato es

el “antecedente necesario para llegar al conocimiento exacto de una cosa” y la información puede definirse como el proceso de adquisición de conocimientos que permiten precisar o ampliar los que ya se tenían sobre una realidad. Cuando el segmento de la realidad que es objeto de información es una persona, estamos frente a datos de carácter personal.

La irrupción de la informática obligó a un replanteo del derecho a la intimidad, por la estructuración de grandes bancos de datos de carácter personal y la posibilidad del entrecruzamiento de la información contenida en los mismos. La toma de conciencia sobre esta circunstancia llevó a sostener que el derecho a la intimidad no podía seguir considerándose simplemente la ausencia de información acerca de nosotros en la mente de los demás (el “déjenme solo”), sino que debía adquirir el carácter de un control sobre la información que nos concerniera, o sea la facultad del sujeto de controlar aquella que sobre él figurara en los bancos de datos, concepto que ha sido denominado “autodeterminación informativa”.

Una vez relevados los principios y reglas que rigen en dicho campo, se establecerán las consecuencias que se derivan de su inobservancia, en particular la responsabilidad derivada de la difusión de informes sobre solvencia crediticia.

Importancia del tema

El tratamiento de los datos personales tiene una gran incidencia en la actividad económica, y afecta en especial un aspecto intangible pero muy sensible del desarrollo empresario, como es el prestigio e imagen de un comerciante.

La imagen del empresario no solo se construye en base a sus aciertos industriales, mercantiles o de servicios, sino también sobre la percepción que sus clientes y proveedores, así como las entidades crediticias, tienen acerca de su comportamiento en relación a las obligaciones dinerarias.

Un dato de relevancia relativa, como sería la solicitud de radicación de un juicio (que quizás nunca se haga efectivo), la inserción en un listado de deudores morosos (erróneo, desactualizado, e incluso impertinente), o la pérdida de instrumentos de uso corriente (cuentas corrientes, tarjetas de crédito, etc.), pueden dañar este aspecto intangible del activo empresario, que es su prestigio e imagen.

Pero estas consecuencias, también se extienden a los consumidores en general, que pueden ver restringido su acceso al crédito, en forma arbitraria, por la difusión de datos personales erróneos. Se afecta lo que los colombianos por ejemplo, llaman el “buen nombre” de una persona. Alguna jurisprudencia nacional ha denominado a esta consecuencia negativa, “lesión al crédito”.

Uno de nuestros puntos de investigación ha de ser la estructura de los informes sobre riesgo crediticio, en los que suelen mezclarse los datos referidos a la solvencia patrimonial, con los informes sobre cumplimiento o incumplimiento de obligaciones de contenido patrimonial, sin respetar el principio de calidad de los datos (art. 4, Ley 25.326).

La circunstancia de ser incluido en un listado de deudores morosos en forma inexacta ocasiona un daño que se revela por sí mismo, sin necesidad de acreditarlo, ya que puede valorarse como notorio. Es conocido en general, por todos quienes desarrollan actividades financieras, comerciales, industriales, profesionales o laborales, el efecto negativo que tiene para una persona aparecer como deudor moroso en una publicación como la que efectúan las empresas que brindan informes sobre solvencia o riesgo crediticio.

Otro de los temas a abordar está referido a la difusión o publicidad de juicios patrimoniales, por parte de tribunales, con una visión crítica de algunas modalidades que se han desarrollado en nuestro país y se apartan del principio de calidad en el tratamiento de los datos personales.

Se trata de una problemática que registra diversas regulaciones en el derecho comparado y donde puede advertirse que en el tratamiento de datos personales referidos al cumplimiento de obligaciones dinerarias, e incluso a los informes de riesgo crediticio, es importante el consentimiento del titular.

Aún cuando en nuestro derecho positivo esté excusado el consentimiento previo del titular de los datos, en materia de informes crediticios, la omisión de información o conocimiento, afecta el ejercicio de los derechos de acceso, rectificación y cancelación, consagrados en el artículo 43, párrafo 3º de la Constitución Nacional. También es posible vincular esta situación con el derecho a una información adecuada, oportuna y veraz con que cuenta todo consumidor (art. 42, CN).

Partiendo del factor de atribución subjetivo basado en la culpa o negligencia, hay que considerar el agravamiento de la responsabilidad del gestor de una base de datos, en función de su profesionalidad.

Ello no excluye que en base a consideraciones derivadas del riesgo, proceda establecer un factor de atribución objetivo, o por emplazamiento, aún cuando en el texto positivo argentino no se reconozca como causa a la “actividad riesgosa”, sino al riesgo de la cosa.

Nuestra hipotesis es que el acento debe ponerse en la obligación de un gestor de una base de datos personales de observar y aplicar en el tratamiento, cesión y difusión de esta información, los principios de licitud, finalidad, calidad, consentimiento e información, que se despreden tanto de la Ley 25.326, como de los ámbitos y las normas internacionales en los que Argentina ha solicitado ser considerada país que brinda protección equivalente en esta materia (Directiva 46/95 CE).

Para establecer quienes son legitimados pasivos frente al reclamo resarcitorio por los daños ocasionados por informes crediticios erróneos, o en los que no se ha observado el tratamiento de calidad, se analiza qué sujetos pueden estar incluidos en la categoría de responsables de bancos de datos personales. La situación alcanza no sólo a las empresas que brindan informes de riesgo crediticio, sino también a los bancos, a las empresas emisoras de tarjetas de crédito y al Banco Central de la República Argentina.

Puede presentarse también una eventual responsabilidad de quien adopte decisiones con efectos jurídicos sobre una persona o que le afecte de manera significativa, cuando se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, no solo en el ámbito público, extremo ya contemplado en la ley argentina, sino también en las relaciones entre particulares.

Establecidos estos presupuestos, se analizan las consecuencias que, en el ámbito del Derecho de Daños tienen los informes crediticios erróneos, tanto cuando el hecho generador del daño se produzca en el ámbito contractual como extracontractual, y la procedencia del resarcimiento del daño moral, que alguna jurisprudencia ha considerado un hecho notorio, así como el daño material, incluida la

llamada “pérdida de chance”.

En definitiva, nuestra tesis apunta a establecer que los informes sobre cumplimiento de obligaciones dinerarias, así como los informes sobre la solvencia crediticia de las personas, integran el universo de los datos de carácter personal, y que en consecuencia, deben merecer un tratamiento ajustado a los principios de calidad, consentimiento e información. Que cuando ello no ocurre, estamos frente a una conducta antijurídica.

Que esta conducta, por parte de entidades financieras, incluido el propio Banco Central, y de las empresas dedicadas a proveer esta información a terceros, constituye una conducta antijurídica, generadora de daño resarcible.

También nos proponemos demostrar que incurren en una conducta antijurídica, que denominamos “uso arbitrario de la información personal” (contenida en informes sobre cumplimiento de obligaciones dinerarias o de riesgo crediticio), quienes adopten decisiones que afecten a una persona, basados exclusivamente en informes obtenidos de un tratamiento automatizado de los datos.

Nuestra hipótesis de trabajo es que existe responsabilidad en cabeza de todos aquellos sujetos que manejan bases de datos de carácter personal, referidas al cumplimiento de obligaciones de contenido patrimonial, cuando el tratamiento de esta información se lleva a cabo sin tener en cuenta los principios previstos en el articulo 4 de la Ley 25.326 (LPDPA), relativos a la calidad del dato.

La conducta antijurídica consiste en realizar el tratamiento de estos datos sin observar los principios mencionados, que exigen que los datos sean ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

En el caso de los llamados “informes crediticios”, el principio de calidad se especifica con la limitación del art. 26 inc.4), Ley 25.326 en cuanto “sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados”.

Son legitimados pasivos no solo las empresas de informes crediticios, sino todos aquellos que almacenan y brindan informes, especialmente los bancos y

entidades financieras, el Banco Central de la República Argentina, y el Poder Judicial en la medida que difunda información de esta naturaleza. Nos referimos específicamente a los listados de juicios distribuidos por la Cámara Nacional de Apelaciones en lo Comercial y otros tribunales del país.

En todos estos casos, consideramos que existe una obligación tácita de seguridad, que en el caso que tratamos se implementa observando las reglas de "calidad en el tratamiento de los datos". Ella exige que la información que se trate sea cierta, adecuada, pertinente y no excesiva en relación al ámbito y finalidad para la que se hubiera obtenido, y en el caso de los llamados "informes crediticios", los datos sean significativos para evaluar la solvencia económico-financiera de los afectados.

Sobre esta premisa vamos a analizar las consecuencias que se derivan en el terreno de la responsabilidad civil, con motivo de la difusión de datos que informan errónea o inadecuadamente sobre el cumplimiento de obligaciones dinerarias, por parte de entidades bancarias, incluido el Banco Central de la República Argentina, las empresas de informes crediticios y el Poder Judicial, en cuanto no adecuen su actividad, en esta materia, a los principios de la Ley 25.326 (LPDPA).

Capítulo 1. Protección de los datos personales: del derecho a la intimidad a la autodeterminación informativa

Sumario: El derecho a la intimidad o vida privada. Antecedentes. Concepto. Reconocimiento normativo. Protección de datos personales. Concepto de datos personales. Impacto de las nuevas tecnologías. Autodeterminación informativa. Antecedentes

La vinculación entre el derecho a la intimidad, o en su versión más amplia, el derecho a la privacidad, con el llamado "habeas data" constituye una referencia insoslayable en nuestra doctrina[1].

La Ley argentina Nº 25.326 de Protección de Datos Personales y Habeas Data incursiona en este terreno, aunque amplía el objeto a la protección integral de los datos personales, para garantizar, además del derecho a la intimidad, el derecho al honor, así como el acceso a la información conforme a lo establecido en la

[1] Ver al respecto Altmark, Daniel R. y Molina Quiroga, Eduardo, "Habeas Data y reforma constitucional", I Congreso Internacional de Informática y Derecho, Mérida; España 1995, En Informática y Derecho, UNED, Dir. Valentín Carrascosa López, Vol. 11 y 12, Ídem: "Habeas Data", en LA LEY 1996-A, 1554. Cf. Bergel, Salvador D. "El Habeas data: instrumento protector de la privacidad", en Revista de Derecho Privado y Comunitario, Ed. Rubinzal Culzoni Nº 7, Derecho Privado en la reforma constitucional, Santa Fe, 1994; Nuestras ponencias: El derecho a la intimidad y las bases de datos personales...", Primeras Jornadas de Derecho Civil, Morón, 1994; Campanella de Rizzi Elena M. y Stodart de Sasim, María, "Derecho a la Intimidad e Informática", LA LEY, 1984-B-667; Beckerman, Jorge, "Banco de Datos y responsabilidad objetiva", Congreso Internacional de Informática y Derecho, AABA-ADIJ, Bs. As. ,octubre 1990, p.390. Más recientemente, Slaibe, María Eugenia y Gabot, Claudio, "Hábeas data: su alcance en la legislación comparada y en nuestra jurisprudencia", LA LEY, 2000-B, 27; y otros artículos de los mismos autores, vinculándolo siempre con la doctrina de "Ponzetti de Balbín"; Ekmekdjian, Miguel Angel, "El 'habeas data' en la reforma constitucional", LA LEY, 1995, E-946; Bianchi, Alberto, "'Habeas data' y derecho a la privacidad", ED, 161-866; Egües, Alberto J., "El "right to privacy" y el "habeas data" comercial", LA LEY, 2000-C, 1272; Bayo, Oscar, "Habeas-data. Un derecho constitucional en su adecuado cauce como resultado de una decisión elogiable.", LLC 1995, 945; Cafferata, Juan Carlos, "La acción de Hábeas Data", LLC, 1996, 313; Muruzábal, Claudio, "Más allá del hábeas data, la otra cara de la privacidad" Infobae, 28/11/2003; entre muchos otros.

Constitución Nacional (art. 43)[2].

También se ha relacionado al habeas data con el derecho a la identidad personal[3], a la imagen[4], el honor[5] y la reputación[6].

Por esta razón, vamos a reseñar previamente algunos aspectos del derecho a la intimidad, para luego analizar el fenómeno de la protección de datos, tal como lo concebimos.

1.1. El derecho a la intimidad o vida privada

1.1.1. Antecedentes

El reconocimiento del llamado derecho a la intimidad como bien susceptible de tutela jurídica parece remontarse a fines del siglo XIX, ya que hasta entonces era considerado exclusivamente como un hecho resultante de la costumbre social o bien

---

[2] El Art. 1 de la LPDPA dice: "La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional."

[3] Palazzi, Pablo A., "El Habeas data en el derecho argentino", Revista Electrónica Internacional Venezolana de Derecho e Informática-REIVDI Nº 1, enero-abril 1999, http://www.omdi.et/; Rivera, Julio César, "Instituciones de Derecho Civil", t. II; Guastavino, Elías, "Irregular tramitación de la ley de la intimidad", LA LEY, 1975-A, 1270; Vanossi, Jorge R., "El hábeas data: no puede ni debe contraponerse a la libertad de los medios de prensa", ED, 159-948, esp. pág. 949, entre otros

[4] Si bien el planteo es más amplio, mencionan este aspecto Álvarez B. de Bozo, Miriam; Ávila Hernández, Flor María; Peñaranda Quintero Héctor Ramón, "La libertad informática: derecho fundamental en la Constitución Venezolana", http://biblioteca.tsj.gov.ve/cgi-win/be_alex.exe?Autor=Alvarez+B.+de+Bozo,+Miriam.&Nombrebd=btsj&TiposDoc=M/ Universidad del Zulia (LUZ). Maracaibo. Venezuela, Organización Mundial de Derecho e Informática (OMDI). Maracaibo. Venezuela.

[5] Así lo hace el Art.1 de la LPDPA supra citada, y puede asimilarse en un sentido lato a la reputación

[6] Puccinelli, Oscar Raúl, "Protección de datos de carácter personal", Ed. Astrea, Buenos Aires, 2004.

del denominado respeto moral debido a la persona[7].

Con motivo de los inconvenientes que le estaban ocasionando determinadas publicaciones periodísticas, un joven abogado de Boston, Samuel D.Warren[8] en colaboración con Luis D.Brandeis[9] publican el trabajo titulado “The right to Privacy” en la "Harvard Law Review"[10] , ensayo en que los autores plantean que todo individuo tiene derecho a "ser dejado en paz", o a "ser dejado tranquilo", o a "que lo dejen solo", o a "no ser importunado"[11], es decir plantean la necesidad del reconocimiento de la existencia de una vida íntima, requiriendo el arbitrio de los medios adecuados para protegerla al modo en que se protege la propiedad privada[12].

Se menciona también, investigando los orígenes, que Kohler, en Alemania, se había referido ya en 1880 a un "derecho individual que protege el secreto de la vida

---

[7] Frossini, Vittorio, "Informática y Derecho", Ed.Themis, Bogotá, Colombia, 1988, p. 65 y otros; Rivera, Julio, ob.cit y en "Derecho Civil, Parte General, Temas". Ed. Abeledo Perrot, Bs. As. , 1987; Fernández Sessarego, Carlos, "El Derecho a la Identidad Personal y otras figuras", Ed. Astrea, Bs. As., 1992, p.153; v.adde: Díaz Molina, Iván M., "El derecho a la vida privada. Una urgente necesidad", LA LEY, 126-981, 984; Leonfanti, María Antonia, " El derecho a la intimidad en la Argentina ", LA LEY, 1975-B-1319.

[8] Warren se había casado con la hija del Senador Bayard y había principiado a llevar una vida de lujo y rumbosa, hecho que atrajo la curiosidad y chismografía de la llamada prensa amarilla, hasta el punto de convertirse en un escándalo, sobre todo en la puritana sociedad bostoniana de fin de siglo. Ver adde: Egües, Alberto J., “El "right to privacy" y el "Habeas data" comercial”, LA LEY, 2000-C, 1272, donde se brindan otros interesantes detalles de este antecedente. También Puente de la Mora, Ximena, “Privacidad de la información personal y su protección legal en Estados Unidos”, Revista Derecho Informático Alfa Redi Nº 097, agosto 2006.

[9] Brandeis luego llegó a ser Juez de la Corte Suprema de los EE.UU.

[10] Harvard Law Review, vol. IV, No.5, 1890, pág. 193/220. También Warren, Samuel y Brandeis, Louis, “El derecho a la intimidad”, Civitas, 1995, Madrid.

[11] Leonfanti, María, op.cit. supra.

[12] En el citado artículo, decían "La prensa ha sobrepasado en todo sentido las fronteras claramente demarcadas a la prudencia y la decencia. El chisme no es ya el recurso del ocioso o del corrupto, sino que se ha convertido en un comercio que se realiza con provecho y con solvencia. Para satisfacer un gusto espurio se expanden los detalles de las relaciones sexuales desde las columnas de los diarios. Para dar ocupación al indolente se llenan columnas con chistes y habladurías que solamente se pueden conseguir introduciéndose en el círculo de la familia..." (citado por Díaz Molina, Iván, op.cit.)

íntima de la publicidad no autorizada"[13].

Pero en nuestro medio es común señalar que fue el trabajo de Warren y Brandeis aquél que por primera vez reunió y analizó una serie de casos de los cuales podía concluirse la existencia de un derecho más amplio que protegía a los individuos, frente a lo que calificaran como crecientes excesos de la prensa. Este texto tiene como antecedente directo la publicación del Juez norteamericano Thomas A. Cooley, quien en 1873 editaría su obra "The elements of Torts", y cuya trascendencia se debe a la definición que el autor dio a la palabra "intimidad", entendida ésta como "*the right to be let alone*", concepto que la doctrina tradicionalmente entiende en castellano como "el derecho a ser dejado en paz", o "el derecho a ser dejado a solas"[14].

Se ha sostenido que el desarrollo del concepto de Derecho a la intimidad y a la vida privada, en el marco ideológico liberal se presenta como un derecho a la libertad, en cuanto derecho del individuo a hacer lo que le parece, esto es, a estar sólo, a no ser incomodado, a tomar decisiones en la esfera privada sin la intervención estatal. Esta no injerencia incluye, entre otras, las decisiones referidas a la libertad sexual, la libertad de actuar libremente en el interior del propio domicilio, la libertad de revelar o no las conductas íntimas y la libertad a la identidad. Esta concepción se desarrolla a fines del siglo XVIII al calor de un marco ideológico en el cual el Estado llega a ser visto como un "enemigo". El concepto de libertad tiene un sentido negativo (libertad negativa) que significa no sufrir interferencias de otros (un derecho pasivo), y cuanto más amplia es el área de no-interferencia, más amplia es la libertad. Aún cuando se admite que la libre acción de los hombres debe ser limitada por la ley, debe preservarse un área mínima de libertad personal que no debe ser violada, a fin de preservar el desarrollo mínimo de sus facultades naturales. Ello explica la necesidad

---

[13] Fernández Sessarego, op.cit., p.153 y ss.
[14] Colley, Thomas, "The elements of Torts", 2a edición, 1988, p. 29. Proser y Keeton, "The Law of Torts"; p. 849, 5ª edición, West Publishing, St. Paul, USA, 1984, citados por Egües, ob.cit. supra. Ver también, Cerda Silva, Alberto, "Autodeterminación informativa y leyes de protección de datos", Revista chilena de Derecho Informático Nº 3 Diciembre 2003, Universidad de Chile, Facultad de Derecho, http://www.derechoinformatico.uchile.cl/CDA/der_informatico_completo/...

de trazar una frontera entre el área de la vida privada y la de la autoridad pública.[15]

Otra fuente mencionada del artículo de Warren y Brandeis Warren es un artículo escrito también en 1890 por E. L. Godkin, un famoso comentarista social de la época, en el que se afirmaba que: “la privacidad es un producto moderno, uno de los lujos de la civilización, el cual no sólo pasaba desapercibido, sino que era desconocido en las sociedades primitivas... el principal enemigo de la privacidad en la vida moderna es el interés de la gente de conocer los asuntos personales que en días después los periódicos divulgaran como chisme...” agrega Godkin que “mientras que la comunicación fue solamente oral se divulgaban los hechos únicamente de persona a persona, sobre un área pequeña y eran divulgados solamente en el círculo inmediato de conocidos... mientras que ahora la comunicación a cerca de la privacidad es impresa, y fabrica una víctima con todos los defectos, mismos que son conocidos cientos de miles de millas de su lugar de origen, llevando la información con todos los detalles de una persona”.[16]

En la elaboración del célebre artículo titulado The Right to Privacy, publicado en The Harvard Law Review también en 1890, Warren y Brandeis citan el artículo de Godkin, presentando además gran similitud en sus razonamientos. No obstante esta semejanza, en algunos aspectos defieren en un punto importante; mientras Godkin entiende que la solución al problema que presenta la protección de la privacidad de los individuos pasa por la esperanza de que cambie la actitud de la gente al respecto, Warren y Brandeis fieles a su formación como abogados, afirmaron que se podía proteger la privacidad mediante la ley.[17]

La característica saliente de este "derecho a la intimidad", según la descripción original que del mismo efectuaran Warren y Brandeis, consistía en que no se trataba de un derecho reconocido al individuo frente al poder público estatal, sino de un

---

[15] Riande Juárez, Noé Adolfo, “La desprotección de los Datos Personales”, Centro de Información Documental, Infoleg: Derecho y Nuevas Tecnologías, http://infoleg.mecon.gov.ar/default1.htm/

[16] Véase Adams Elbridge, L., “The Right to Privacy and its Relation to the Law of Libel”, 39 American Law Review, 37, January – February 1905. y págs. 37 a 58, citado por Puente de la Mora, ob.cit. supra.

[17] Puente de la Mora, ob.cit. supra.

derecho reconocido a los individuos frente a otros individuos particulares conformados, sustancialmente, por los medios de prensa a través de los cuales se producía la "invasión a la intimidad"[18].

Se trataba de un derecho individual de naturaleza infraconstitucional cuya infracción por otro particular y sustancialmente por la prensa, daba derecho a reclamar el resarcimiento de los "daños y perjuicios" ("torts") cuya existencia sólo podía considerarse tal, en la medida que no hubiese mediado un previo "consentimiento" del damnificado por la publicación[19].

No se trataba, desde luego, de la posibilidad de impedir una publicación que no contara con el "consentimiento" de aquellos a quienes la misma se refería, sino que la ausencia de tal recaudo hacía presumir la existencia de una invasión a la intimidad en los supuestos de haberse utilizado el nombre o el retrato de una persona, con fines comerciales y "sin su consentimiento escrito"[20].

Esta limitada forma de reconocimiento del derecho a la intimidad, como un derecho individual a obtener un resarcimiento respecto de aquellos individuos particulares que no respetaran el "derecho a ser dejado a solas", fue adoptada por la ley del Estado de Nueva York en 1903[21] y, con similares restricciones, fue seguida por leyes de los restantes estados norteamericanos[22].

La Constitución de Estados Unidos no utiliza en ninguno de sus artículos y enmiendas, la palabra "*privacy"*, que se emplea en el derecho de ese país para definir el derecho en cuestión. Sin embargo y en palabras del propio Louis Brandeis cuando ya integraba la Corte Suprema norteamericana, este "derecho a ser dejado a solas, es el más comprensivo de los derechos y el más valioso para los hombres civilizados"[23].

---

[18] Egües, ob.cit. supra.
[19] Egües, ob.cit. supra.
[20] Egües, ob.cit, supra.
[21] NW York Sesiones Las 1903, ch.132, && 1-2. Actualmente enmendada en 1921 (Cfr., Egües. ob.cit. supra).
[22] Se ha dicho que, hasta 1980, el único estado norteamericano que no lo reconocía era Rhode Island. Note, "Tort Recovery for Invasion of Privacy", 1980, 59 Neb. L. Rev. 808. (Cfr., Egües, ob.cit.supra).
[23] Brandeis, Louis, en su disidencia en "Olmstead vs. United States"; 277 US 438, 478

O, como se dijo en otro fallo, el concepto conlleva el "hecho moral de que una persona se pertenece a sí mismo y no a otros, ni a la sociedad como un todo[24]. El enfoque de raigambre constitucional del derecho a la intimidad que denotan tales expresiones se vincula históricamente con el principio de la inviolabilidad del "domicilio" basado en el principio inglés según el cual "la casa de un hombre es su castillo". Quizás la mejor versión de ese principio de derecho inglés pueda atribuirse a William Pitt, cuando proclamara que "el hombre más pobre puede, en su casa, enfrentar a todas las fuerzas del Rey. Su casa puede ser frágil; su piso puede temblar; el viento puede soplar a su través; la tormenta puede entrar; la lluvia puede entrar, pero el Rey de Inglaterra no puede entrar y todas sus fuerzas no pueden cruzar el umbral de esa casa en ruinas"[25].

Se afirma que la primer persona en vincular el principio de la intimidad de la casa de un hombre con el principio de su inviolabilidad habría sido un miembro del Consejo Privado del Rey, en 1589, quien basándose en la Carta Magna sostuvo que era un símbolo de la libertad frente a cualquier autoridad, sujeta por igual al imperio de la ley[26]. El principio "la casa de un hombre es su castillo" fue invocado por los líderes de la revolución norteamericana como opuesto a una ley impositiva de Massachussets de 1754 por la que, en forma genérica, se autorizaban los allanamientos indiscriminados ("general warrants") y el interrogatorio de personas acerca de "la cantidad de rhum, vino y otras bebidas alcohólicas que hubiese consumido en su casa el año anterior, gravando ese consumo por galón"[27]. Este notorio exceso tributario,

---

(1928). http://supreme.justia.com/us/389/347/case.html.

[24] "Thorburg vs. American College of Obstetricians & Gynecologsgist" 106 S.Ct 2169, 2187 n.5 (1986). http://supreme.justia.com/us/389/347/case.html.

[25] Discurso pronunciado en 1763, en el Parlamento, según Lasson, Nelson B., "The History and Development of the Fourth Amendment to the United States Constitution", Baltimore; John Hopkins University Press, 1937, ps. 49-50. El autor aclara que existen numerosas versiones de la expresión y que su fecha no es segura. La traducción transcripta es de Egües, en el artículo que venimos citando. Una versión similar brinda González, Joaquín V. “Manual de la Constitución Argentina”, actualizado por Quiroga Lavié, Humberto, Ed. La Ley, Buenos Aires, 2001. atribuyendo la expresión a Lord Chattam.

[26] Levy, Leonard W., "Origins of the Fourth Amendment"; Political Science Quarterly, Vol. 114, N° 1, p. 84, Academy of Political Science, New York, 1999, citado por Egües, ob.cit.supra.

[27] Ídem nota anterior.

habría sido el origen de la resistencia de los colonos que, en el ámbito de cada Estado, adoptaron sucesivas "Declaraciones de Derechos" reflejadas finalmente en la Cuarta Enmienda de la Constitución norteamericana, ratificada en 1791, según la cual "el derecho del pueblo a estar seguro en sus personas, domicilios, papeles y efectos contra pesquisas y aprehensiones arbitrarias será inviolable y no se expedirán al efecto mandamientos que no se apoyen en un motivo probable, estén corroborados mediante juramento y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas"[28].

Sin embargo, la expansión de la concepción del derecho a la intimidad desde el ámbito del derecho privado hacia su interpretación como un derecho subjetivo de índole constitucional, no se produjo sino hasta la finalización de la Segunda Guerra Mundial.

Hasta allí, la jurisprudencia de la Corte Suprema norteamericana había sido pacífica en sostener que "la seguridad proporcionada por la enmienda cuarta contra pesquisas y aprehensiones irrazonables sólo se aplica a la acción gubernativa[29] en tanto "no es invadida por actos ilegales de individuos en los cuales el gobierno no tiene parte"[30].

La cuestión fue explícitamente considerada por la Suprema Corte norteamericana al resolver en 1967 el precedente "Katz"[31], donde señaló que la cuarta Enmienda de la Constitución norteamericana, relativa a la inviolabilidad del domicilio, debía ser interpretada como destinada a "proteger personas y no lugares", lo que

---

[28] El texto literal expresa: "The right of the people to be secure in their persons, houses, papers and effects, against ureasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable cause, supported by oath of affirmation and particularly describing the place to be searched and the persons or things to be seized". La traducción corresponde a Egües, ob.cit.supra.

[29] "Smith vs. Maryland", 18 How, 71,76 (1855) Traducción de Amadeo, Mario, en "La Constitución de los Estados Unidos de América Anotada con Jurisprudencia", Ed. Kraft, Buenos Aires, 1949. El traductor utilizó la expresión "perquisiciones y secuestros" que se sustituyó por "pesquisas y aprehensiones" por entenderla más apropiada.(Conf. Egües, ob.cit).

[30] "Burdeau vs. McDowell", 256 US 298, 465 (1921), http://supreme.justia.com/us/256/465/case.html/

[31] "Katz vs. United States"; 389 US 347,351 (1967), http://supreme.justia.com/us/389/347/case.html.

configuró una sustancial expansión del derecho a la intimidad del ámbito del derecho privado hacia un universo más vasto en el que arraigaba una "área constitucional protegida"[32] de intimidad individual.

1.1.2. Concepto

Aprehender la noción de intimidad no resulta un tema simple por la multiplicidad de de definiciones o descripciones que la doctrina ha efectuado sobre este derecho sujetivo[33]. Se lo denomina igualmente derecho a la vida privada y aún derecho a la privacidad.

Díaz Molina dice que “es el derecho personal que compete a toda persona de sensibilidad ordinaria, de no permitir que los aspectos privados de su vida, de su persona, de su conducta y de sus empresas, sean llevados al comentario público o con fines comerciales, cuando no exista un legítimo interés por parte del Estado o de la sociedad”.[34]

Cifuentes lo define como “el derecho personalísimo que permite sustraer a la persona de la publicidad o de otras turbaciones de su vida privada, el cual está limitado por las necesidades sociales y los intereses públicos”[35], y que la expresión “intimidad” está empleada como sinónimo de vida privada, de soledad total o en compañía, pero que lo esencial en esta protección no es el conocimiento sino la publicidad de estos hechos, o cualquier hostigamiento o perturbación a este estado.[36]

Kemelmajer cita también a un congreso de juristas de países nórdicos, que asumió la definición del profesor Stromholm, considerando a la intimidad como “el

---

[32] Conf. Egües, ob.cit.supra.
[33] Kemelmajer de Carlucci, Aída R., en Belluscio, Augusto C. (Director) – Zannoni, Eduardo A. (Coordinador), “Código Civil y leyes complementarias. Comentado, anotado y concordado”, tomo 5, Editorial Astrea, Buenos Aires, 1994, p.72.
[34] Díaz Molina, Iván, “El derecho a la vida privada”, LA LEY, 126-985 y cita de Kemelmajer de Carlucci, ob.cit.supra.
[35] Cifuentes, Santos, “El derecho a la intimidad”, ED., 57-832 y “Derechos personalísimos”, Editorial Astrea, 2da, edición, Buenos Aires, 1995. Coincide en esta definición Rivera, Julio C, “Derecho a la intimidad”, LA LEY, 1980-D,912 (nota 15) y mismo autor, en Belluscio -Zannoni, ob.cit., parág. 8 Pág.278.
[36] Cifuentes, Santos, “ob.cit, supra.

derecho para una persona de ser libre, de llevar su propia existencia, como lo estime conveniente, con el mínimum de injerencias exteriores"[37].

Goldenberg lo ha descrito como "el derecho que permite al individuo preservar, mediante acciones legales, su intimidad, es decir, la parte no comunicable de su existencia"[38].

De Cupis sostiene que toda persona tiene asuntos o negocios, designios o afecciones, que pertenecen a ese sujeto o a su familia, que prefiere mantener como una esfera secreta, o al menos reservada de su vida, de la que tenga el poder de alejar a los demás[39].

Se mencionan en este ámbito aquellos datos, hechos o situaciones desconocidos para la comunidad, que son verídicos y que están reservados al conocimiento del sujeto mismo, o de un grupo reducido de personas, cuya divulgación o conocimiento por otros trae aparejado algún daño[40].

Fernández Sessarego dice que el derecho a la intimidad es "la respuesta jurídica al interés de cada persona de lograr un ámbito en el cual pueda desarrollar, sin intrusión, curiosidad, fisgoneo ni injerencia de los demás, aquello que constituye su vida privada, es decir la exigencia existencial de vivir libre de un indebido control, vigilancia o espionaje"[41].

Aunque no existe consenso al respecto, se considera que la "vida privada" es el género e incluye como núcleo central a la intimidad, aunque pueden usarse como

---

[37] Kemelmajer, ob.cit., quien remite a Leonfanti, María A. "El derecho a la intimidad en la Argentina (nuevo artículo del Código Civil)", LA LEY, 1975-B,1319, III.
[38] Goldenberg, Isidoro H, "La tutela de la vida privada", LA LEY, 1976-A,576, II, 3.
[39] De Cupis, Adriano, en "I Diritto della personalitá", y "Instituzioni di diritto privato", Giuffre editore, Milán, 1980, p.45, entre otros.
[40] Cf. Castán Tobeñas José María, en el prólogo de "El derecho a la intimidad" de Ferreira Rubio, Delia, citado por Vázquez Ferreyra, Roberto en "El derecho a la intimidad, al honor y a la propia imagen (Con especial referencia a la legislación española y a propósito de un fallo del Tribunal Supremo Español)", J.A. 1989, agosto 2 Nº 563.
[41] Fernández Sessarego, op.cit., p.163. Cfr.: Ferreyra Rubio, Delia M. "El derecho a la intimidad. Análisis del artículo 1071 bis del Código Civil", Editorial Universidad, Buenos Aires, 1982, p.39/40.

sinónimos. En cuanto a las nociones de "reserva" y "secreto", existe una diferencia de grado: secreto sería lo que no está destinado a ser conocido por terceros, mientras que la reserva sería aquello cuya difusión pública debe evitarse.

Nino hace esta distinción entre “privacidad” e “intimidad”[42], que en general compartimos, junto a otros autores, como Colautti[43], aunque no todos la aceptan. La exposición de motivos de la derogada LORTAD 5/92 española, aclara que “… se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de las persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo- la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que lo desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.”

1.1.3. Reconocimiento normativo

Desde el punto de vista de los antecedentes normativos referidos a la protección del derecho a la intimidad, uno de los más antiguos que merecen ser citados es el anteproyecto del Código Civil Boliviano de Angel Ossorio y Gallardo[44].

---

[42] Nino, Carlos S. “Fundamentos de Derecho Constitucional”, Ed. Astrea, Buenos Aires, 1992, ps. 304/335.

[43] Colautti, Carlos, “Reflexiones preliminares sobre el "Habeas data", LA LEY, 1996-C, 917.

[44] El anteproyecto es de 1943, y sería la fuente directa de nuestro actual artículo 1071 bis del Código Civil. Su texto dice: “Art. 20. Todas las personas tienen derecho a que sea respetada su vida íntima. El que, aun sin dolo ni culpa, se entrometiese en la vida ajena publicando retratos, divulgando secretos, difundiendo correspondencia, mortificando a otro en sus costumbres o perturbando de cualquier otro modo su intimidad, será obligado a cesar en tales actividades y a indemnizar al agraviado. Los

La Declaración Universal de los Derechos del Hombre de la Asamblea General de las Naciones Unidas de 1948[45], estableció que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (art. 12).

La Declaración Americana de Derechos y Deberes del Hombre[46], la Convención Europea de Salvaguarda de los Derechos del Hombre y las Libertades Fundamentales[47], la Convención Americana sobre Derechos Humanos[48] y el Pacto Internacional de Derechos Civiles y Políticos[49], reconocieron este derecho a la intimidad o a la vida privada. Más recientemente lo ha receptado la Carta de Derechos Fundamentales de la Unión Europea[50]. También deben mencionarse la Convención

---

tribunales regularán libremente, con arreglo a las circunstancias del caso, el modo de aplicar estas dos sanciones". Cf. Leonfanti, María, op.cit., Anexo A, número 11, p.1330/1.

[45] Teherán, 10/12/1948, http://www.un.org/spanish/aboutun/hrights.htm/

[46] Bogotá, abril 1948, también incorporada al texto constitucional (Art. 75 inc. 22 CN). Ver Art. V sobre vida privada. ,http://www.cidh.oas.org/Basicos/Basicos1.htm/

[47] "Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales", Roma, 04/11/1950, en su versión revisada según el protocolo nº 11, en su dice "Artículo 8. Derecho al respeto de la vida privada y familiar: 1 Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2 No podrá haber ingerencia de la autoridad pública en el ejercicio de este derecho salvo cuando esta ingerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de terceros.".

[48] San José de Costa Rica, 22/11/1969, Art., 11: "...2 nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.", http://www.oas.org/juridico/spanis/tratados/b-32.html/

[49] Pacto Internacional de Derechos Civiles y Políticos, A.G. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) p. 52, ONU Doc. A/6316 (1966), 999 U.N.T.S. 171, entrada en vigor 23/03/1976. Artículo 17: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

[50] Esta Carta reafirma, respetando las competencias y misiones de la Comunidad y de la Unión, así como el principio de subsidiariedad, los derechos reconocidos especialmente por las tradiciones constitucionales y las obligaciones internacionales

sobre los Derechos del Niño[51], la Convención internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares[52].

En el Derecho argentino podemos citar el artículo 19 de la Constitución Nacional, que consagra el denominado "principio de reserva"[53], el artículo 18, que garantiza la inviolabilidad del domicilio, la correspondencia y los papeles privados[54], y el artículo 33 que reconoce los llamados "derechos implícitos". También mencionamos la antigua ley de marcas[55] (art. 4 ley 3975), así como lo dispuesto por la Ley 11.723 de Propiedad Intelectual (arts. 31 y 32)[56], y finalmente el art.1071 bis del Código Civil (Ley

---

comunes de los Estados miembros, el Tratado de la Unión Europea y los Tratados comunitarios, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, las Cartas Sociales adoptadas por la Comunidad y por el Consejo de Europa, así como por la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas y del Tribunal Europeo de Derechos Humanos". (2000/C 364/01) Publicado el 18/12/2000 en el Diario Oficial de las Comunidades Europeas (DOC) (C 364/1). Artículo 7: Respeto de la vida privada y familiar: Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones. En el artículo 8 se refiere a la protección de los datos de carácter personal, que reiteraremos más adelante.

[51] Artículo 16: "1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación. 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.", http://www.unhchr.ch/spanish/html/menu3/b/k2crc_sp.htm/

[52] Adoptada por la Asamblea General en su resolución 45/158, 18/12/1990. Artículo 14: "Ningún trabajador migratorio o familiar suyo será sometido a injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia u otras comunicaciones ni a ataques ilegales contra su honor y buen nombre. Todos los trabajadores migratorios tendrán derecho a la protección de la ley contra tales injerencias o ataques."

[53] Artículo 19 Constitución Nacional: "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"

[54] Estos principios tienen un profundo arraigo en el Derecho Público Argentino, existiendo disposiciones similares en el Estatuto Provisional de 1815, luego recogido en el Reglamento de 1817 y en las Constituciones unitarias de 1819 y 1826. Cf. Ramella, Pablo, "El Derecho a la Intimidad", LA LEY, 140-1175.

[55] Ley 3975, Art. 4, que establecía que los nombres y retratos de las personas no podían usarse como marcas sin el consentimiento de sus titulares o de sus herederos hasta el cuarto grado inclusive.

[56] Art. 31 ley 11723: "El retrato fotográfico de una persona no puede ser puesto en el comercio sin el consentimiento expreso de la persona misma, y muerta ésta de su cónyuge e hijos o descendientes directos de éstos, o en su defecto del padre o de la madre. Faltando el cónyuge, los hijos, el padre o la madre, o los descendientes

21.173)[57].

El "leading case" en Argentina fue el caso Ponzetti de Balbín[58], en el que la Corte Suprema de Justicia de la Nación sostuvo que “El derecho a la privacidad e intimidad se fundamenta constitucionalmente en el art. 19 de la ley suprema. En relación directa con la libertad individual protege jurídicamente un ámbito de autonomía individual constituida por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o actos que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para la intimidad.”

Este fallo señero propone que “El derecho a la privacidad comprende no sólo a la esfera doméstica, el círculo familiar de amistad, sino otros aspectos de la personalidad espiritual física de las personas tales como la integridad corporal o la imagen y nadie puede inmiscuirse en la vida privada de una persona ni violar áreas de su actividad no destinadas a ser difundidas, sin su consentimiento o el de sus familiares autorizados para ello y sólo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la

---

directos de los hijos, la publicación es libre. La persona que haya dado su consentimiento puede revocarlo resarciendo daños y perjuicios. Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés público o que se hubiera desarrollado en público". Y el artículo 32 dice: "El derecho de publicar las cartas pertenece al autor. Después de la muerte del autor es necesario el consentimiento de las personas mencionadas en el artículo que antecede y en el orden ahí indicado". El primer texto está más vinculado con lo que modernamente se conoce como el "derecho a la propia imagen", que tendría autonomía en relación al derecho a la intimidad.

[57] Art. 1071 bis Cód. Civil: "El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otro en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieran cesado, y a pagar una indemnización que fijará equitativamente el juez de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esa medida fuese procedente para una adecuada reparación".

[58] CSJN, 11/12/1984, “Ponzetti de Balbín, Indalia c/ Editorial Atlántida, S. A.”, LA LEY, 1985-B, 120.

sociedad, las buenas costumbres o la persecución del crimen.”

La reforma constitucional de 1994 estableció en el artículo 43 un párrafo tercero que reza: "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 aquellos. No podrá afectarse el secreto de las fuentes de información periodística." Sobre el particular nos extenderemos más adelante.

1.2. Protección de datos personales

1.2.1. Concepto de datos personales

La información es un concepto complejo, que se integra con “datos”. El dato es el “antecedente necesario para llegar al conocimiento exacto de una cosa” y la información puede definirse como el proceso de adquisición de conocimientos que permiten precisar o ampliar los que ya se tenían sobre una realidad[59].

En el contexto de la información procesada o tratada automatizadamente, el “fichero” o "banco de datos" es un lugar (físico o virtual), archivo u oficina donde se asientan datos. Los datos por sí mismos no nos permiten la adopción de la decisión más conveniente porque no aportan los conocimientos necesarios. Hay que adicionar, combinar, excluir, comparar, estos datos para obtener un resultado que nos sea útil. Es lo que denominamos procesamiento de datos. La "información" es el resultado de esta transformación (procesamiento) de los datos.

Los datos registrados pueden pertenecer a una persona o a una cosa, o a la

[59] Esto lo hemos sostenido, entre otras oportunidades, en "Protección de datos personales como derecho autónomo: principios rectores. Informes de solvencia crediticia: uso arbitrario. Daño moral y material", http://www.eldial.com.ar/doctri/notas/nt030510.html/. Debe entenderse como dato al “antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho; representación de una información de manera adecuada para su tratamiento por un ordenador”. Diccionario de la Lengua Española, Real Academia Española, Vigésima Primera Edición, Madrid, 1992, pág. 469.

relación de ambas. Los registros de datos pueden clasificarse de diversas maneras[60], pero en esta oportunidad nos preocupa especialmente poner énfasis en los datos personales contenidos y procesados en bancos de datos.

Hemos asignado el nombre de “bancos de datos” a todo conjunto estructurado de datos (en este caso, personales), centralizados o repartidos en diversos emplazamientos y accesibles con arreglo a criterios determinados, que tengan por objeto o efecto facilitar la utilización o el cotejo de datos relativos a los interesados[61].

Cuando el segmento de la realidad que es objeto de información es una persona, estamos frente a datos de carácter personal[62], con un alcance amplio, es decir que si de las operaciones de tratamiento posibles pueden establecerse

---

60 Falcón, Enrique M, "Hábeas Data, concepto y procedimiento", Abeledo Perrot, Bs. As., 1996.

61 La Directiva 95/46/CE, del Parlamento y Consejo Europeo, establece en sus considerandos que “los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata”. El artículo 2 de la Directiva citada define como “fichero de datos personales” a “todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica”.

62 Se ha dicho que esta descripción contiene un criterio que restringiría el alcance del término (Peyrano, Guillermo, “Nuevas problemáticas del tratamiento de datos personales. El tratamiento de informaciones que proporcionan datos personales por parte de medios periodísticos a través de Internet”, JA 7/04/2004, Lexis Nº 0003/010468. Ver también REDI Revista Electrónica de Derecho Informático - Número 58 (Mayo de 2003), manifestando que si bien no caben dudas que en los datos personales resulta imposible prescindirse de la persona, no obstante ello el carácter se mantendría en aquellos supuestos en los que si bien la realidad representada por el dato no es una persona, la información puede ser vinculada a la misma por asociación. Se agrega que la amplitud de posibilidades que brindan los medios informáticos a esas operaciones hace desaconsejable utilizar criterios restrictivos, por cuanto podrían quedar excluidas de la debida tutela legal múltiples tipos de informaciones susceptibles de ser vinculadas con extrema facilidad a las personas. Es decir que si de las operaciones de tratamiento posibles pueden establecerse relaciones referencias o asociaciones, con personas -sean éstas determinadas o determinables- deba considerarse a los datos involucrados como "datos de carácter personal", debiendo ser así tenidos en cuenta (Peyrano, Guillermo, "Bancos de datos y tratamiento de datos personales: análisis de algunas problemáticas fundamentales". JA, Boletín nº 6242, 18/4/2001, p. 6). Aclaramos que compartimos este criterio amplio.

relaciones referencias o asociaciones, con personas -sean éstas determinadas o determinables- deba considerarse a los datos involucrados como "datos de carácter personal", debiendo ser así tenidos en cuenta[63].

En principio, se denominan datos personales aquellos que permiten identificar a la persona a la que pertenecen[64]; en cambio, no se consideran tales los que se refieren a personas indeterminadas. El nombre y apellido es un dato personal (nominativo); la cantidad de personas de género femenino o masculino que concurren a un curso es un dato general[65].

Dentro del género "datos personales" se denominan "sensibles"[66] los referidos a determinadas facetas o aspectos de una persona, tales como el culto que profesa, su pertenencia racial, su ideología política, y en general la información que permite determinar su fisonomía moral e ideológica[67]. La preocupación esencial que rodea el

---

63 Peyrano, Guillermo, ob.cit nota supra.
64 La Directiva 95/46/CE define "datos personales" como "toda información sobre una persona física identificada o identificable ("el interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social". La Convención para la Protección de las Personas frente al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa, firmada en 1981 en Estrasburgo, la definición de datos personales es: "toda información concerniente a una persona física identificada o identificable.
65 La mencionada Directiva establece que “No se considerarán de carácter personal los datos reunidos en estadística de tal modo que los interesados dejan de ser razonablemente identificables”.
66 o también “datos especiales”
67 Al respecto, Novoa Monreal, Eduardo, "Derecho a la vida privada y libertad de información", Editorial Siglo XXI, págs. 45 y 46, 1979, hace el siguiente "recuento empírico" sobre las actividades, situaciones y fenómenos pertenecientes a la vida privada: " a] ideas y creencias religiosas, filosóficas, mágicas y políticas que el individuo desee sustraer del conocimiento ajeno; b] aspectos concernientes a la vida amorosa y sexual; c] aspectos no conocidos por extraños de la vida familiar, especialmente los de índole embarazosa para el individuo o para el grupo; d] defectos o anomalías físicos o psíquicos no ostensibles; e] comportamiento del sujeto que no es conocido de los extraños y que de ser conocido originaría críticas o desmejoraría la apreciación de éstos hacen de aquél; f] afecciones de la salud cuyo conocimiento menoscabe el juicio que para fines sociales o profesionales formulan los demás acerca del sujeto; "g] contenido de comunicaciones escritas u orales de tipo personal, esto es, dirigidas únicamente para el conocimiento de una o más personas determinadas; h] la vida pasada del sujeto, en cuanto pueda ser motivo de bochorno para éste; i] orígenes

tratamiento de estos datos, además de la tutela del derecho a la intimidad, o vida privada, es sin duda, la posibilidad de discriminación[68].

1.2.2. Impacto de las nuevas tecnologías

El almacenamiento y recopilación de datos de carácter personal no es una actividad que haya surgido con la irrupción de la informática. Por el contrario, la existencia de los ficheros manuales con datos de carácter personal auguraba los riesgos de datos incompletos, falsos o utilizados para un propósito diferente para el cual se habían recogido.

Sin embargo, es evidente que la preocupación en esta materia ha crecido a partir del tratamiento automatizado de este tipo de información.

La irrupción de la informática obligó a un replanteo del derecho a la intimidad, por la estructuración de grandes bancos de datos de carácter personal, y la posibilidad del entrecruzamiento de la información contenida en los mismos[69].

Con la difusión del fenómeno informático empieza a hablarse de “protección de datos personales”

Se ha dicho que la noción de protección de datos puede conducir a falsas

---

familiares que lastimen la posición social y, en igual caso, cuestiones concernientes a la filiación y a los actos de estado civil; j] el cumplimiento de las funciones fisiológicas de excreción, y hechos o actos relativos al propio cuerpo que son tenidos por repugnantes o socialmente inaceptables (ruidos corporales, intromisión de dedos en cavidades naturales, etc.); k] momentos penosos o de extremo abatimiento; y, j] en general, todo dato, hecho o actividad personal no conocidos por otros, cuyo conocimiento por terceros produzca turbación moral o psíquica al afectado (desnudez, embarazo prematrimonial).”

[68] Cf.: Directiva 95/46 (Art. 8) establece que: ”Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad”. En similar sentido, Convenio 108, y leyes de España, Hungría, Bélgica, Dinamarca, Francia, Italia (Art. 22.1 ley 675), Gran Bretaña, etc.

[69] Altmark, Daniel R. y Molina Quiroga, E, obras citadas ut supra; Cf. Campanella de Rizzi Elena M. y Stodart de Sasim, María, ob.cit. supra; Beckerman, Jorge, ob.cit. supra, etc.

apariencias respecto de su contenido, ya que no va destinada a proteger a los datos per se, sino a una parte del derecho a la intimidad personal, es decir, la que se refiere a la información individual. Hondius ha definido la protección de datos como "aquella parte de la legislación que protege el derecho fundamental de libertad, en particular del derecho individual a la intimidad, respecto del procesamiento manual o automático de datos"[70].

La toma de conciencia sobre esta circunstancia nos llevó a sostener, hace un tiempo, que el derecho a la intimidad no podía seguir considerándose simplemente la ausencia de información acerca de nosotros en la mente de los demás (el "déjenme solo"), sino que debía adquirir el carácter de un control sobre la información que nos concerniera, o sea la facultad del sujeto de controlar la información personal que sobre él figurara en los bancos de datos[71].

Parece evidente que la categoría de "protección de datos" ha surgido para aplicarse a nuevas realidades jurídicas, que sólo parcialmente, pueden ser descriptas o fundamentadas a través de la noción tradicional de "intimidad", y que incluso el encuadre como “derecho personalísimo” genera restricciones[72].

---

[70] Hondius, Frits W., A decade of international data protection, “Netherlands of International Law Review”, Vol. 30, N° 2, 1983, p. 105, citado por Estadella Yuste, Olga, "La protección de la intimidad frente a la transmisión internacional de datos personales", Ed. Tecnos, Centre d’Investigació de la Comunicació, Generalitat de Catalunya, Barcelona,1995.

[71] Cf. Pérez Luño, Antonio Enrique, “Nuevas Tecnologías, Sociedad y Derecho: El Impacto Socio-jurídico de la Nueva Tecnología de la Información”, Fundesco Madrid, 1987; Lucas Murillo de la Cueva, Pablo, “El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática”, Tecnos, Madrid, 1990; García González, Aristeo, “La protección de datos personales. Derecho fundamental del Siglo XXI. Un estudio comparado”, Revista Derecho Informático – Alfa Redi Nº 100, noviembre 2006, entre muchos otros. El III Congreso Internacional de Daños, AABA, Bs. As., 1993) –donde fuimos ponentes- aprobó entre sus Conclusiones: De lege lata: "1.Cuando la información constituida por datos personales nominativos recibe un tratamiento electrónico, la adecuada tutela del derecho a la intimidad requiere reconocer a toda persona la facultad de controlar la que le concierne. Dicha facultad comprende: a) el derecho a la información; b) el derecho de rectificación y cancelación de datos inexactos o caducos; c) el derecho a que los datos sean utilizados de acuerdo a la finalidad prevista; d) el derecho a impedir el acopio de datos que hacen a su personalidad o ideología",

[72] Basándose en que es un derecho "personalísimo", el Supremo Tribunal Federal de

El derecho a la "protección de datos" pertenece al contexto de la era informática, y cada día es más dudoso afirmar que esta compleja disciplina legal estuviera ya implícita en las referencias generales al derecho a la intimidad insertas en cuerpos normativos del ámbito nacional o internacional de la era preinformática[73].

1.2.3. Autodeterminación informativa

La fundamentación jurídica del derecho a la protección de datos personales debe relacionarse con el tradicional derecho a la intimidad, o a la vida privada, pero lo excede.

El control de la información personal está relacionado con el concepto de autonomía individual para decidir, hasta cierto límite, cuándo y qué información referida a una persona, puede ser objeto de procesamiento automatizado, por lo que también se ha denominado a la protección del dato personal, autodeterminación informativa, e incluso libertad informática[74].

La protección de los datos personales no se plantea exclusivamente a consecuencia de problemas individuales, sino que también expresa conflictos que incluyen a todos los individuos de la comunidad internacional, problema que es analizado bajo la óptica del flujo internacional de datos. Este derecho no sólo comprende una idea individualista de protección a la intimidad sino que también tutela a los intereses de un grupo social contra el procesamiento, almacenamiento y recolección de información, especialmente si advertimos la vinculación con prácticas discriminatorias[75].

El tratamiento automatizado de datos personales se ha convertido en un arma estratégica de manipulación de conductas individuales, y la aplicación de avanzados

---

Brasil negó legitimación a la madre de un preso político, asesinado en las prisiones militares (Cid. por de Urioste, Mercedes, en “Protección de datos personales”, Investigaciones 1 (1998) p.148, Subsecretaría de investigación en derecho comparado de la CSJN).

[73] Cf.: Estadella Yuste, Olga, ob.cit.supra.

[74] Frosini, Vittorio, “Informática y Derecho”, p.68 y ss., Ed. Themis, Bogotá, Colombia, 1988.

[75] Estadella Yuste, ob. cit. supra.

métodos telemáticos a la información de carácter personal ha dejado de ser la excepción para convertirse en una rutina diaria.[76]

El derecho a la protección de datos personales, además de emparentarse con el tradicional derecho a la intimidad, lo excede porque alcanza a datos que son públicos, o si se quiere, no confidenciales, incide en otros derechos personalísimos como el honor, la imagen, o la identidad. Fue gradualmente adquiriendo el reconocimiento de un derecho individual de carácter personalísimo, tanto en la doctrina como en la legislación, como veremos más adelante[77].

El núcleo de la protección de los datos personales se dirige a que el particular interesado tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga. En tal sentido, este derecho forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad. El señorío del hombre sobre sí se extiende a los datos sobre sus hábitos y costumbres, su sistema de valores y de creencias, su patrimonio, sus relaciones familiares, económicas y sociales, respecto de todo lo cual tiene derecho a la

---

[76] Cf., entre otros: Correa, Carlos y otros, "Informática, Libertad y Derechos Humanos", en Correa, Nazar Espeche, Czar de Zalduendo y Batto, “Derecho Informático”, Depalma, Buenos Aires, 1987; Giannatonio, Ettore, "Introduzione all'informatica guiridica" citado en: "Impacto de la Informática en la sociedad” (Protección de datos personales. Derecho a la intimidad); Stiglitz, Rosana M., LA LEY, 1987-E-859; Carrascosa López, Valentín, en "Derecho a la Intimidad e Informática", en Informática y Derecho UNED, 1-1992, pag. 23, etc.

[77] Si bien habíamos sostenido una posición similar en "La protección de datos personales o autodeterminación informativa", V Congreso Iberoamericano de Informática y Derecho, La Habana, Cuba, 1996, quien ha desarrollado específicamente este punto de vista es Cifuentes, Santos. "Protección inmediata de los datos privados de la persona. Habeas data operativo", LA LEY, 1995-E, 193; "Derecho personalísimo a los datos personales", LA LEY, 1997-E, 1323; y "Acciones procesales del art. 43 de la Constitución Nacional", LA LEY, 1999-A, 258. La misma posición se advierte en el voto de Bueres, Alberto, su voto en CNCiv., sala D, 23/02/1999, Lascano Quintana, Guillermo V. c/ Veraz S.A., LA LEY, 1999-E, 152; LA LEY, 2000-B, 679; RCyS, 1999, 792 y DJ, 1999-3, 760: “Cualquier persona física tiene un derecho personalísimo de "dominio" respecto de sus datos personales ("hábeas data" "eres dueño de tus datos" o "Tiene tus datos"), que no puede colectarse sin su aquiescencia previa, o como mínimo, anoticiándolo de inmediato sobre la confección de una ficha informatizada de sus datos personales a los efectos que pudieran corresponder. Y menos aún, estableciendo una "base de relación" con los datos de otras personas físicas o jurídicas.”

autodeterminación informativa[78].

1.2.4. La sentencia alemana del censo

El punto central de esta evolución –desde la protección a la intimidad hacia el reconocimiento de un derecho autónomo- se encuentra en la jurisprudencia del Tribunal Constitucional alemán.

En una primera etapa, la jurisprudencia alemana había sostenido la llamada "teoría de las esferas", según la cual se establecía una protección diferenciada de acuerdo con el mayor o menor grado de afectación de la intimidad[79].

Esta concepción restrictiva, fue abandonada en favor de una tutela considerablemente más amplia, en el fallo conocido como "sentencia del censo" [80], en la que el Tribunal Constitucional alemán se expidió con relación a una Ley de Censo, votada por el Parlamento (Bundestag), según la cual, y a fin de mejorar el aprovechamiento de los recursos sociales, se compelía a los ciudadanos a responder un interrogatorio que abarcaba una serie de datos privados. Aunque los datos eran

---

[78] CSJN, 15/10/1998, "Urteaga, Facundo R. c/ Estado Mayor Conjunto de las Fuerzas Armadas", voto del Dr. Santiago E. Petracchi, LA LEY, 1998-F,237.

[79] Esta doctrina fue elaborada especialmente en el caso sobre el Mikrozensus, cf. BVerfGE 27, 1 y sigtes; Alexy, Robert, "Theorie der Grundrechte", 1994 (segunda edición), pág. 327 traducida por Garzón Valdés, Ernesto como "Teoría de los derechos fundamentales" (Centro de Estudios Constitucionales, Madrid, 2002 (3ª, reimpresión), p.349 y ss.; Alexy, Robert, "Los Derechos Fundamentales en el Estado Constitucional Democrático", en Carbonell, Miguel (Edit.), Neoconstitucionalismo(s), 2ª Edición, Trotta, Madrid, 2005. Ver adde: Hassemer, Winfred y Sánchez, Alfredo Chirino, "El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales", Editores del Puerto, Buenos Aires, 1997, p. 172.

[80] Sentencia de 15/12/1983 (Ref. 1 BvR 209/83) en las demandas de inconstitucionalidad contra la Ley sobre el recuento de la población, de las profesiones, de las viviendas y de los centros de trabajo (Ley del Censo de 1983) de 25/03/1982 (publicada en el Boletín de Legislación Federal –BGBI- I, pág. 369), el Tribunal Constitucional Federal –Sala Primera- dicto dicha sentencia, con la participación del Presidente Benda y de los Jueces Simón, Hesse, Katzenstein, Niemeyer, Heussner, Niedermaier, Henschel (según extracto publicado por la revista Derecho Público Contemporáneo Nº 7, de la Agrupación de Abogados de la Contraloría General de la República de Colombia, basado en algunas partes de la sentencia traducida por Manuel Daranas, para el Boletín de Jurisprudencia Constitucional Nº 33, de 1984)

relevados en forma anónima, iban a ser cotejados con los registrados en los Estados Federales (Länder), y ello, hipotéticamente, permitiría identificar a sus titulares. El Tribunal, aun cuando confirmó la validez de la mayor parte de la ley, obligó a realizar modificaciones en ciertos puntos, relativos al modo en que se podía autorizar la recolección y almacenamiento de los datos[81].

Existe consenso en atribuir a esta sentencia la configuración del concepto de autodeterminación informativa o libertad informática, que es reconocido actualmente en forma predominante como el fundamento del hábeas data en las legislaciones que contemplan derechos análogos[82].

Según lo indica el profesor alemán Erhard Denninger, la expresión autodeterminación informativa se venía fraguando ya desde hace algunos años, y si bien su origen es alemán, salió a la luz a través de sentencias como la de la Ley de ayuda a la inversión de 1954 o la sentencia Lüth de 1958 que se refirió al "valor y la dignidad de la persona que actúa como un miembro libre con autodeterminación libre

---

[81] Confr. recesión en Kommers, Donald, "The Constitutional Jurisprudence of the Federal Republic of Germany", Durham, Londres, 1989, pág. 332 y voto Dr. Petracchi en "Urteaga"

[82] Pérez Luño, Antonio Enrique, "Intimidad y protección de datos personales: del hábeas corpus al hábeas data", en García San Miguel, Luis (comp.), "Estudios sobre el derecho a la intimidad", Madrid, 1992, págs. 36 y sigtes., esp. 44; Bidart Campos, Germán, "El derecho de petición, de acceso a la información y el recurso de insistencia en el derecho colombiano", ED, 166-41; Vanossi, Jorge R., "El hábeas data: no puede ni debe contraponerse a la libertad de los medios de prensa", ED, 159-948, esp. pág. 949; respecto de regímenes legislativos en particular: Chirino Sánchez, Alfredo, "El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales", Buenos Aires, 1997, con referencia a la Ley Orgánica 5/1992 de Regulación del tratamiento Automatizado de Datos de Carácter personal (LORTAD) de España; Hassemer, Winfried, "Theorie und Soziologie des Verbrechens", Frankfurt a. M., 1973, págs. 36 y sigtes., sobre la Ley Federal de Protección de datos de la República Federal de Alemania (BDSG) y del Land Hesse (HDSG); Bianchi, Alberto, "Hábeas data y derecho a la privacidad", ED, 161-866, esp. pág. 874, con relación a la Data Protection Act inglesa, de 1984, y a la Privacy Act norteamericana, de 1974, voto de Santiago Petracchi en "Urteaga". García González, Aristeo, "La protección de datos personales. Derecho fundamental del Siglo XXI. Un estudio comparado", Revista Derecho Informático – Alfa Redi Nº 100, noviembre 2006), entre otros.

en una sociedad libre"[83].

En un informe encargado por Ministerio Federal del Interior alemán del año 1971, Steinmüller y otros hablaban del "derecho a la autodeterminación informativa sobre la imagen de una persona o de un grupo de personas" o el "derecho a la autodeterminación informativa del ciudadano referente a la imagen de su propia persona". El citado Denninger, en 1981, se refiere ya a la "separación de la protección constitucional y el derecho fundamental de autodeterminación informativa"[84].

Según este concepto es el ciudadano quien debe decidir sobre la cesión y uso de sus datos personales. Este derecho -se dijo- puede ser restringido por medio de una ley por razones de utilidad social, pero respetando el principio de proporcionalidad y garantizando que no se produzca la vulneración del derecho a la personalidad[85].

De tal modo, en un Estado de Derecho, el ciudadano es propietario de los datos que sobre él se registren y por lo tanto, ellos deben estar a su disposición para que sea él quien decida si los cede o en qué condiciones lo hace.

El tribunal alemán dijo en esta sentencia que "esta facultad requiere en las condiciones actuales y futuras de la elaboración automática de datos una medida especial de protección. Aparece ante todo amenazada por el hecho de que los procesos de decisión ya no se pueden retrotraer como antiguamente a registros y

---

[83] Denninger, Erhard, en Pérez Luño, Antonio (director de la edición), "Problemas actuales de la documentación y la informática jurídica", pág. 271, Editorial Tecnos S.A., Madrid, 1987.
[84] Ibídem, pág. 272. Profundiza en esta obra el mismo autor señalando que "Entendiendo el DAI (Derecho a la Autodeterminación Informativa) como facultad general de disponer sobre datos propios personales, el Tribunal ha puesto el acento, de forma decisiva, respecto a una conclusión teórica (y constitucional); la autodeterminación informativa no sólo depende de los datos sino de su elaboración. No es la clasificación abstracta, categórica, de un dato según la mayor o menor cercanía al "ámbito íntimo de la vida" de una persona; tampoco es la cuestión de si un dato por naturaleza tiene caracteres de secreto o no lo que decide si es digno de ser protegido o no, sino el contexto de su uso. La sentencia Zensus parte de la coexistencia de ambos criterios; dice que no depende sólo del tipo de información sino que lo que importa son su utilidad y la posibilidad de su aplicación".
[85] Cf. Hassemer (juez del Tribunal Constitucional alemán, y Comisionado para la Protección de Datos de Hesse (Datenschutzbeauftragter), citado por Petracchi en "Urteaga".

documentos compilados manualmente; antes bien, hoy día, gracias a la ayuda de la elaboración automática de datos, la información individual sobre circunstancias personales u objetivas de una persona determinada o, en su caso, determinable [datos de referencia personal, cfr. artículo 2°, parrafo 1, de la Ley Federal de Protección de Datos] son, técnicamente hablando, acumulables sin limite alguno y en cualquier momento se pueden recabar en cuestión de segundos, cualquier que sea la distancia. Es más, esa información puede - especialmente con el montaje de sistemas integrados de información- refundirse con otras colecciones de datos en un perfil de personalidad parcial o ampliamente definido, sin que el interesado pueda controlar suficientemente su exactitud y su utilización. De este modo se han ensanchado en una medida hasta ahora desconocida las posibilidades de indagación e influencia susceptibles de incidir sobre la conducta del individuo, siquiera por la presión psicológica que supone el interés del público en aquélla."

Y agregó: "Ahora bien, la autodeterminación del individuo presupone -también en las condiciones de las técnicas modernas de tratamiento de la información- que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada. El que no pueda percibir con seguridad suficiente qué informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse substancialmente cohibido en su libertad de planificar o decidir por autodeterminación. No serían compatibles con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciese posible al primero, en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo sabe algo sobre él."

"Quien se siente inseguro de si en todo momento se registran cualesquiera comportamientos divergentes y se catalogan, utilizan o transmiten permanentemente a título de información procurará no llamar la atención con esa clase de comportamiento. Quien sepa de antemano que su participación, por ejemplo, en una reunión o en una iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales [artículo 8° y 9° de la Ley Fundamental]."

“Esto no sólo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos. De lo que antecede se deduce lo siguiente: la libre eclosión de la personalidad presupone, en las condiciones modernas de la elaboración de datos, la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitadas de los datos concernientes a la persona. Esta protección cae, por lo tanto, dentro del ámbito del derecho fundamental del artículo 2°, párrafo 1, en relación con el artículo 1°, párrafo 1, de la Ley Fundamental (alemana). El derecho fundamental garantiza, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y la utilización de sus datos personales.”

El Tribunal aclaró que “Este derecho a la autodeterminación informativa no está, sin embargo, garantizado sin límites. El individuo no tiene ningún derecho sobre sus datos en el sentido de una soberanía absoluta e irrestringible, sino que es más bien una personalidad que se desenvuelve dentro de la comunidad social y que está llamada a comunicarse. La información, incluso en la medida en que se refiera a la persona como tal, ofrece un retrato de la realidad social que no cabe asignar exclusivamente al interesado. La Ley Fundamental (alemana) ha resuelto la tensión individuo-comunidad en el sentido de la referencia y vinculación comunitaria de la persona, como ya ha sido puesto varias veces de relieve en la jurisprudencia del Tribunal Constitucional Federal [...]. El individuo tiene, pues, que aceptar en principio determinadas limitaciones de su derecho a la autodeterminación informativa en aras del interés preponderante de la colectividad.”

Sin embargo, también señaló que “Estas limitaciones necesitan, ... un fundamento legal (constitucional), del que se deduzcan con suficiente claridad y de modo inteligible para el ciudadano los supuestos y el ámbito de las limitaciones y que responda, por lo tanto, al imperativo de claridad normativa inherente al Estado de Derecho [Tribunal Constitucional Federal 45, 400 (420) con otros considerandos].” Y volvió a destacar que “El legislador debe, además, tener a la vista en sus reglamentaciones el principio fundamental de la proporcionalidad, el cual se desprende, como principio fundamental revestido de rango constitucional, de la propia esencia de los derechos fundamentales del mismo, que como expresión que son del

derecho general del ciudadano a la libertad frente al Estado, sólo pueden ser restringidos por el poder público en tanto en cuanto esto sea indispensable para la salvaguardia del interés general [Tribunal Constitucional Federal 19, 342 (348) jurispr. const.].”

Por esta razón, recomendó que “A la vista de los peligros ya expuestos de la utilización de medios automáticos para la elaboración de datos, el legislador tiene que adoptar también más precauciones organizativas y jurídico-procesales que en el pasado para conjurar el riesgo de vulneración del derecho a la personalidad [cf.Tribunal Constitucional Federal 53, 30 (65); 63, 131(143)].”

Durante varios años, en los países con un alto grado de desarrollo en sus esquemas de derechos fundamentales se ha convertido en algo natural y evidente que la protección de la privacidad del ciudadano está íntimamente unida al derecho a la información. La Freedom of Information es el gemelo del derecho a la protección de datos personales. Para decirlo con las palabras del Tribunal Constitucional alemán, “si un ciudadano no tiene información sobre quién ha obtenido información sobre él, qué tipo de información y con qué medios la ha obtenido, ya no podrá participar en la vida pública sin miedo”.[86]

Es decir que el control de la información personal está relacionado con el concepto de autonomía individual para decidir, hasta cierto límite, cuándo y qué información referida a una persona puede ser objeto de procesamiento (automatizado o no), por lo que también se ha denominado a la protección de datos personales, autodeterminación informativa, e incluso libertad informática.

1.2.5. Derecho de tercera generación

También se incluye a la protección de datos personales, autodeterminación informativa o libertad informática como parte del núcleo de los derechos denominados de "tercera generación".

Estos derechos de tercera generación se presentan como una respuesta al

[86] confr. Hassemer, op. cit., por Petracchi en “Urteaga”.

fenómeno de lo que se ha denominado "contaminación de las libertades" *–pollution des libertés–* término con el que en algunos sectores de la teoría social anglosajona se hace alusión a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías[87].

Además de la autodeterminación informativa o libertad informática integran el plexo de los derechos de tercera generación el derecho a la paz, los derechos de los consumidores, el derecho a un medio ambiente sano y el derecho a una calidad de vida, derechos éstos dirigidos a potenciar la esfera de libertades del individuo en la era tecnológica.[88] Se mencionan también como derechos de tercera generación a la autodeterminación, la independencia económica y política, la identidad nacional y cultural, a la coexistencia pacífica, al entendimiento y confianza, a la cooperación internacional y regional, la justicia internacional, el uso de los avances de las ciencias y la tecnología, la solución de los problemas alimenticios, demográficos, educativos y ecológicos.[89]

En síntesis, coincidimos con quien afirma que el derecho fundamental a la protección de los datos de carácter personal, como derecho de la llamada tercera generación, es uno de los exponentes del conflicto tecnología-Derecho, cuya razón de ser reside en dar al individuo la posibilidad efectiva de disponer y controlar los datos que le conciernen.[90]

---

[87] Pérez Luño, Antonio Enrique, "La Tercera Generación de los Derechos Humanos", Thomson-Aranzadi, Madrid, 2006; García González, Aristeo, ob.cit. supra; Reyes Krafft, Alfredo Alejandro, "Protección de datos personales en México. Génesis legislativa" (Revista Derecho Informático - Alfa Redi Nº 100 noviembre 2006); Guerrero Picó, María del Carmen, "El derecho fundamental a la protección de los datos de carácter personal en la Constitución europea", http://www.ugr.es/~redce/REDCE4/articulos/12guerrero.htm#nota7/

[88] Álvarez B. de Bozo, Miriam; Ávila Hernández, Flor María; Peñaranda Quintero Héctor Ramón, "La libertad informática: derecho fundamental en la Constitución Venezolana", ob.cit. supra.

[89] Reyes Krafft, ob.cit supra.

[90] Guerrero Picó, ob.cit. supra.

Capítulo 2. Derecho comparado. Documentos internacionales

Sumario: Primeros antecedentes. Declaraciones ONU y otros Organismos Internacionales Recomendaciones de la Asamblea General de la ONU Directrices y Directivas Europeas. Directrices del Comité de Ministros. Otras iniciativas relacionadas. Directrices para la Protección de la Privacidad y el Flujo Internacional de Datos Personales de la OCDE. El Convenio 108 de Estrasburgo. Acuerdo de Schengen. La Directiva 95/46/CE. Principios consagrados por la Directiva 95/46/CE. Derechos consagrados por la Directiva 95/46/CE. Limitaciones impuestas por los Estados por la Directiva 95/46/CE. Reglamento CE Nº 45/2001. Otros actos normativos europeos. Directivas sectoriales europeas. Síntesis

2.1. Primeros antecedentes

En el derecho comparado encontramos numerosos antecedentes normativos referidos a la protección de los datos personales.

Se dice que el reconocimiento del derecho a controlar los datos de carácter personal tiene su origen en la Constitución de Weimar (Alemania), del año 1919, que reconocía el deber de velar por la información que contenían los expedientes personales de los funcionarios públicos en el artículo 129, inciso tercero. Esta norma decía que “Todo funcionario debe tener un recurso contra la decisión disciplinaria que le afecte y la posibilidad de un procedimiento de revisión. Los hechos que le son desfavorables no deben ser anotados en su expediente personal sino después de haberle dado ocasión de justificarse respecto a ellos” y agregaba que “El funcionario tiene derecho a examinar su expediente personal”, para finalizar estableciendo que “La inviolabilidad de los derechos adquiridos y el recurso a los tribunales para la reclamación de derechos pecuniarios son de modo especial igualmente garantizados a los militares de carrera. Para el resto, su situación está regulada por una ley del Reich (Estado)”.

De este artículo se desprenden una serie de principios que formarían parte de lo que representa el esquema tradicional del habeas data en la mayoría de los ordenamientos jurídicos: el reconocimiento de un recurso para revisar datos de su vida personal, a tener conocimiento de los datos que se guardan sobre su persona, el

derecho a un debido proceso, el derecho a que se rectifique la información que se tiene sobre una persona, e incluso el derecho a exigir una indemnización de carácter pecuniario. No son más que las primeras pinceladas de todo un proceso que hasta nuestros días se encuentra en proceso de perfeccionamiento[1].

Masciotra menciona la Real Ordenanza sobre libertad de Prensa, de Suecia en 1766, que proclamaba expresamente el derecho de los ciudadanos, aunque con ciertos límites, al conocimiento de la documentación[2].

El mismo autor se refiere a una ley de Francia de 1905 que imponía la obligación de comunicar al ciudadano el contenido de su legajo personal antes de decidir cualquier medida disciplinaria en su contra.[3]

2.2. Declaraciones ONU y otros Organismos Internacionales

2.2.1. Recomendaciones de la Asamblea General de la ONU

La Conferencia Internacional de Derechos Humanos[4] declaró su preocupación ante el riesgo potencial de violación de los derechos humanos que implicaban los avances científicos y tecnológicos[5], correspondiéndole a la Asamblea General de la ONU recomendar a los Estados la realización de estudios que sirvieran de base para la redacción de normas que protegieran adecuadamente los derechos y libertades

---

[1] Coronel Carcelén, Felipe Francisco, "La protección del derecho a la vida privada en Internet y otros medios de comunicación electrónicos" (borrador de tesis UCPChile), (http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/coronel.pdf/

[2] Masciotra, Mario, "El hábeas data. La garantía polifuncional", Librería Editora Platense, La Plata, 2003, p.52, quien cita a Díaz Maynard, Daniel, en su informe del proyecto de ley de "Derecho a la información y acción de hábeas data", presentado ante el Parlamento de la República Oriental del Uruguay, http://www.parlamento.gub.uy/repartidos/camara/d2002060114-01.htm/

[3] Masciotra, ob.cit. supra, p.53.

[4] Teherán, 1968.

[5] El punto 18 de la Proclamación de Teherán, reza: "18. Si bien los recientes descubrimientos científicos y adelantos tecnológicos han abierto amplias perspectivas para el progreso económico, social y cultural, esta evolución puede, sin embargo, comprometer los derechos y las libertades de los individuos y por ello requerirá una atención permanente", ONU, Doc. A/CONF.32/41 p. (1968).

individuales, mencionando particularmente "las aplicaciones de la electrónica que puedan afectar los derechos de la persona y los límites que deberían fijarse para estas aplicaciones en una sociedad democrática"[6].

La Asamblea General de la Organización de Naciones Unidas aprobó en 1989 los “Principios rectores para la reglamentación de los ficheros computadorizados de datos personales”.[7]

La Resolución 45/95 de la Asamblea General de la ONU, de 14 de diciembre de 1990, recoge la versión revisada de los mencionados Principios Rectores aplicables a los Ficheros Computadorizados de Datos Personales[8].

Estos principios, que son similares a los que contemplan los documentos europeos, sostienen lo siguiente:

1. Principio de la licitud y lealtad: Las informaciones relativas a las personas no se deberían recoger ni elaborar con procedimientos desleales o ilícitos, ni utilizarse con fines contrarios a los propósitos y principios de la Carta de las Naciones Unidas.

2. Principio de exactitud: Las personas encargadas de la creación de un fichero o de su funcionamiento deberían tener la obligación de verificar la exactitud y pertinencia de los datos registrados y cerciorarse de que siguen siendo lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen, periódicamente o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando.

---

[6] Cf. Correa y otros. op.cit. supra; ONU, "Los derechos humanos los adelantos científicos y tecnológicos”, Nueva York, 1983. El Estudio preparado por la Secretaría General entre 1973 y 1976, sobre este tema, plantea los problemas que introduce el uso de computadoras para el registro de datos personales, destacando la posibilidad del acceso indiscriminado a la información y el aumento del margen de errores en dicha información, como consecuencia de faltas técnicas o programación defectuosa, recomendando la adopción de resguardos de tipo físico, técnico y jurídico, que permitan equilibrar los beneficios del uso de sistemas computarizados con el respeto de los derechos humanos.

[7] Resolución 44/49 U.N. GAOR Supp. (No. 49) p. 211, ONU Doc. A/44/49 (1989).

[8] Resolución 45/95, de 14/12/1990 de la Asamblea General, http://www.un.org/spanish/documents/ga/res/...

3. Principio de finalidad: La finalidad de un fichero y su utilización en función de esta finalidad deberían especificarse y justificarse y, en el momento de su creación, ser objeto de una medida de publicidad o ponerse en conocimiento de la persona interesada a fin de que ulteriormente sea posible asegurarse de que: a) Todos los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida; b) Ninguno de esos datos personales es utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado; c) El período de conservación de los datos personales no excede del necesario para alcanzar la finalidad con que se han registrado.

4. Principio de acceso de la persona interesada: Toda persona que demuestre su identidad tiene derecho a saber si se está procesando información que le concierne, a conseguir una comunicación inteligible de ella sin demoras o gastos excesivos, a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos y, cuando esta información sea comunicada, a conocer los destinatarios. Debería preverse una vía de recurso, en su caso, ante la autoridad encargada del control (de conformidad con el principio 8 infra). En caso de rectificación, el costo debería sufragarlo el responsable del fichero. Es conveniente que las disposiciones de este principio se apliquen a todas las personas, cualquiera que sea su nacionalidad o su residencia.

5. Principio de no discriminación: A reserva de las excepciones previstas con criterio limitativo en el principio siguiente (6), no deberían registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, o sobre la participación en una asociación o la afiliación a un sindicato.

6. Facultad de establecer excepciones: Sólo pueden autorizarse excepciones a los principios 1 a 4 si son necesarias para proteger la seguridad nacional, el orden público, la salud o la moral pública y, en particular, los derechos y libertades de los demás, especialmente de personas perseguidas (cláusula humanitaria), a reserva de que estas excepciones se hayan previsto expresamente por la ley o por una reglamentación equivalente, adoptada de conformidad con el sistema jurídico nacional, en que se definan expresamente los límites y se establezcan las garantías apropiadas. Las excepciones al principio 5, relativo a la prohibición de discriminación, deberían

estar sujetas a las mismas garantías que las previstas para las excepciones a los principios 1 a 4 y sólo podrían autorizarse dentro de los límites previstos por la Carta Internacional de Derechos Humanos[9] y demás instrumentos pertinentes en materia de protección de los derechos y de lucha contra la discriminación.

7. Principio de seguridad: Se deberían adoptar medidas apropiadas para proteger los ficheros contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático.

8. Control y sanciones: Cada legislación debería designar una autoridad que, de conformidad con el sistema jurídico interno, se encargue de controlar el respeto de los principios anteriormente enunciados. Dicha autoridad debería ofrecer garantías de imparcialidad, de independencia con respecto a las personas u organismos responsables del procesamiento de los datos o de su aplicación, y de competencia técnica. En caso de violación de las disposiciones de la legislación interna promulgada en virtud de los principios anteriormente enunciados, deberían preverse sanciones penales y de otro tipo así como recursos individuales apropiados.

9. Flujo de datos a través de las fronteras: Cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos. Cuando no haya garantías comparables, no se podrán imponer limitaciones injustificadas a dicha circulación, y sólo en la medida en que así lo exija la protección de la vida privada.

10. Campo de aplicación: Los presentes principios deberían aplicarse en primer lugar a todos los ficheros computadorizados, tanto públicos como privados y, por extensión facultativa y a reserva de las adaptaciones pertinentes, a los ficheros manuales. Podrían tomarse disposiciones particulares, igualmente facultativas, para extender la aplicación total o parcial de estos principios a los ficheros de las personas

[9] Así se denomina al conjunto integrado por la "Declaración Internacional de Derechos Humanos (1948), junto con el "Pacto Internacional sobre Derechos Civiles y Políticos", el "Pacto Internacional de Derechos Económicos, Sociales y Culturales" y sus respectivos protocolos opcionales (1966).

jurídicas, en particular cuando contengan en parte información sobre personas físicas.

Se recomienda que las Organizaciones internacionales apliquen estos principios rectores y que "debería preverse de manera específica una excepción a estos principios cuando el fichero tenga por finalidad proteger los derechos humanos y las libertades fundamentales de la persona de que se trate, o prestar asistencia humanitaria".

2.3. Directrices y Directivas Europeas

Sin duda, es en Europa donde pueden rastrearse los principales antecedentes documentales de la protección de datos personales. En primer término, reseñaremos los estudios y recomendaciones de principios de la década del setenta, para ir luego a las directrices de la Organización para la Cooperación y el Desarrollo Económico (en adelante, OCDE), el Convenio de 1981 y finalizar con las Directivas de la Comunidad Europea.

2.3.1. Directrices del Comité de Ministros

En Europa podemos citar como primera expresión relativa a la protección de datos de carácter personal dos resoluciones del Comité de Ministros, en las que se encuentran los primeros antecedentes de lo que luego serían el Convenio de Estrasburgo y las Directivas de la Comisión y el Parlamento europeos.

La primera es la Resolución Nº 22, de 1973, relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado[10].

En dicha Resolución se parte de la base que los sistemas informáticos se usaban ya a una escala importante y cada vez mayor en lo relativo al registro de datos de carácter personal de los individuos y que para impedir abusos con motivo del registro, el tratamiento y la difusión de datos de carácter personal por los bancos

[10] Adoptada por el comité de Ministros el 26/09/1973, durante la 224a. Reunión de los Delegados de los Ministros.

electrónicos de datos del sector privado convenía adoptar medidas legislativas para proteger a los individuos.

En esta dirección, y hasta que se concretara un acuerdo internacional, se elaboran una serie de principios aplicables a la información relativa a las personas que se halle registrada en banco de datos electrónicos del sector privado, entendiendo por "informaciones relativas a las personas" la referente a las personas físicas, y por "banco de datos electrónicos" todo sistema de tratamiento electrónico de la información que se utilice para gestionar información relativa a las personas y para difundirla.

Aquí encontramos por primera vez las reglas que luego constituirán los principios reguladores del tratamiento de datos personales. Ellos son:

1) La información registrada deberá ser exacta y mantenerse actualizada.

2) Por lo general, no se registrará información relativa a la intimidad de las personas o que pueda dar lugar a discriminación, o al menos no deberá difundirse.

3) La información deberá ser adecuada y pertinente para la finalidad que se persiga.

4) La información no deberá obtenerse por medios fraudulentos o desleales.

5) Deberán determinarse normas para establecer el periodo máximo de conservación o utilización de determinadas categorías de información.

6) Sin la autorización correspondiente, no podrá utilizarse la información para fines distintos de aquellos para los que se hubiera registrado, ni podrá facilitarse a terceros.

7) Por lo general, la persona pertinente tendrá derecho a conocer la información registrada que le concierna, así como a conocer la finalidad del registro de la misma y las comunicaciones efectuadas.

8) Deberá hacerse lo necesario para corregir la información inexacta y para suprimir la que haya caducado o se haya obtenido ilícitamente.

9) Deberán adoptarse precauciones para evitar abusos o usos inadecuados de la información.Los bancos de datos electrónicos deberán disponer de sistemas de seguridad para impedir que personas que no tengan derecho a obtener la información accedan a ella y para detectar el desvío de ésta, con intención o sin ella. El acceso a la información deberá estar limitado a las personas que tengan interés legítimo en conocerla. El personal responsable de la puesta en funcionamiento de los banco de datos electrónicos deberá estar sujeto a normas de actuación destinadas a impedir el uso incorrecto de la información y, en particular, a normas de secreto profesional. Los datos estadísticos sólo podrán difundirse de forma abreviada y de tal manera que resulte imposible determinar a quien pertenecen.

La otra es la Resolución Nº 29 de 1974, relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector publico[11].

En este documento, el objetivo declarado es contribuir a la comprensión y la confianza del público en lo referente a las nuevas técnicas administrativas considerando que la utilización de los bancos de datos electrónicos por las autoridades públicas había suscitado una mayor sensibilización respecto a la necesidad de proteger la vida privada de los individuos.

Se recomienda a los Estados miembros que adopten todas las medidas que consideren necesarias para aplicar los principios que se señalan a continuación.

El público deberá ser informado regularmente de la creación, el funcionamiento y el desarrollo de los bancos de datos electrónicos en el sector publico.

La información registrada deberá: a) obtenerse por medios lícitos y leales, b) ser exacta y estar actualizada, c) ser adecuada y pertinente para la finalidad perseguida. Deberá hacerse lo necesario para corregir la información inexacta y para suprimir la que sea inadecuada, no pertinente o caduca.

[11] Adoptada por el comité de Ministros el 20/09/1974, durante la 236a. reunión de los Delegados de los Ministros.

En particular, cuando los bancos de datos electrónicos traten información relativa a la intimidad de la vida privada de las personas, o cuando el tratamiento de las información pueda dar origen a discriminaciones, la creación de los mismos deberá ser prevista por la ley o por una reglamentación especial, o su existencia deberá hacerse pública en una declaración o un documento, de conformidad con el sistema jurídico de cada Estado Miembro. Dicha ley, reglamentación, declaración o documento deberán precisar la finalidad del registro y de la utilización de la información, así como las condiciones en que ésta podrá ser facilitada dentro del sector público o a personas u organismos privados;

La información registrada no deberá utilizarse para fines distintos de los que se hubieran definido, salvo que la ley autorice expresamente una excepción, que una autoridad competente la conceda, o que se modifiquen las normas por las que se regula la utilización del banco de datos electrónicos.

Deberán establecerse normas para determinar el plazo máximo de conservación o utilización de determinadas categorías de información.

No obstante, este principio podrá ser derogado en caso de que la utilización de dicha información para fines estadísticos, científicos o históricos exija su conservación durante un período no determinado. En tal caso, deberán adoptarse medidas para no atentar contra la vida privada de los interesados.

Todas las personas tendrán derecho a conocer la información registrada que les concierna. Toda excepción a este principio o toda limitación del ejercicio de tal derecho deberán estar estrictamente reglamentadas.

Deberán tomarse precauciones contra abusos o usos inadecuados de la información. A tal fin: a) cualquiera que intervenga en la creación de un banco de datos electrónicos deberá estar vinculado por normas de actuación destinadas a prevenir el uso incorrecto de la información y, en particular, deberá estar obligado al secreto; b) Los bancos de datos electrónicos deberán disponer de sistemas de seguridad para impedir que personas que no tengan derecho a obtener la información accedan a ella y para detectar desvíos de ésta, intencionales o no.

El acceso a la información que no pueda comunicarse libremente al público

también deberá quedar limitado a las personas facultadas para tener conocimiento de la misma en el ejercicio de sus funciones.

Cuando los datos se utilicen con fines estadísticos únicamente podrán ser difundidos de forma que resulte imposible atribuirlos a una persona determinada.

Como puede advertirse, aun con diferentes redacciones, estos principios han sido luego recogidos, total o parcialmente, por la mayoría de las normas del derecho comparado, incluida la legislación argentina.

2.3.2. Otras iniciativas relacionadas

Hasta el comienzo de la década de los ochenta, se sucederán otras iniciativas de diversa envergadura.

La Resolución del Parlamento Europeo del 21 de febrero de 1975, sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática[12] que, basándose en el Informe Mansfield de la Comisión Jurídica, alienta a adoptar una directiva sobre libertad individual e informática, con el objeto de asegurar a los ciudadanos comunitarios la mejor protección frente a abusos en el tratamiento de sus datos y de evitar la elaboración de legislaciones nacionales contradictorias.

El 18 de mayo de 1977 se crea la Subcomisión «Informática y derechos de la persona» en el seno de la Comisión Jurídica del Parlamento europeo.

La Resolución del 8 de mayo de 1979 del Parlamento europeo sobre la "protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática"[13] toma como referencia el Informe Bayerl y constata que la regulación de la protección de datos puede incidir, directamente, en la instauración y funcionamiento del mercado común, perturbando la competencia[14].

---

[12] JO Nº C 60, 13/03/1975, p. 48.
[13] JO Nº C 140, 05/06/1979, p. 34.
[14] Guerrero Picó, María del Carmen, "El derecho fundamental a la protección de datos

2.3.3. Directrices para la Protección de la Privacidad y el Flujo Internacional de Datos Personales de la OCDE

La Organización para la Cooperación y el Desarrollo Económico (OCDE) es una organización internacional intergubernamental que reúne a los países más industrializados de economía de mercado, cuyas raíces se remontan a 1948, a través de la Organización para la Cooperación Económica Europea, encargada de administrar el Plan Marshall para la reconstrucción europea. El objetivo que persigue es estimular y desarrollar la economía y el comercio internacional; por ende, los estudios realizados en su seno tienen como fin último la identificación y análisis de las consecuencias que los nuevos desarrollos tecnológicos tienen en la economía y en el comercio mundial[15].

En 1969 la OCDE creó el Grupo de Expertos sobre Bancos de Datos (*Data Bank Panel*), que se dedicó al análisis y estudio de diferentes aspectos relacionados con datos personales y la privacidad. El Simposio de Viena de 1977, organizado por dicho grupo, recogió un conjunto de principios básicos que reconocen: (a) la necesidad de que la información fluya de forma regulada entre los países; (b) que es legítimo que los países impongan regulaciones para el flujo de información que pueda resultar contraria al orden público, o que atente contra la seguridad nacional; (c) que el flujo de información tiene un valor económico intrínseco importante para las economías de los países; (d) que los países deben adoptar medidas de seguridad mínimas para la protección de la información, así como regular sobre la protección de dicha información, para evitar su uso o aprovechamiento ilegítimos; y (e) que los países deben asumir un compromiso de adopción de principios generales para la protección de datos personales[16].

En 1978, en el seno de la OCDE se creó el Grupo de Expertos sobre Barreras Transfronterizas de Información y Protección de Privacidad, al que le fue encomendado desarrollar lineamientos de consenso general con la finalidad de

---

personales en la Constitución Europea", http://www.ugr.es/

[15] Ver http://www.oecd.org/

[16] Reyes Krafft, Alfredo Alejandro, "Protección de datos personales en México. Génesis legislativa", Revista Derecho Informático - Alfa Redi Nº 100, noviembre 2006.

armonizar las legislaciones domésticas o nacionales de los paises; el resultado de la tarea fue publicado bajo el título “Lineamientos sobre la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales”, de 1980 (OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) [17].

Su contenido es muy similar al del Convenio del Consejo de Europa sobre protección de datos, el cual será tratado más adelante. Ello ha contribuido a consagrar, en el ámbito internacional, cuatro normas jurídicas o principios básicos que deberán ser respetados en las transmisiones de datos, dentro de las fronteras de los Estados, o entre éstos. En relación a las transmisiones internacionales de datos, estas Directrices recomiendan los siguientes principios:

“a) los Estados deben tener en cuenta las implicaciones del procesamiento interno y reexportación de datos personales a otros Estados (parágrafo 15). El énfasis de esta cláusula pone de relieve la necesidad de un respeto mutuo entre los Estados en el área de la protección de datos personales y la vida privada. Ello implica que la normativa nacional sobre transferencias internacionales de datos no debe estar destinada a eludir o violar las regulaciones de otros Estados en materia de protección de datos personales y vida privada;

b) cada Estado debe tomar las medidas razonables y apropiadas para que las transmisiones internacionales sean ininterrumpidas y seguras, incluso cuando se realizan a través del territorio de un Estado miembro (esta cláusula no es más que la extensión del principio básico de seguridad a la transmisión internacional de datos);

c) los Estados deben evitar, en general, restringir las transferencias internacionales de datos personales, excepto cuando: 1) los Estados receptores “no observen” el contenido de las Directrices; 2) cuando la reexportación de datos personales eluda las disposiciones internas del Estado transmisor; ó 3) cuando ciertas categorías de datos personales -e.g. datos sensibles- reciban una protección especial

[17] Recomendación relativa a las directrices aplicables a la protección de la vida privada y a los flujos transfronterizos de datos personales, adoptada por el Consejo de la OCDE el 23/09/1980. Su texto en francés: http://www.oecd.org/document/18/0,2340,fr_2649_34255_1815225_1_1_1_1,00.html/.

en la legislación interna y tal protección no sea equivalente en otros Estados;

d) los Estados deben evitar adoptar disposiciones normativas, políticas y prácticas legales cuando: 1) la única finalidad sea proteger la intimidad y las libertades individuales, si para ello se obstaculiza la transmisión internacional de datos; 2) el contenido de las disposiciones exceda de la normativa ya existente sobre el tema. Con esta cláusula, las Directrices intentan buscar un equilibrio entre la protección de la intimidad y la libre circulación internacional de información."

En 1985, la OCDE adoptó una declaración sobre las transferencias internacionales de datos no personales[18] y posteriormente creó una "Comisión sobre información automatizada y privacidad" para estudiar una posible revisión de las Directrices de 1980.[19]

2.3.4. El Convenio 108 de Estrasburgo

La "Convención Europea para la protección de los individuos con relación al procesamiento automático de datos personales", conocida como Convenio de Estrasburgo ó Convenio 108, suscripto por veintiún estados europeos el 21 de enero de 1981[20], sobre la base de los antecedentes que hemos mencionado, estableció un conjunto de principios básicos para la protección de los datos de carácter personal, bajo el rótulo de "calidad de los datos".

Del mencionado convenio destacamos el artículo 5º sobre "Calidad de los datos", que establece: "Los datos de carácter personal que sean objeto de un tratamiento automatizado: a) se obtendrán y tratarán leal y legítimamente; b) se

---

[18] Declaración relativa a los flujos transfronterizos de datos no personales, adoptada por los gobiernos de los Países Miembros de la OCDE el 11/04/1985.
[19] Recomendación relativa a las directrices de política criptográfica, adoptada por el Consejo de la OCDE el 02/03/1997 y Declaración relativa a la protección de la intimidad en las redes globales, realizada por los ministros de la OCDE en la conferencia "Un mundo sin fronteras: comprender el potencial del comercio electrónico global", celebrada entre el 7 y el 9/10/1998 en Ottawa, Canadá.
[20] Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter Personal, Estrasburgo, 28/01/1981, BOE, 15/11/1985. Su texto lo hemos reproducido en Altmark -Molina Quiroga, "Régimen jurídico de los bancos de datos", ut supra cit.

registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; d) serán exactos y si fuera necesario puestos al día; e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado."

Se lo considera el primer instrumento jurídico internacional contraído con vocación universal en el ámbito de la protección de datos y, junto a otros textos dictados en la época por la Organización para la Cooperación y el Desarrollo Económico[21], tiene indudable relevancia a nivel europeo[22].

A pesar de la necesidad de elaborar un texto propio, es decir lo que se conoce como "Directiva", sobre protección de datos de carácter personal, y haber recomendado la comisión que el Convenio fuera ratificado antes de terminar 1982, se abrió un período de análisis y estudios que duró varios años.

Otro instrumento importante es la Resolución del Parlamento de 9 de marzo de 1982, sobre la protección de los derechos de la persona ante el desarrollo de los progresos técnicos en el ámbito de la informática[23].

2.3.5. Acuerdo de Schengen

El 14 de junio de 1985 Alemania, Bélgica, Francia, Holanda y Luxemburgo adoptaron un acuerdo relativo a la supresión gradual de controles en las fronteras comunes, denominado "Acuerdo de Schengen", y el 19 de junio de 1990, su Convenio de aplicación[24].

---

[21] Como las Líneas directrices que han de regir en lo concerniente a la protección de la vida privada y los flujos transfronterizos de datos de carácter personal, de 23/09/1980, que hemos glosado supra.
[22] Heredero Higueras, "La Directiva comunitaria de protección de los datos de carácter personal, Aranzadi, Pamplona, 1997; Guerrero Picó, ob.cit. supra.
[23] JO núm. C 87, de 05/04/1982.
[24] El acuerdo del Gobierno Español está publicado en BOCG, Senado, Serie IV, 20/02/ 1992.

Este acuerdo comprende el control del cruce de fronteras interiores y exteriores, las peticiones de asilo y la cooperación policial y judicial penal, instaurando un sistema de información común, denominado “Sistema de Información Schengen” (SIS).

El SIS se compone de dos partes: una nacional, en cada uno de los Estados partícipes e idénticas entre sí, y una unidad de apoyo técnico, cuya gestión recae sobre Francia. Las autoridades designadas por las Partes pueden consultar este sistema de redes informáticas, que incluye datos concernientes a personas buscadas para su detención a efectos de extradición; nacionales de países terceros que estén incluidos en la lista de no admisibles en un Estado firmante; personas desaparecidas; testigos y personas citadas para comparecer ante las autoridades judiciales; personas o vehículos registrados a efectos de vigilancia y objetos buscados con vistas a su incautación o como pruebas en un procedimiento penal.

En lo que respecta a las personas, las categorías de datos cuyo registro se permite son: el nombre y los apellidos (en su caso, también los alias, pero registrados por separado), los rasgos físicos particulares, objetivos e inalterables, la primera letra del segundo nombre, la fecha y el lugar de nacimiento, el sexo, la nacionalidad, la indicación de si están armadas o son violentas, el motivo de la inscripción y la conducta que debe observarse. No se autorizan más anotaciones, en particular las referidas a los datos sensibles a los que alude el art. 6 del Convenio número 108 del Consejo de Europa, esto es, aquéllos que revelen origen racial o estén referidos a opiniones políticas, convicciones religiosas o similares, salud, vida sexual y condenas penales.

Sin ser ésta la única referencia que sobre la materia se puede encontrar en el Convenio, los arts. 102 a 118 articulan el elenco de garantías que protegen a las personas concernidas frente a la recogida, tratamiento y transmisión de sus datos de carácter personal en el marco del SIS. Más allá de imponer ciertas medidas de seguridad al responsable que trata la información, se consagran los principios de exactitud, actualidad, licitud, limitación temporal y adecuación a los fines perseguidos y se reconocen los derechos de acceso, rectificación y cancelación del afectado, si bien contemplándose un amplio número de excepciones, que han sido criticadas por considerarse no siempre justificadas y que, redactadas de manera indeterminada, no permiten asegurar la proporcionalidad de tales salvedades, y han motivado que se

consideren insuficientes las garantías en este ámbito.[25]

2.3.6. La Directiva 95/46/CE

Las exigencias del mercado europeo implican la circulación de un Estado a otro, entre otros bienes y servicios, de los datos de carácter personal, ya que su tratamiento es cada vez más demandado por el sector económico privado.

Las diferencias jurídicas en la regulación en esta materia conspiraban contra un flujo transfronterizo de datos y se planteó la necesidad de armonizar las legislaciones nacionales en materia de protección de datos de carácter personal.

El trámite de la Directiva que reemplazaría al Convenio 108 no resultó sencillo. El 18 de julio de 1990 la Comisión presentó al Consejo la primera propuesta de Directiva[26], que provocó muchas observaciones. En julio de 1992, se presentó una nueva propuesta[27] que suprime la distinción entre tratamiento público y privado y se atenúa la incidencia del consentimiento para determinar la licitud del tratamiento. Se introduce el concepto "tratamiento" en vez de hacer girar las normas en torno al concepto de "fichero" (más restringido) y se da la posibilidad de eximir de la notificación a determinados tratamientos o de simplificar sus trámites. Así se aprueba finalmente[28].

La "Directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal y a la libre circulación de estos datos"[29] (en adelante, Directiva

---

[25] Guerrero Picó, ob.cit. En sentido coincidente fueron la mayoría de las ponencias de autores españoles en el IV Congreso Iberoamericano de Informática y Derecho, Bariloche, Argentina, 1994.
[26] COM (90) 314-SYN 287 y 288, de 24/09/1990.
[27] COM (92) 422 final, DO Nº C 311, de 27/11/1992.
[28] Guerrero Picó, ob.cit. supra.
[29] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24/10/1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Diario Oficial N° L 281 de 23/11/1995, P. 0031-0050) En Legislación comunitaria vigente: documento 31995L0046 (cons. http://europa.eu.int/). Ver Padilla, Miguel M., "La directiva 95/46/CE de la Unión Europea", LA LEY, 1999-B, 970.

95/46/CE) se concibe, en realidad, como una herramienta para impedir las trabas a la libre circulación de información personal en el contexto del mercado interior europeo.[30]

El ámbito de aplicación de la Directiva es más restringido que el del Convenio 108, ya que rige el tratamiento total o parcialmente automatizado de datos personales e, igualmente, el tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (art. 3.1), sin ser lo más relevante el soporte en el que se consignan los datos personales. Se excluyen los tratamientos realizados en ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario; los tratamientos de datos cuyo objeto sea la seguridad pública (v. gr., video-vigilancia policial), la defensa y la seguridad del Estado (incluido el bienestar económico de éste cuando dicho tratamiento esté relacionado con la seguridad del mismo), las actividades del Estado en materia penal y los tratamientos hechos por las personas físicas en el ejercicio de actividades exclusivamente personales o domésticas (art. 3.2).

Este capítulo de excepciones generó algunos conflictos interpretativos, resueltos en 2003 por el Tribunal de Justicia de las Comunidades Europeas (en adelante, TJCE). En uno de los casos, Austria consultó si se aplicaba la Directiva 95/46/CE frente a algunas disposiciones de su Ley federal constitucional sobre la limitación de la retribución de funcionarios públicos, que obliga a recoger datos sobre los ingresos de ciertos empleados de sociedades y entidades públicas, con el fin de incluirlos (indicando el nombre de las personas afectadas), en el informe anual del Tribunal de Cuentas, destinado a ser hecho público[31]. En otro caso se trataba de una página web personal, creada por una catequista sueca, en la que ésta había incluido

---

[30] Guerrero Picó, ob.cit. supra, señala que es una forma de evitar que la defensa de los derechos fundamentales se torne en freno para los objetivos de la integración económica, eludiendo por demás el inconveniente de que dicha tutela sea argüida por las Administraciones nacionales para falsear la competencia e incumplir los cometidos que les atribuye el Derecho comunitario.

[31] Sentencia del 20/05/2003 sobre los asuntos C-465/00, “Rechnungshof contra Österreichischer Rundfunk” y los asuntos acumulados C-138/01 y C-139/01 («Neukomm» y «Lauermann» contra «Österreichischer Rundfunk»), según Guerrero Picó, ob.cit. supra http://curia.europa.eu/jurisp/cgi.bin/form.pl?/ang=es/

datos personales de sus compañeros[32].

En las conclusiones presentadas en los dos expediente, el Abogado General afirmó que ambas situaciones estaban fuera del ámbito de aplicación de la Directiva 95/46/CE, porque la primera actividad atañe a la política presupuestaria nacional, no regulada a nivel comunitario, y en el segundo caso, porque se trataba de una actividad no económica y la Comunidad Europea no tiene competencia para dictar normas en materia de derechos fundamentales, argumentando que el art. 100 A TCE (actual art. 95 TCE) no podía invocarse como el fundamento de medidas que no encuentran su justificación en el objetivo de promover "el establecimiento y el funcionamiento del mercado interior".[33]

El TJCE entendió que la aplicabilidad de la Directiva 95/46 no podía depender de que las situaciones concretas en análisis tengan un vínculo suficiente con el ejercicio de las libertades fundamentales garantizadas por el Tratado y, en particular en los referidos asuntos, con la libre circulación de los trabajadores, ya que una interpretación contraria podría hacer que los límites del ámbito de aplicación de la referida Directiva se volvieran particularmente inciertos y aleatorios, lo que sería contrario al objetivo esencial de ésta. Recordó que el fin es la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros para eliminar los obstáculos al funcionamiento del mercado interior derivados precisamente de las disparidades entre las legislaciones nacionales[34]. Esta posición se reafirmó en

---

[32] Sentencia 6/11/2003, que da respuesta al asunto C-101/01, «Göta hovrätt» contra «Bodil Lindqvist») (http://curia.europa.eu/jurisp/cgi.bin/form.pl?/ang=es/ DO C7 de 10/01/2004, p.3

[33] Conclusiones del Abogado General A. Tizziano presentadas el 14/11/2002 (asunto C-465/00 y asuntos acumulados C-138/01 y C-139/01) y el 19/09/2002 (asunto C-101/01). En la doctrina española apoya las tesis del Abogado General, cuestionando la base jurídica de la Directiva, Ruiz, Miguel, "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico", (RDCE , Nº 14, Enero-Abril 2003, pp. 7-43), citados por Guerrero Picó, ob.cit. supra.

[34] En la sentencia del 20/05/2003, la parte resolutiva dice: "El Tribunal de Justicia, pronunciándose sobre las cuestiones planteadas por el Verfassungsgerichtshof mediante resolución de 12 de diciembre de 2000 y por el Oberster Gerichtshof mediante resoluciones de 14 y 28 de febrero de 2001, declara: 1) Los artículos 6, apartado 1, letra c), y 7, letras c) y e), de la Directiva 95/46/CE del Parlamento

la segunda sentencia que concluyó que la obligación de suministrar al Tribunal de Cuentas austríaco el nombre e ingresos de las personas ligadas al sector público que perciben un determinado sueldo y la inclusión de datos personales en una página web personal sí estaban comprendidas por la Directiva 95/46/CE. Aclaró que distinta cuestión es si en él se cumplen los requisitos que permiten limitar legítimamente el derecho fundamental a la protección de datos personales (los del art. 8.2 CEDH), en el caso austríaco, extremo que deben apreciar los órganos jurisdiccionales nacionales; o, en el caso sueco, cómo ha de resolverse el conflicto entre el derecho a la protección de datos y el derecho de creación artística o la libertad de expresión[35].

Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, no se oponen a una normativa nacional, como la controvertida en los asuntos principales, siempre que se demuestre que la amplia divulgación no sólo del importe de los ingresos anuales, cuando éstos superan un límite determinado, de las personas empleadas por entidades sujetas al control del Rechnungshof, sino también de los nombres de los beneficiarios de dichos ingresos, es necesaria y apropiada para lograr el objetivo de buena gestión de los recursos públicos perseguido por el constituyente, extremo que ha de ser comprobado por los órganos jurisdiccionales remitentes. 2) Los artículos 6, apartado 1, letra c), y 7, letras c) y e), de la Directiva 95/46 son directamente aplicables, en el sentido de que un particular puede invocarlos ante los órganos jurisdiccionales nacionales para evitar la aplicación de normas de Derecho interno contrarias a dichas disposiciones."

[35] En la sentencia del 6/11/ 2003, el Tribunal de Justicia, pronunciándose sobre las cuestiones planteadas por el Göta hovrätt mediante resolución de 23 de febrero de 2001, declara: "1) La conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. 2) Un tratamiento de datos personales de esta naturaleza no está comprendido en ninguna de las excepciones que figuran en el artículo 3, apartado 2, de la Directiva 95/46. 3) La indicación de que una persona se ha lesionado un pie y está en situación de baja parcial constituye un dato personal relativo a la salud en el sentido del artículo 8, apartado 1, de la Directiva 95/46. 4) No existe una «transferencia a un país tercero de datos» en el sentido del artículo 25 de la Directiva 95/46 cuando una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por una persona física o jurídica que gestiona el sitio Internet en el que se puede consultar la página web que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquellas

2.3.6.1 Principios consagrados por la Directiva 95/46/CE

Los principios que como mínimo deben acoger las normas nacionales en materia de protección de datos personales están bastante detallados en la Directiva 95/46/CE y son los siguientes:

1) Calidad de los datos (art. 6). La Directiva parte de que todo tratamiento ha de adecuarse al principio de lealtad y licitud. Después especifica que la recogida de datos personales debe responder a fines determinados, explícitos y legítimos y que éstos no podrán ser tratados posteriormente de manera incompatible con tales fines. La sentencia del TJCE de 20 de mayo de 2003, que hemos mencionado, ha declarado el efecto directo del art. 6.1,c), que es el que atiende a estos extremos. Un particular puede invocarlos ante los órganos jurisdiccionales nacionales para evitar la aplicación de normas de Derecho interno contrarias a dichas disposiciones[36].

También se limita el plazo de conservación de los datos al establecer que éstos no se conservarán durante más tiempo que el preciso para realizar los fines que motivaron la recogida o tratamiento (limitación que no afecta a los datos almacenados con fines históricos, estadísticos o científicos). Transcurrido ese lapso, no se

---

que se encuentren en países terceros. 5) Las disposiciones de la Directiva 95/46 no entrañan, por sí mismas, una restricción contraria al principio general de la libertad de expresión o a otros derechos y libertades vigentes en la Unión Europea y que tienen su equivalente, entre otros, en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado en Roma el 4 de noviembre de 1950. Incumbe a las autoridades y a los órganos jurisdiccionales nacionales encargados de aplicar la normativa nacional que adapta el Derecho interno a la Directiva 95/46 garantizar el justo equilibrio entre los derechos e intereses en juego, incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario. 6) Las medidas adoptadas por los Estados miembros para garantizar la protección de los datos personales deben atenerse tanto a las disposiciones de la Directiva 95/46 como a su objetivo, que consiste en mantener el equilibrio entre la libre circulación de datos personales y la tutela del derecho a la intimidad. En cambio, nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a lo dispuesto en la Directiva 95/46 a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello." (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62001J0101:ES:HTML/

[36] Ver nota anterior donde se transcribe la parte dispositiva de la sentencia mencionada

conservarán en forma que permita identificar al individuo.

El principio de proporcionalidad de la información, que integra la exigencia de calidad, exige que la información personal sea adecuada, pertinente y no excesiva con relación a los fines del tratamiento. En este sentido, los datos deberán ser exactos y estar actualizados para que en cada momento respondan con fidelidad a la realidad del sujeto. De no cumplirse esta previsión, se prevé un procedimiento de rectificación o cancelación de los mismos.

2) Legitimidad del tratamiento (art. 7). Las condiciones concurrentes que requiere un tratamiento de datos personales para ser considerado legítimo son: a) que el interesado preste su consentimiento inequívoco (expreso o tácito); b) que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte o bien para la aplicación de medidas precontractuales adoptadas a petición de éste; c) que sea preciso para cumplir una obligación jurídica a la que esté sujeto el responsable del tratamiento; d) que se requiera para proteger el interés vital del interesado; e) que deba hacerse para cumplir una misión de interés público o inherente al ejercicio del poder público conferida al responsable del tratamiento o a un tercero a quien se comuniquen los datos; f) que sea preciso para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos (v. gr. los ficheros de solvencia y morosidad), siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado.

El TJCE declaró en mayo de 2003 el efecto directo de los derechos consagrados en los apartados c) y e) del art. 7.[37]

3) Datos sensibles o especialmente protegidos (art. 8). Los datos que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos o aspectos referidos a la salud o la sexualidad, calificados de “sensibles”, son merecedores de una mayor protección en atención a que pudieran ser el fundamento de decisiones discriminatorias o especialmente

[37] Ver nota anterior donde se transcribe la parte dispositiva de la sentencia mencionada

perjudiciales para sus titulares. Su tratamiento está prohibido, aunque la regla admite numerosas salvedades.

Excepcionalmente, podrán tratarse si: a) el interesado prestó su consentimiento explícito (a no ser que lo prohíba la legislación nacional); b) el tratamiento tenga que realizarse para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral (si se prevé en la legislación y con las garantías adecuadas); c) el tratamiento es requerido para salvaguardar el interés vital del interesado u otra persona (v. gr. si él está física o jurídicamente incapacitado); d) el tratamiento se efectúa en el curso de sus actividades legítimas y con las debidas garantías por una fundación, asociación o cualquier organismo sin fin de lucro cuya finalidad sea política, filosófica, religiosa o sindical, siempre que concierna exclusivamente a sus miembros o personas que mantengan contactos regulares con ellas (no obstante, no se cederán a terceros sin consentimiento de los titulares); e) se trata de datos que el interesado ha hecho manifiestamente públicos o es algo necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

La prohibición general tampoco operará en contextos relacionados con la salud: cuando el tratamiento se deba a la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios. Será así cuando se realice por un profesional sanitario sujeto al secreto profesional o una persona ligada a una obligación equivalente. A la vez, la Directiva deja la puerta abierta a los Estados para establecer un régimen más amplio de excepciones. Están autorizados a hacerlo, implantando las garantías adecuadas, a través de su legislación o mediando una decisión de su autoridad de control. Su proceder habrá de estar motivado por significativas razones de interés público y deberán notificarlo a la Comisión[38].

[38] Hemos efectuado una aproximación al tema, en relación al derecho positivo argentino, en Molina Quiroga, Eduardo, “"Los datos de salud en la ley 25.326 de Protección de Datos Personales", LexisNexis 0003/010495 ó 0003010502 –JA 2004-II-1395 – SJA 28/04/2004; Wierzba, Sandra M., “Protección de Datos de Salud en Procesos Judiciales. Transparencia judicial y confidencialidad de datos de litigantes

La norma comunitaria alude específicamente a otros dos tipos de datos: a) los relativos a infracciones, condenas penales o medidas de seguridad. Su tratamiento estará sometido al control de la autoridad pública, más podrá realizarse por otros sujetos si hay previstas garantías específicas en el Derecho nacional y el Estado no lo impide. El registro completo de las condenas penales sólo puede efectuarse bajo el control de los poderes públicos y queda a la voluntad de los Estados miembros someter a ese control a los datos relativos a sanciones administrativas o procesos civiles. b) Los números de identificación. No se prohíbe la existencia de un número nacional o similar de identificación de los ciudadanos[39]; serán los Estados quienes fijen las condiciones en que éste podrá ser objeto de tratamiento.

4) Tratamientos realizados con fines periodísticos, de expresión artística o literaria (art. 9). La norma comunitaria no ignora el conflicto que pudiera darse entre la protección de datos y otros derechos fundamentales, por lo que indica a los Estados que podrán establecer excepciones al régimen general si los datos son tratados con fines periodísticos, de expresión artística o literaria, pero al indicar que "sólo" versarán sobre las disposiciones de los capítulos II (condiciones generales de licitud de los tratamientos), IV (transferencias internacionales) y VI (autoridad de control), se abarca prácticamente todo el sistema protector de la Directiva.

5) Confidencialidad y seguridad (arts. 16 y 17). Entre otras medidas de control de los tratamientos se propone restringir el acceso a los datos personales a sus encargados o a terceros que actúen bajo instrucciones del responsable del tratamiento o por imperativo legal.

El responsable del tratamiento está obligado a aplicar las medidas técnicas y de organización adecuadas para proteger los datos personales contra su destrucción (accidental o ilícita), su pérdida, alteración, difusión o acceso no autorizados (en particular cuando haya una transmisión de datos dentro de una red) y contra cualquier

---

con VIH-SIDA:¿existe oposición entre tales principios?"; Tanús, Daniel Gustavo, "La protección de los datos personales de salud y la ley 25.326", Revista Derecho y Nuevas Tecnologías, Nº 4-5, Editorial Ad-Hoc, Buenos Aires, 2003.

[39] La Constitución de Portugal de 1978 lo prohíbe en su artículo 35 inciso 5: "É proibida a atribuição de um número nacional único aos cidadãos".

otro tratamiento ilícito. Las medidas de protección y las obligaciones de seguridad que conciernen al responsable del tratamiento se hacen extensivas al encargado del mismo, que habrá de estar vinculado a aquél por medio de un contrato.

Estos principios deben ser observados por el responsable del tratamiento con independencia de que éste sea consentido por la persona concernida. Como dijimos, el centro de gravedad del sistema protector instaurado por la Directiva 95/46/CE se desplaza a las condiciones de licitud del tratamiento, a diferencia de la propuesta de Directiva de 1990, que daba mayor relevancia al papel jugado por el consentimiento.[40]

2.3.6.2. Derechos

En otro orden de consideraciones, la Directiva 95/46/CE determina que deben reconocerse los siguientes derechos a las personas concernidas:

1) El derecho a ser informado, tanto si los datos se obtienen del titular como si no (arts. 10 y 11). Este derecho es primordial para el correcto funcionamiento del sistema de protección de datos pues difícilmente se podrán ejercer derechos como el de acceso u oposición al tratamiento si el individuo no ha obtenido una previa información de ciertos extremos.[41]

Salvo que hubiera sido informada con anterioridad, el responsable del tratamiento o su representante deben advertir a la persona de quien recaben sus datos sobre la identidad de ambos y los fines del tratamiento. Cuando sea preciso para garantizar un tratamiento leal de los datos deben comunicar quiénes son los destinatarios o las categorías de destinatarios de los datos, el carácter obligatorio o no de su respuesta más las consecuencias de una negativa a ella y la existencia de los derechos de acceso y rectificación.

En la hipótesis de que los datos no se recabaran del interesado, la obligación de informar procede, en idénticos términos, desde el momento del registro de los datos o, cuando se piensen comunicar a un tercero, en el momento de la primera

---

[40] Cf. Guerrero Pico, ob.cit. supra.
[41] Ídem. Es una opinión que hemos compartido en todas nuestras exposiciones.

comunicación. No es preciso informar (adoptando las garantías pertinentes) si se trata de un tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley.

2) Los derechos de acceso, rectificación y cancelación (art. 12). Los Estados miembros tienen que garantizar al interesado el derecho a obtener del responsable del tratamiento libremente, sin restricciones, con una periodicidad razonable y sin retrasos ni gastos excesivos, la confirmación de la existencia o no de tratamientos de datos que le conciernan, los fines de tales tratamientos, las categorías de datos que constan y los destinatarios o las categorías de destinatarios a quienes se comunicarán dichos datos. El responsable tendrá que hacerle saber, de manera inteligible, qué datos son objeto de tratamiento y su origen, así como la lógica utilizada en los tratamientos automatizados que los contengan (al menos en los casos en que se vayan a adoptar decisiones automatizadas).

El interesado tiene derecho a la rectificación, supresión o bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva (v. gr. por ser incompletos o inexactos). La rectificación, supresión o bloqueo debe notificarse luego a los terceros a quienes se hayan comunicado los datos, a no ser que resulte imposible o suponga un esfuerzo desproporcionado.

3) El derecho de oposición (art. 14). En primer lugar, el interesado puede oponerse a que sus datos sean objeto de tratamiento, “al menos” en los supuestos del art. 7,e) y f) (cumplimiento de una misión de interés público o inherente al ejercicio de un poder público o tratamiento necesario para satisfacer un interés legítimo del responsable), en cualquier momento y por razones legítimas propias de su situación particular, salvo que el Estado decida no permitirlo. En segundo lugar, se faculta al individuo a oponerse, previa petición y sin gastos, al tratamiento de sus datos destinado a la prospección. Antes de que dichos datos se comuniquen por primera vez a terceros o se usen en nombre de éstos (también a efectos de prospección) deberá informársele y ofrecerle expresamente la posibilidad de oponerse, igualmente sin

gastos, a dicha comunicación o utilización.[42]

4) Perfiles. El derecho a no verse sometido a una decisión basada en tratamientos automatizados de datos (art. 15). Las personas tienen el derecho a no verse sometidas a una decisión que tenga efectos jurídicos sobre ellas o les afecte de manera significativa y se base sólo en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad (rendimiento laboral, crédito, fiabilidad, conducta, etc.). Se exceptúan los supuestos en que la decisión se adopte en el marco de la celebración o ejecución de un contrato hecho a petición del interesado o cuando éste tenga la posibilidad de defender su punto de vista para salvaguardar su interés legítimo y también cuando esa valoración esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

5) El derecho a una indemnización (art. 23). La persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la Directiva, tiene derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. La responsabilidad objetiva de dicho responsable podrá excluirse si demuestra que no cabe imputarle el hecho que ha provocado el daño.[43]

6) El derecho a un sistema de recursos y sanciones (arts. 22 y 24). Aparte de la existencia de un recurso administrativo ante la autoridad nacional de protección de datos (art. 28), se puede acudir a la vía judicial en caso de violación de los derechos

---

[42] Según Guerrero Picó, ob.cit. supra, la Directiva prescinde de reconocer un derecho general de oposición aunque, vistos los términos en los que se pronuncia, tampoco cabe concluir que lo circunscribe únicamente a los dos supuestos que enuncia.

[43] v.gr. por responsabilidad del interesado o fuerza mayor, como señala el considerando 55 de la Directiva: ”Considerando que las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados; que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento de datos, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor; que deben imponerse sanciones a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva”.

de los interesados. Para ello, los Estados deben establecer las medidas adecuadas para garantizar la plena aplicación de la Directiva, fijando las sanciones que deben aplicarse cuando no se respeten las pautas que proporciona. Sin esta referencia el sistema de garantías, simplemente, no estaría completo.

2.3.6.3. Limitaciones impuestas por los Estados.

El art. 13 faculta a los Estados a establecer límites al principio de calidad de los datos, información, acceso, rectificación y cancelación y a la obligación de dar publicidad a los tratamientos. Estos límites proceden cuando constituyan una medida necesaria para la salvaguarda de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección y represión de infracciones penales o de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos de seguridad pública, infracciones penales e interés económico; g) la protección del interesado o de los derechos y libertades de otras personas.

De la misma manera, sin perjuicio del establecimiento de las garantías legales apropiadas, los Estados pueden, si manifiestamente no existe ningún riesgo de atentado contra la vida privada del interesado, limitar mediante disposición legislativa los derechos de acceso, rectificación y cancelación cuando los datos vayan a ser exclusivamente tratados con fines de investigación científica o estadística.

Las transferencias internacionales de datos personales sólo pueden efectuarse cuando se garantice un nivel de protección adecuado (arts. 25 y 26). Los criterios a tomar en consideración, en cada supuesto concreto, para valorar la adecuación son: la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y de destino final, la legislación (general o sectorial) vigente, las normas profesionales y las medidas de seguridad en vigor.

La Directiva 95/46/CE erige a la Comisión en garante de las transferencias internacionales de datos. Cuando ella misma (directamente o informada por un Estado miembro) comprueba que un tercer Estado no garantiza un nivel de protección

adecuado, debe adoptar las medidas adecuadas para evitar cualquier transferencia de datos a ese país y realizar las negociaciones pertinentes para corregir tal situación. En sentido contrario, la Comisión puede hacer constar que un país tercero asegura un nivel de protección adecuado, vista su legislación interna o sus compromisos internacionales.

Así ha ocurrido con Argentina, Suiza, Hungría, la Bailía de Guernsey y la Isla de Man y, en determinados supuestos, de Estados Unidos (empresas adheridas al Acuerdo sobre Puerto Seguro y "Passenger Name Records" PNR)[44] y Canadá (entidades privadas de ámbito federal que recojan, utilicen o divulguen datos personales en sus actividades comerciales).[45]

Sin embargo, realizar una transferencia de datos a un tercer Estado aun cuando no garantice un nivel adecuado de protección puede ser legítimo. Salvo disposición en contra del Estado miembro, se permitirá siempre y cuando: a) medie el consentimiento inequívoco del interesado a la transferencia; b) la transferencia se requiera para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado; c) sea preciso para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del titular de los datos, entre el responsable del tratamiento y un tercero; d) sea necesario o venga legalmente exigido para la salvaguarda de un interés público importante o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; e) se pretenda para la protección de un interés vital del interesado; f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y abierto a la consulta general o por cualquier persona que pueda demostrar

---

[44] Cuestiones que abordaremos más adelante.

[45] Decisiones de la Comisión de 26/07/2000, sobre Suiza, Hungría (hoy Estado miembro) y Puerto Seguro (DO Nº L 215, de 25/08/2000, p. 1, 4 y 7, respectivamente); de 20/12/2001, sobre Canadá (DO Nº L 2, de 04/01/2002, p. 13); de 30/06/2003, sobre Argentina (DO Nº L 168, de 05/07/2003, p. 19); de 21/11/ 2003, sobre Guernsey (DO Nº L 308, de 25/11/2003, p. 27) y de 28/04/2004, sobre la Isla de Man (DO Nº L 208, de 10/06/2004, p. 47), entre otras. Pueden consultarse en http://www.agpd.es/index.php?dSeccion=86 ó en http://ec.europa.eu/justice_home/fsj/privacy/workinggroups/wpdocs/2005_eu.htm

un interés legítimo (cumpliendo las condiciones que establezca la ley para la consulta).

Los Estados miembros también pueden autorizar transferencias de datos personales informando a la Comisión si el responsable del tratamiento ofrece garantías suficientes respecto de la protección de la vida privada y sus derechos instrumentales. En este sentido, es frecuente que tales garantías se deriven de cláusulas contractuales apropiadas.

Un caso que está resultando especialmente polémico es el acceso al PNR («Passenger Name Records» ó registro de nombre de pasajeros) por parte de las autoridades estadounidenses. De hecho, ha motivado un grave conflicto entre las instituciones de la Unión, al que nos referiremos más adelante.

Luego del 11 de setiembre de 2001, en Estados Unidos se dicta una batería de leyes y normas diversas dirigidas a reforzar la seguridad nacional.[46] Entre ellas, la "Aviation and Transport Security Act", de 19 de noviembre de 2001 y la "Enhanced Border Security and Visa Entry Reform Act", de 14 de mayo de 2002, obligan a todas las compañías dedicadas al transporte aéreo internacional de pasajeros, con vuelos con destino, origen o escala en Estados Unidos, a proporcionar acceso electrónico al PNR[47] al Servicio de Aduanas y Protección de Fronteras del Departamento de Seguridad Interior estadounidense. De esta suerte, entrando informáticamente en el registro electrónico de las compañías y utilizando el sistema APIS ("Advance Passenger Information System"), las autoridades norteamericanas pretenden determinar de antemano el peligro potencial que podría entrañar cada uno de los pasajeros, asegurar la identificación y detención de cualquier terrorista o individuo

[46] Hacemos una enumeración al referirnos a la legislación estadounidense.
[47] Dependiendo de los usos comerciales, en el PNR pueden constar hasta sesenta tipos de datos que permiten identificar al pasajero, las personas que lo acompañan, las que han efectuado la reserva en su nombre, la agencia o el empleado que tramitó la reserva y/o emitió el billete, y los miembros de la tripulación: itinerario y billetes, medios de pago, número de tarjeta de crédito, condiciones especiales ofrecidas a grupos específicos (pasajeros frecuentes, miembros de grupos especiales), direcciones de correo electrónico y direcciones físicas, números de teléfono particulares y/o profesionales declarados, personas de contacto, servicios específicos vinculados al estado de salud y preferencias sobre alimentación, observaciones concretas efectuadas por el personal de la compañía aérea, detalles relacionados con las reservas para el alquiler de un automóvil,

responsable de delitos graves o impedir su entrada en Estados Unidos[48].

Esta orden ocasiona espinosos problemas desde el punto de vista de la protección de datos personales, como veremos luego. Estados Unidos no reconoce con carácter general el derecho fundamental a la protección de datos personales, pese a que la privacidad se menciona en la Cuarta Enmienda a la Constitución norteamericana. Lo hace básicamente cuando existe un riesgo de abuso gubernamental en el trato de la información personal y, de este modo, la ley federal interviene sólo frente a él («Privacy Act» de diciembre de 1974) o cuando se trata de negocios que almacenan información personal sensible (v. gr. datos médicos, financieros o sobre el alquiler de determinadas películas de vídeo). En el resto de casos, si se disciplina, se hace por medio de disposiciones de carácter autorregulatorio. Además, en el concreto ámbito al que se alude, no existe tutela alguna respecto de los datos de pasajeros que no son ciudadanos de los Estados Unidos (o residentes legales) ni tampoco recurso judicial contra eventuales abusos en la aplicación de dichas medidas.[49]

Acceder al PNR significaba realizar una transferencia internacional ilegal según los cánones de la Directiva 95/46/CE; por ello, entre junio de 2002 y mayo de 2004 se desarrolló un complejo proceso de negociación para paliar tal contradicción. Dicho proceso culminó con la autorización de las transferencias a través de la Decisión del 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de Estados Unidos («Bureau of Customs and Border Protection»)**[50]** y la Decisión 2004/496/CE del Consejo, de 17 de mayo, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos**[51]**.

---

[48] Guerrero Picó, ob.cit. supra.
[49] Guerrero Picó, ob.cit. supra.
[50] Puede consultarse en http://eur-lex.europa.es/
[51] DO N° L 235 de 06/07/2004, p. 11 y DO Nº L 183, de 20/05/2004, p. 83,

No obstante, vistos los términos del acuerdo, el acceso al PNR seguía sin respetar el contenido y la finalidad de la Directiva 95/46/CE, por lo que ambos textos fueron recurridos por el Parlamento Europeo ante TJCE el 25 de junio de 2004. El Tribunal de Justicia de la Unión Europea, en un fallo de su Gran Sala, de fecha 30 de mayo de 2006, resolvió anular el mencionado Acuerdo.[52]

2.3.7. Reglamento CE Nº 45/2001

El denominado "Reglamento (CE) N° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos"[53], contiene disposiciones muy parecidas a las de la Directiva 95/46/CE, si bien el capítulo IV se refiere a la protección de los datos en el contexto de las redes internas de telecomunicación, esto es, al objeto de la antigua Directiva 97/66/CE.[54]

Consagra el principio de calidad de los datos (art. 4), de licitud del tratamiento (art. 5) -previendo el cambio de fines (art. 6)-, de información (arts. 11 y 12) y de confidencialidad y seguridad (arts. 21 a 23), estableciendo determinadas particularidades en lo que respecta al tratamiento de las categorías especiales de datos (art. 10). Reconoce los derechos de acceso (art. 13), rectificación (art. 14),

---

respectivamente. Pueden consultarse en http://eur-lex.europa.es/

[52] Asuntos acumulados C-317/04 y C-318/04. La parte dispositiva dice: "1) Anular la Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos, y la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos." (http://eur-lex.europa.eu/LexUriServ/site/es/oj/2006/c_178/c_17820060729es00010002.pdf/, Publicado en el DO 29/07/2006, C 178/1.

[53] Diario Oficial N° L 008, 12/01/2001, p. 0001 – 0022.

[54] Vid. también la Decisión 2004/644/CE del Consejo, de 13/09/2004, por la que se adoptan las normas de desarrollo del Reglamento (CE) Nº 45/2001 (DO Nº L 296, 21/09/2004, p. 16).

bloqueo (art. 15), supresión (art. 16), notificación a terceros (art. 17), oposición (art. 18) y no sometimiento a decisiones individuales automatizadas (art. 19), recogiendo un régimen de excepciones en el art. 20. Establece asimismo cuáles son las obligaciones del responsable del tratamiento (arts. 24-31) e implanta un sistema de recursos (arts. 32-33) y sanciones (art. 49). También encuentran acomodo en él algunas normas destinadas a regular la transmisión de datos de carácter personal, distinguiendo en función de que ésta se lleve a efecto entre las instituciones u organismos comunitarios (art. 7) o con otros diferentes (arts. 8 y 9).

El Reglamento crea una autoridad de control independiente, el Supervisor Europeo de Protección de Datos[55], quien no puede recibir instrucción alguna y le corresponde fiscalizar la aplicación efectiva de las disposiciones reglamentarias por las instituciones y organismos comunitarios.

Las tareas que se le encomiendan son: investigar eventuales violaciones de las normas sobre protección de datos (a iniciativa propia o en respuesta a reclamaciones) y comunicar a los interesados su resultado en plazo razonable; supervisar y asegurar la aplicación del Reglamento y cualquier otro acto comunitario que proteja en el plano institucional a las personas físicas (salvo los tratamientos que realice el TJCE cuando actúe en el ejercicio de sus funciones jurisdiccionales); asesorar, previa petición o a iniciativa propia, a todas las instituciones y organismos comunitarios, especialmente antes de que elaboren normas internas sobre este tema; colaborar con las autoridades de control nacionales y participar en las actividades del Grupo del art. 29; hacer públicas y explicitar los motivos en los que se fundan las excepciones o autorizaciones que el Reglamento permite adoptar (en materia de datos sensibles, información cuando los datos no proceden del titular, decisiones automatizadas o datos de tráfico de las comunicaciones); mantener un registro de los tratamientos y efectuar una comprobación previa de los que se le notifiquen.

Además, entre sus competencias está: asesorar a las personas en el ejercicio de sus derechos; acudir al responsable del tratamiento en caso de presunta infracción y formular propuestas encaminadas a corregirla; ordenar la atención de los derechos

[55] http://www.edps.eu.int/

que se denieguen indebidamente; advertir o amonestar, cuando proceda, al responsable del tratamiento; imponer una prohibición temporal o definitiva del tratamiento; someter un asunto a la institución u organismo comunitario de que se trate; someter un asunto al TJCE en las condiciones previstas en el Tratado e intervenir en los asuntos presentados ante él. Anualmente presentará un informe sobre su actividad al Parlamento Europeo, Consejo y Comisión y lo hará público.

Merece la pena destacar que, sin perjuicio de eventuales recursos ante el TJCE, todo interesado está facultado a presentar (sin necesidad de pasar por la vía jerárquica) una reclamación ante el Supervisor si considera violados los derechos que le reconoce el art. 286 TCE[56]. Por otra parte, las decisiones del Supervisor son susceptibles de recurso ante el TJCE.

2.3.8 Otros actos normativos europeos

La Comunidad Europea ha producido varios actos normativos referidos a la protección de datos personales, además de los ya mencionados, que enunciaremos a título informativo.

Resolución del Consejo de la Unión Europea de 19 de enero de 1999 sobre la dimensión relativa a los consumidores en la sociedad de la información (1999/C 23/01).[57]

---

[56] Artículo286 (Tratado constitutivo de la Unión Europea). “1.A partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo. 2. Con anterioridad a la fecha indicada en el apartado 1, el Consejo establecerá, con arreglo al Procedimiento previsto en el artículo 251, un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes. (Diario Oficial de la Unión Europea 29/12/2006). Su texto en español puede consultarse en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:321E:0001:0331:ES:pdf

[57] EUR-Lex: Legislación comunitaria vigente, Documento 399Y0128(01) Capítulos del Repertorio donde puede consultarse este documento: 15.20 - Protección del consumidor; 13.20.60 - Tecnología de la información, telecomunicaciones, informática. Resolución del Consejo de 19/01/1999 sobre la dimensión relativa a los consumidores en la sociedad de la información Diario Oficial N° C 023, 28/01/1999, p. 0001 – 0003.

Acto del Consejo de 12 de marzo de 1999 por el que se fijan las normas para la transmisión por Europol de datos personales a Estados y organismos terceros.[58]

Decisión de la Comisión 2001/497/CE, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE.[59]

Decisión de la Comisión 2002/16/CE, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE.[60]

Acto del Consejo, de 28 de febrero de 2002, que modifica el Acto del Consejo de 12 de marzo de 1999 por el que se fijan las normas para la transmisión por Europol de datos personales a Estados y organismos terceros.[61]

Resolución del Consejo de 18 de febrero de 2003 sobre un enfoque europeo orientado hacia una cultura de seguridad de las redes y de la información.[62]

Reglamento (CE) n° 1882/2003 del Parlamento Europeo y del Consejo de 29 de septiembre de 2003 sobre la adaptación a la Decisión 1999/468/CE del Consejo de las disposiciones relativas a los comités que asisten a la Comisión en el ejercicio de sus competencias de ejecución previstas en los actos sujetos al procedimiento establecido en el artículo 251 del Tratado CE.[63]

Directiva 2004/33/CE de la Comisión, de 22 de marzo de 2004, por la que se aplica la Directiva 2002/98/CE del Parlamento Europeo y del Consejo en lo que se refiere a determinados requisitos técnicos de la sangre y los componentes

---

[58] Diario Oficial N° C 088, 30/03/1999, p. 0001 – 0003 (31999F0330).
[59] Diario Oficial N° L 181, 04/07/2001, p. 0019 – 0031(32001D0497) [notificada con el número C(2001) 1539].
[60] Diario Oficial N° L 006, 10/01/2002, p. 0052 – 0062 (32002D0016) [notificada con el número C(2001) 4540].
[61] Diario Oficial N° C 076, 27/03/2002, p. 0001 – 0002 (32002X0327(01).
[62] Diario Oficial N° C 048, 28/02/2003, p. 0001 – 0002 (32003G0228(01).
[63] Diario Oficial N° L 284, 31/10/2003, p. 0001 – 0053 (32003R1882).

sanguíneos.[64]

Decisión de la Comisión 2004/535/CE, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (Bureau of Customs and Border Protection).[65]

Decisión del comité mixto del EEE n° 105/2004 de 9 de julio de 2004 por la que se modifica el anexo XI (Servicios de telecomunicaciones) del Acuerdo EEE.[66]

Decisión del Consejo 2004/644/CE, de 13 de septiembre de 2004, por la que se adoptan las normas de desarrollo del Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.[67]

Reglamento (CE) N° 2006/2004 del Parlamento Europeo y del Consejo, de 27 de octubre de 2004, sobre la cooperación entre las autoridades nacionales encargadas de la aplicación de la legislación de protección de los consumidores («Reglamento sobre la cooperación en materia de protección de los consumidores»).[68]

Reglamento (CE) n° 2073/2004 del Consejo, de 16 de noviembre de 2004, sobre cooperación administrativa en el ámbito de los impuestos especiales.[69]

Decisión de la Comisión 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a

---

[64] Diario Oficial N° L 091, 30/03/2004, p. 0025 – 0039 (32004L0033).
[65] Diario Oficial N° L 235, 06/07/2004, p. 0011 – 0022 (32004D0535) (notificada con el número C(2004) 1914).
[66] Diario Oficial N° L 376, 23/12/2004, p. 0035 – 0036 (22004D0105).
[67] Diario Oficial N° L 296, 21/09/2004, p. 0016 – 0022 (32004D0644).
[68] Diario Oficial N° L 364, 09/12/2004, p. 0001 – 0011 (32004R2006).
[69] Diario Oficial N° L 359, 04/12/2004, p. 0001 – 0010 (32004R2073).

terceros países.[70]

También debemos mencionar la Carta de Derechos Fundamentales de la Unión Europea de 2000[71], cuyo artículo 8 establece: "(Protección de datos de carácter personal). 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

2.3.9. Directivas sectoriales.

Junto a la propuesta de Directiva general sobre protección de datos (luego Directiva 95/46), se propugnaba la adopción de otra serie de actos referidos a sectores más específicos, como el de las telecomunicaciones, pero recién en diciembre de 1997 se aprobó la Directiva 97/66/CE del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[72], norma sectorial relativa al tratamiento de los datos de carácter personal y a la protección de la intimidad en el ámbito de las telecomunicaciones, que precisa y completa a la Directiva 95/46/CE.

Ésta ha sido reemplazada por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos de carácter personal y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).[73]

Luego de los atentados sufridos en el Continente y en aras a aumentar la

---

[70] Diario Oficial n° L 385, 29/12/2004, p. 0074 – 0084 (32004D0915) (notificada con el número C(2004) 5271).
[71] Diario Oficial de las Comunidades Europeas C 364/1,18/12/2000, http://www.europarl.europa.eu/charter/pdf/txt_es.pdf
[72] Diario Oficial N° L 024, 30/01/1998, p. 0001–0008; EUR-Lex: Legislación comunitaria vigente - Documento 397L0066.
[73] Diario Oficial N° L 201, 31/07/2002, p. 0037 – 0047.

defensa nacional y la seguridad publica, se aprobó la Directiva 2006/24/CE que introdujo diversas modificaciones a la Directiva 2002/58/CE.[74]

Esta Directiva se plantea "armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro.

Aclara que se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado, pero no al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas (art. 1).

Si bien se exige la conservación de una variada gama de datos para cumplir con el objetivo mencionado, se establece que "no podrá conservarse ningún dato que revele el contenido de la comunicación" (art. 5 ap.2).

El período de conservación de los datos es por un período de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación (art. 6).

En cuanto a la Protección y seguridad de los datos, se enfatiza que "sin perjuicio de lo dispuesto en las … Directivas 95/46/CE y 2002/58/CE, los Estados miembros velarán por que los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones cumplan, en lo

[74] Directiva 2006/24/CE del Parlamento europeo y del Consejo, 15/03/2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Su texto puede consultarse en español en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF.

que respecta a los datos conservados de conformidad con la presente Directiva, como mínimo los siguientes principios de seguridad de los datos: a) los datos conservados serán de la misma calidad y estarán sometidos a las mismas normas de seguridad y protección que los datos existentes en la red; b) los datos estarán sujetos a las medidas técnicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, pérdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos; c) los datos estarán sujetos a medidas técnicas y organizativas apropiadas para velar por que sólo puedan acceder a ellos las personas especialmente autorizadas, y d) los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación" (art. 7).

Los Estados miembros debían trasponer estas directrices a sus legislaciones internas antes de setiembre de 2007. Los efectos de esta nueva Directiva serán analizados en setiembre de 2010 para evaluar su impacto en las relaciones económicas y en los consumidores y actualizar los datos técnicos, sobre todo los contenidos en el art. 5 que enumera los datos a conservar.

2.4. Síntesis

La reseña de los documentos (recomendaciones, declaraciones, tratados europeos, directivas y reglamentos) indican que existe una clara preocupación internacional por los efectos que produce el tratamiento de datos personales, y las principales pautas o criterios que se encuentran en los mismos constituyen elementos orientadores y de consulta imprescindible cuando se analice la aplicación de la normativa argentina en esta materia. Como se irá corroborando al relevar otros sectores del derecho comparado, la moderna construcción de protección de los datos personales o autodeterminación informativa, como se prefiera, excede largamente el ámbito de la tutela a la intimidad o vida privada, aún cuando claramente la contiene.

Capítulo 3. Derecho comparado. Constituciones y Leyes europeas

Sumario: 1. Constituciones europeas. Portugal, España, Países Bajos, Croacia, Albania, Bulgaria, Eslovenia, Eslovaquia, Rusia, Bielorrusia (Belarús), Bosnia-Herzegovina, Hungría, Polonia, Finlandia, Estonia, 2. Leyes nacionales, Suecia, Alemania, Francia, Austria, Dinamarca, Noruega, Luxemburgo, Finlandia, Islandia, Gran Bretaña, Portugal, Hungría, Bélgica, Italia, Otras legislaciones. Síntesis.

El continente europeo puede considerarse la cuna de la protección de datos personales y por ello vamos a reseñar las normas constitucionales y la legislación de sus países.

La primera ley que se ocupó de este tema fue la del Estado (Land) de Hesse de la ex-República Federal de Alemania el 7 de octubre de 1970[1]. Posteriormente se sancionaron numerosas normas de nivel nacional, incluso con anterioridad al Convenio de Estrasburgo que mencionamos en el capítulo anterior. En algunos países, a la sanción de leyes específicas precedió una protección a nivel constitucional.

3.1. Constituciones europeas

3.1.1. Portugal

La Constitución de 1976 incluyó el artículo 35, con el siguiente texto: "1)Todos los ciudadanos tienen derecho a tomar conocimiento de los datos contenidos en ficheros y registros informáticos[2] a su respecto, pudiendo exigir su rectificación y actualización, sin perjuicio de lo dispuesto por las leyes sobre secretos de Estado y secretos de Justicia; 2) Está prohibido el acceso a ficheros y registros informáticos para conocer datos personales de terceros o por interconexión, salvo los casos excepcionales previstos por la ley; 3) La informática no puede ser utilizada para el tratamiento de datos referidos a convicciones filosóficas o políticas, de filiación partidaria o sindical, de fe religiosa o vida privada, salvo cuando se trate de

[1] "Datenschutz", 07/10/1970, del Land de Hesse, ex República Federal Alemana, modificada en 31/01/1978 y en 06/11/1986. También debe mencionarse la "Landesdatenschutzgesetz", de 24/01/1974 de Renania -Palatinado.
[2] "mecanográficos" decía su primera versión.

procesamiento de datos estadísticos que no se identifiquen individualmente"[3].

Este artículo fue modificado en 1997, para concordar con la Directiva 95/46/CE sobre la protección a los datos contenidos en ficheros manuales. El texto actual dice: "Artículo 35º: (Utilización de la informática). 1. Todos los ciudadanos tienen el derecho de acceso a los datos informatizados que se refieran a ellos, pudiendo exigir su rectificación y actualización, y el derecho de conocer la finalidad a que se destinan, en los términos de la ley. 2. La ley define el concepto de datos personales, así como las condiciones aplicables a su tratamiento automatizado, conexión, trasmisión y utilización, y garantiza su protección, por medio de una autoridad administrativa independiente. 3. La informática no puede ser utilizada para el tratamiento de datos referentes a convicciones filosóficas o políticas, filiaciones partidarias o sindicales, fé religiosa, vida privada y origen étnico, salvo mediante el consentimiento expreso del titular, autorización prevista por ley con garantias de no discriminación o para el procesamiento de datos estatísticos no individualmente identificables. 4. Está prohibido el acesso a los datos personales de terceros, salvo en casos excepcionales previstos en la ley. 5. Está prohibida la atribución de um número nacional único a los ciudadanos. 6. Se garantiza a todos el libre aceso a las redes informáticas de uso público, debiendo definir la ley el régimen aplicable al flujo de datos transfronterizos y las formas adecuadas de protección de datos personales y de otros cuya salvaguarda se justifique por razones de interes nacional."[4]

---

[3] El texto puede consultarse en http://www.constitucion.es/otras_constituciones/europa/txt/constitucion_portugal.html

[4] http://www.parlamento.pt/const_leg/crp_port/crp_97_html. El texto en portugués dice: "Artigo 35.º: (Utilização da informática). 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. 5. É proibida a atribuição de um número

3.1.2. España

La Constitución de 1978 incluyó el artículo artículo 18 inciso 4) que reza: “La ley limitará el uso de la información para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de los derechos”.[5]

3.1.3. Países Bajos

En 1983 se incorporó a la Constitución, en su artículo 10, este texto: “1. Toda persona tiene derecho al respeto de su vida privada, salvo las restricciones dispuestas por la ley o en virtud de la ley. 2. La ley establecerá normas para la protección de la vida privada en relación con la recogida y difusión de datos personales. 3. La ley establecerá normas referentes al derecho de toda persona a conocer los datos registrados que le afecten y su utilización, así como a poder rectificarlos.”[6]

Ya a fines o en la década de los noventa, varios países europeos introdujeron textos constitucionales referidos a la protección de datos personales.

3.1.4. Croacia

En 1990, incluyó en en el art. 37 de su Constitución el siguiente texto: “(1) Se garantiza la seguridad y el secreto de los datos personales. Sin el consentimiento por parte de la persona concernida no puede recolectarse, procesarse ni usar datos personales, solo bajo las condiciones especificadas en la ley. (2) La protección de los

---

nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei.”, http://www.assembleiadarepublica.pt/

[5] http://www.constitucion.es/constitucion/castellano/index.html/

[6] La Constitución de los Países Bajos data de 1814 y hasta 1830, año en que Bélgica se separó del Reino de los Países Bajos se aplicó también a dicho país. Tras diversas vicisitudes históricas entre las que destacaríamos, las grandes reformas parlamentarias de 1848, la introducción del sufragio universal limitado a los varones, en 1917, y la modificación de la composición de las Cámaras en 1956, se procedería a una revisión general de la Constitución en 1983, en relación con el texto de 1972., http://www.constitucion.es/otras_constituciones/europa/holanda.html/

datos y la supervisión de los sistemas de información en la República de Croacia son resultado por la ley (3) El uso de los datos personales en forma contraria a los fines indicados en la recolección está prohibido".[7]

3.1.5. Albania

En 1991, también contempló en su artículo 35 un texto similar: 1. "Nadie está obligado, salvo cuando la ley lo requiera, a hacer públicos los datos conectados con su persona. 2. La recolección, uso y publicidad de los datos sobre una persona es posible con su consentimiento, excepto en los casos previstos por la ley 3. Cada uno tiene derecho a conocer los datos recogidos sobre él, salvo los casos previstos por la ley. 4. Cada uno tiene derecho a la rectificación o supresión de los datos falsos o recolectados en violación a la ley".[8]

3.1.6. Bulgaria

También en 1991 este país introdujoe el tema en el artículo 32 de su Constitución, con el siguiente texto: "(1) La vida privada de los ciudadanos es inviolable. Cada uno tiene derecho para pedir protección ante cualquier injerencia ilegal en su vida privada o asuntos familiares y contra ataques a su honor, dignidad y reputación (2) Nadie puede ser seguido, fotografiado, filmado, registrado o sometido a cualquier otra actividad similar, sin su conocimiento o con su desaprobación expresa,

---

[7] Artículo 37 (en inglés –la traducción del texto principal es propia) "(1) Everyone is guaranteed the safety and secrecy of personal data. Without consent from the person concerned, personal data may be collected, processed, and used only under conditions specified by law.(2) Protection of data and supervision of the work of information systems in the Republic are regulated by law. (3) The use of personal data contrary to the purpose of their collection is prohibited.",
http://www.fuhem.es/portal/areas/paz/mediterraneo/constituciones/Croacia.htm/

[8] Articulo 35 (en inglés –la traducción del texto principal es nuestra): "1. No one may be obliged, except when the law requires it, to make public data connected with his person. 2. The collection, use and making public of data about a person is done with his consent, except for the cases provided by law. 3. Everyone has the right to become acquainted with data collected about him, except for the cases provided by law. 4. Everyone has the right to request the correction or expunging of untrue or incomplete data or data collected in violation of law."

salvo autorización legal".[9]

3.1.7. Eslovenia

La Constitución de 1991 protegió el derecho a la privacidad y otros derechos personalísimos, en el artículo 35, con este tenor: "Se garantiza la inviolabilidad de la integridad de toda persona, tanto física como mental, su vida privada y derechos de la personalidad."

El artículo 37 está referido a la protección de la privacidad de la correspondencia y de otros medios de comunicación, de este modo: "(1) Se garantiza la privacidad (o confidencialidad) de la correspondencia y otros medios de comunicación (2) Solo por ley y en base a una orden judicial puede suspenderse estos derechos por el tiempo necesario en el curso de una investigación penal o por razones de seguridad nacional".

El artículo 38, específicamente titulado "Protección de datos personales", dice: "Se garantiza la protección de los datos personales. Está prohibido el uso de estos datos para fines distintos a los dados para su recolección. (2) La recolección, procesamiento, destino, seguridad y protección de la confidencialidad de los datos perpersonales será prevista por la ley. (3) Cada uno tiene derecho de acceso a los datos personales recolectados sobre uno y derecho a protección judicial en caso de cualquier abuso sobre los mismos".[10]

---

[9] Artículo 32 (en inglés – la traducción del texto principal es nuestra) "(1) The privacy of citizens shall be inviolable. Everyone shall be entitled to protection against any illegal interference in his private or family affairs and against encroachments on his honour, dignity and reputation. (2) No one shall be followed, photographed, filmed, recorded or subjected to any other similar activity without his knowledge or despite his express disapproval, except when such actions are permitted by a law", http://www.justiniano.com/constituciones/constituciones_del_mundo.htm.

[10] Artículos 35, 37 y 38 (en inglés –la traducción en el texto principal es propia): "Article 35 (Protection of Rights to Privacy and Personality Rights) The inviolability of the physical and mental integrity of every person, his privacy and personality rights shall be guaranteed. Article 37 (Protection of the Privacy of Correspondence and Other Means of Communication) (1) The privacy of correspondence and other means of communication shall be guaranteed. (2) Only a law may prescribe that on the basis of a court order the protection of the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time

3.1.8. Eslovaquia

En 1992, incorporó tres artículos en su Constitución, referidos al tema en análisis. El artículo 19 sobre “Derecho a la privacidad", reza: ”(1) Cada uno tiene derecho a preservación de su dignidad humana y honor personal, y a la protección de su buen nombre. (2) Cada uno tiene derecho a no sufrir injerencias injustificadas en su vida privada ni familiar. (3) Cada uno tiene derecho a la protección contra todo otro uso ilícito de sus datos personales”.

El artículo 22, sobre “Confidencialidad de las comunicaciones”, establece: “Se garantiza la privacidad de la correspondencia y el secreto de los mensajes enviados, así como de otros documentos escritos y la protección de datos personales. (2) No puede violarse la privacidad de la correspondencia ni el secreto de otros documentos escritos o registros, si se mentienen como confidenciales o reservados o son enviados por correo, con excepción de los casos en que lo autorice una ley. Igualmente se garantiza el secreto de los mensajes enviados por telefono, telégrafo u otros medios similares”.

En la tercera parte, dedicada a los derechos políticos, el artículo 26, sobre “libertad de expresión”, dice: “(1) Se garantiza la libertad de discurso y el derecho a la información. (2) Cada uno tiene derecho a expresar sus opiniones oralmente, por escrito, impresas, gráficas u otros medios, así como el derecho de buscar, recibir, y elegir libremente ideas e información sin limite de fronteras. No es necesario permiso para el ejercicio de la prensa. Las empresas de radio y televisión no están sujetas a procedimientos de autorización estatal. Las condiciones deben ser establecidas por ley. (3) Está prohibida la censura. (4) La libertad de expresión y el derecho de elegir y buscar información se pueden restringir por ley cuando existan causas justificadas en una sociedad democrática, para proteger los derechos y libertades de otras personas,

---

where such is necessary for the institution or course of criminal proceedings or for reasons of national security. Article 38 (Protection of Personal Data) (1) The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited. (2) The collection, processing, designated use, supervision and protection of the confidentiality of personal data shall be provided by law. (3) Everyone has the right of access to the collected personal data that relates to him and the right to judicial protection in the event of any abuse of such data.”

la seguridad del Estado, el orden público, o la salud pública y moralidad. (5) La administración estatal y territorial deben proveer información sobre sus actividades de una manera apropiada y en el idioma del Estado. Las condicioes y forma de hacerlo se establecerán por ley".[11]

3.1.9. Rusia

La Constitución de 1993, en su artículo 24 estableció: "1) Está prohibida la recopilación, el almacenamiento, la utilización y divulgación de aspectos de la vida privada de una persona, sin su consentimiento. 2) El Estado y los funcionarios deben permitir el acceso de cada ciudadano a todos los documentos y materiales que afecten sus derechos y libertades, salvo que la ley prevea lo contrario".[12]

---

[11]Arts. 19, 22 y 26 (en inglés –la traducción del texto principal es propia): "artículo 19 sobre "Derecho a la privacidad" (1) Everyone has the right to the preservation of his human dignity and personal honor, and the protection of his good name. (2) Everyone has the right to protection against unwarranted interference in his private and family life. (3) Everyone has the right to protection against the unwarranted collection, publication, or other illicit use of his personal data. Article 22 [Secrecy of Communication] (1) The privacy of correspondence and secrecy of mailed messages and other written documents and the protection of personal data are guaranteed. (2) No one must violate the privacy of correspondence and the secrecy of other written documents and records, whether they are kept in privacy or sent by mail or in another way, with the exception of cases to be set out in a law. Equally guaranteed is the secrecy of messages conveyed by telephone, telegraph, or other similar means. Part 3 Political Rights Article 26 [Freedom of Expression] (1) The freedom of speech and the right to information are guaranteed. (2) Everyone has the right to express his views in word, writing, print, picture, or other means as well as the right to freely seek out, receive, and spread ideas and information without regard for state borders. The issuing of press is not subject to licensing procedures. Enterprise in the fields of radio and television may be pegged to the awarding of an authorization from the state. The conditions will be specified by law. (3) Censorship is banned. (4) The freedom of speech and the right to seek out and spread information can be restricted by law if such a measure is unavoidable in a democratic society to protect the rights and liberties of others, state security, public order, or public health and morality. (5) State bodies and territorial self-administration bodies are under an obligation to provide information on their activities in an appropriate manner and in the state language. The conditions and manner of execution will be specified by law.", http://www.justiniano.com/constituciones/constituciones_del_mundo.htm.

[12] Artículo 24 (en inglés –la traducción en el texto principal es propia) "(1) It shall be forbidden to gather, store, use and disseminate information on the private life of any person without his/her consent. (2) The bodies of state authority and the bodies of local

3.1.10. Bielorrusia (Belarús)

La Constitución de 1994, en su artículo 34, prevé que: “Los ciudadanos de la República de Belarús tienen la garantía de recibir, almacenar y divulgar la información completa, oportuna y confiable sobre las actividades de los organismos estatales, las asociaciones públicas, en sus aspectos políticos, económicos, culturales e internacionales, así como lo referido al ambiente; a requerir a los funcionarios estatales la posibilidad de investigar el material que afecte sus derechos e intereses legítimos. El uso de la información puede restringirse mediante ley, con la finalidad de proteger el honor, la dignidad, la vida personal y familiar de los ciudadanos o la plena implementación de sus derechos”.[13]

3.1.11. Bosnia-Herzegovina

La Constitucion de 1995 incorporó en el denominado “párrafo tercero” una enumeración de derechos humanos y además tiene, como anexo que integra la norma, el listado de los principales tratados en la materia. Entre los derechos que se mencionan se encuentra “el derecho a la vida privada y familiar, al domicilio y la correspondencia”.[14]

---

self-government and the officials thereof shall provide to each citizen access to any documents and materials directly affecting his/her rights and liberties unless otherwise stipulated under the law”, http://www.fuhem.es/portal/areas/paz/mediterraneo/constituciones3/rusia.htm.

[13] Artículo 34 (en inglés – la traducción en el cuerpo principal es propia-) “Article 34. Citizens of the Republic of Belarus shall be guaranteed the right to receive, store and disseminate complete, reliable and timely information of the activities of state bodies and public associations, on political, economic, cultural and international life, and on the state of the environment. State bodies, public associations and officials shall afford citizens of the Republic of Belarus an opportunity to familiarize themselves with material that affects their rights and legitimate interests. The use of information may be restricted by legislation with the purpose to safeguard the honour, dignity, personal and family life of the citizens and the full implementation of their rights.”

[14] La Constitución de 1992 lo mencionaba en el art. 23. Este Nuevo texto menciona los derechos fundamentales en su Paragraph 3 “Enumeration of Rights. All persons within the territory of Bosnia and Herzegovina shall enjoy. the human rights and fundamental freedoms referred to in paragraph 2. above; these include: (a) The right to life. (b) The right not to be subjected to torture or to inhuman or degrading treatment or punishment. (c) The right not to be held in slavery or servitude or to perform torced or compulsory

3.1.12. Hungría

El artículo 59 de la Constitución en su versión más reciente dispuso: "1. En la República Húngara toda persona tiene derecho al honor, a la inviolabilidad del domicilio, además de la protección del secreto privado y de los datos personales. 2. Para la aprobación de la ley sobre la protección de los datos personales será necesario el voto de dos tercios de los Diputados Parlamentarios presentes."[15]

3.1.13. Polonia

La Constitución de 1997 consagró en su artículo 47 el derecho de toda persona a la protección legal de su vida privada y familiar, de su honor y buena reputación y a la libre toma de decisiones sobre su vida personal.

En el artículo 49 se garantiza la libertad y privacidad de las comunicaciones y el artículo 51 establece que no se puede obligar a nadie a divulgar información referente a su persona, salvo autorización constitucional. Las autoridades públicas no pueden adquirir, recolectar ni divulgar información de las personas, salvo la necesaria en un estado democrático y en el marco de la ley. Todos tienen acceso a los documentos oficiales y a los archivos de datos que se refieran a sí mismo. Las limitaciones a este derecho deben establecerse por ley. Todos tienen derecho a exigir la corrección o cancelación de la información personal falsa o incompleta, o aquella adquirida en violación a los principios constitucionales. Los principios y procedimientos

---

labor. (d) The rights to liberty and security of person. (e) The right to a fair hearing in civil and criminal matters, and other rights relating to criminal proceedings. (f) The right to private and family life, home, and correspondence. (g) Freedom of thought, conscience, and religion. (h) Freedom of expression. (i) Freedom of peaceful assembly and freedom of association with others. (j) The right to marry and to found a family. (k) The right to property. (l) The right to education. (m) The right to liberty of movement and residence.",
http://www.justiniano.com/constituciones/constituciones_del_mundo.htm.

[15] La constitución húngara vigente es un texto refundido resultante de las profundas modificaciones introducidas en el texto en vigor (promulgado en 1949) el día 31 de diciembre de 1987, y que ha sido modificado posteriormente en 1989, 1990, 1993 y 1994. El contenido ha variado sustancialmente al pasar Hungría de ser un estado socialista a un estado soberano y democrático de Derecho.
http://www.constitucion.es/otras_constituciones/europa/hungría.html y
http://www.embajada-hungria.org/spanyol/consitucion/constitucion3.htm.

para la recolección y el acceso a la información son establecidos por ley.[16]

3.1.14. Finlandia

La Constitución de 2000, estableció en su artículo 10: “Protección de la privacidad. Se garantiza la privacidad, el honor y la inviolabilidad del domicilio de todas las personas. La protección de los datos personales estará regulada más precisamente por ley. El secreto de las comunicaciones postales, telefónicas y otras confidenciales es inviolable. Se podrán establecer por ley y con el objeto de salvaguardar los derechos fundamentales o esclarecer delitos, medidas imprescindibles que afecten el ámbito de la inviolabilidad del domicilio. Asimismo se podrán establecer por ley las limitaciones al secreto de las comunicaciones imprescindibles en la investigación de delitos contra la seguridad de un individuo o de la sociedad o contra la inviolabilidad del domicilio, en procesos judiciales y en el control de la seguridad, así como durante una privación de libertad.”[17]

3.1.15. Estonia

La Constitución de 1992 consagró en su artículo 26 la protección de la vida

---

[16] El texto en inglés (la traducción en el texto en principal es nuestra) “Article 47: Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life. Article 49: The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute. Article 51: (1) No one may be obliged, except on the basis of statute, to disclose information concerning his person. (2) Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law. (3) Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute. (4) Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute. (5) Principles and procedures for collection of and access to information shall be specified by statute.”; http://www.justiniano.com/constituciones/constituciones_del_mundo.htm.

[17] La Constitución de la República de Finlandia es la más reciente dentro del marco de la Unión Europea. Entró en vigor el 01/03/2000, un mes después de que los finlandeses eligieran a la primera presidenta del país, Tarja Jalonen. La nueva Constitución reitera el principio fundamental recogido en textos anteriores: la soberanía reside en el pueblo representado por el parlamento., http://www.constitucion.es/otras_constituciones/europa/finlandia.html/

privada, incluso familiar[18] y en su artículo 44, bajo el rótulo de derecho a la información, establece el derecho a recibir libremente la información circulada para el uso general, así como la referida a la actividad estatal, según los procedimientos legales y agrega que los ciudadanos estonios tienen derecho a conocer la información que sobre ellos tengan las autoridades estatales, el que solo se puede restringir por la ley para proteger derechos y libertades de otras personas. Consagra también el secreto de la ascendencia de los niños, o los procesos para prevenir o reprimir delitos o aclarar la verdad para un proceso legal. Este derecho, salvo excepción legal alcanza no solo a los estones sino incluso a los apátridas.[19]

3.2. Leyes nacionales

3.2.1. Suecia

Suecia fue el primer estado nacional que sancionó una ley de Protección de datos personales ("*Datalag*") el 11 de mayo de 1973.[20]

---

[18]Texto en inglés: "Article 26 [Family, Privacy] Everyone shall have the right to inviolability of family life and privacy. State and local government authorities and their officials may not interfere with any person's family life or privacy, except in such cases and procedures as determined by law for the protection of health or public morals, public order, the rights and liberties of other persons, the prevention of a crime or the apprehension of a criminal.", http://www.oefre.unibe.ch/law/icl/en__indx.html/

[19] Texto en inglés: "Article 44 [Right to Information] (1) Everyone shall have the right to freely receive information circulated for general use. (2) At the request of Estonian citizens, and to the extent and in accordance with procedures determined by law, all state and local government authorities and their officials shall be obligated to provide information on their work, with the exception of information which is forbidden by law to be divulged, and information which is intended for internal use only. (3) Estonian citizens shall have the right to become acquainted with information about themselves held by state and local government authorities and in state and local government archives, in accordance with procedures determined by law. This right may be restricted by law in order to protect the rights and liberties of other persons, and the secrecy of children's ancestry, as well as to prevent a crime, or in the interests of apprehending a criminal or to clarify the truth for a court case. (4) Unless otherwise determined by law, the rights specified in Paragraphs (2) and (3) shall exist equally for Estonian citizens and citizens of other states and stateless persons who are present in Estonia."

[20] modificada luego parcialmente en 1979, en 1982 y en 1998 (para adaptarla a la Directiva 95/46).

Dicha norma introdujo la creación de un registro público específico obligando a registrar en el mismo los archivos electrónicos de datos personales, ya fueran éstos de carácter público o privado (artículo 1º). Estableció el requisito de otorgamiento de una licencia específica a quien pretendiera gestionar un registro de datos personales.[21]

En el caso de que los datos registrados fueran de los considerados sensibles, la ley exige una autorización expresa para su funcionamiento[22], del órgano encargado de la aplicación de la ley, denominado Inspección de Datos[23]. La ley previó asimismo la existencia de un responsable a los efectos de la habilitación de un banco de datos personal, tanto en el ámbito público como en el privado[24].

La relevancia de esta ley sueca radica en que, a semejanza suya, habrían sido adoptadas las leyes de protección de datos de Francia, Dinamarca, Noruega y Austria (todas de 1978), Luxemburgo (1979), Israel e Islandia (1981), Reino Unido (1984), la Isla de Man y Guernsey (1986) y en Jersey (1987).[25]

---

[21] La licencia consiste en la certificación otorgada por la autoridad de aplicación de la ley (art.2). Dicha certificación se extiende en forma automática una vez realizada la inscripción en el registro estatal creado al efecto (art.26).

[22] Esta autorización está sujeta al cumplimiento de ciertos requisitos tendientes a garantizar que no existen riesgos de invasión de la esfera privada de la persona registrada (arts.2 y 6.); que sólo puede concederse por motivos especiales (arts.3 y 4). No obstante, quedan exceptuados del requisito de autorización los registros llevados por servicios sanitarios, médicos o dentistas y los registros de sus miembros que lleven los sindicatos, organizaciones religiosas o de otro tipo (art.2).

[23] Arts.15 a 18. Tiene amplios poderes de supervisión. La ley prevé sanciones pecuniarias y de privación de libertad para casos de incumplimiento de las disposiciones legales (art.20 y 21) y la obligación de resarcimiento a cargo del responsable del registro cuando se hubiere causado un daño a la persona registrada (art.22).

[24] Arts.7 a 14. El responsable del registro está obligado a adoptar las medidas necesarias para impedir la pérdida, destrucción o acceso no autorizado de los datos y su ulterior cancelación cuando no se correspondan con los fines para los cuales fueron registrados. Asimismo, está obligado a conceder el derecho de acceso a la persona registrada y proceder a las modificaciones o rectificaciones que fuesen solicitadas por ella. Frosini, op.cit. supra, pág.77.

[25] Cfr. Dresner, Stewart H., "Panorama de la legislación europea sobe protección de datos personales". trad. de Ripoll Carulla, Santiago, en: “Informática y Derecho”, N° 6/7, Mérida, España: UNED - Centro Regional de Extremadura, 1994. p. 39, citado por Bazán, Víctor en

La ley fue modificada por ley del 1 de julio de 1982 (sobre recolección de datos), y hubo una adaptación normativa sueca a la Directiva 95/46/CE que se concretó por una ley sancionada el 16 de abril de 1998.[26]

3.2.2. Alemania

La Ley Federal de Alemania de 1977 (Federal Data Protection Law)[27] ordenó sus 47 artículos en 6 capítulos, aplicándose a los registros automáticos y manuales que procesen datos relativos a personas físicas, tanto en el sector público como en el privado (arts. 2 y 3).

Estableció el requisito del consentimiento del interesado previo a la registración del dato, así como la autorización legal para la autorización de un registro (art. 3).

Reguló el derecho al acceso por parte del individuo así como la obligación del responsable de adoptar las medidas de seguridad pertinentes (arts. 4 y 6). Impuso el deber de información o comunicación al ciudadano del registro de sus datos y como organismo de control estatuyó la figura del "Comisario o Delegado Federal para la protección de los datos personales".

El 15 de noviembre de 2006, la República Federal Alemana sancionó una nueva Ley Federal de Protección de datos[28], para adecuar la norma a la Directiva 95/46 CE. La autoridad de aplicación es el Comisionado Federal para la protección de

---

ob.cit. supra.

[26] Personuppgiftslagen, 29/04/1998. Su texto en inglés en: http://www.datainspektionen.se/in_english/personal_data.shtml/. Ver Bazán, Víctor, “La protección de datos personales y el derecho de autodeterminación informativa en perspectiva de Derecho comparado”, LLGran Cuyo, 2005 (junio), 453.

[27] Publicada en Bundesgesetzblatt, parte I, Nº 7 del 01/02/1977, p. 201. Sustituida en 1990 por la Federal Data Protection Act (su texto en inglés, puede consultarse en http://www.uaipit.com/multilingue/documentos.jsp?len=es/

[28] Bundesdatenschutzgesetz (BDSG) OJ EC No. L 281, p. 31 ff. Su texto en inglés y alemán puede consultarse en: http://www.bfdi.bund.de/cln_029/nn_946430/EN/DataProtectionActs/Artikel/Bundesdatenschutzgesetz-FederalDataProtectionAct,templateId=raw,property=publicationFile.pdf/Bundesdatenschutzgesetz-FederalDataProtectionAct.pdf/.

datos y la libertad de información.[29]

3.2.3. Francia

La Ley sobre "Informática, ficheros y libertades" sancionada el 6 de enero de 1978[30], fue la legislación específica que más impacto tuvo sobre los primeros estudios desarrollados en la Argentina en materia de protección de datos personales.

Esta ley creó la Comisión Nacional de Informática y Libertades (CNIL) que cumple funciones de autoridad de aplicación[31]. El artículo 1º de dicha ley estableció que “La informática debe estar al servicio de cada ciudadano. Su desarrollo debe desenvolverse en el marco de la cooperación internacional. No debe afectar la identidad humana ni los derechos humanos, ni la vida privada, ni las libertades individuales o públicas”.

Se aplica a los registros automatizados que contengan datos sobre personas

---

[29] Hay una versión del año 2002, que se publica en http://www.uaipit.com/files/documentos/pdf/0000004276_Federal%20Data%20Protection%20Act.pdf/

[30] Ley 78-17, B.O. République Française, 07/01/1978, p. 227/231. Su texto en francés: http://www.cnil.fr/index.php?id=301. También puede verse en http://www.legifrance.gouv.fr/ Basada en el proyecto Lecaunet, que fuera Ministro de Justicia de J. Chirac, que a su vez, se elaboró sobre el informe que elevaron los miembros de la Comisión sobre Informática y Libertades en 1975. Esta Comisión fue creada por el Presidente de la República en 1974. Modificada 29/04/2004, las reformas más significativas se centran en el tratamiento de las infracciones, las correspondientes a la protección de datos, la biometría, los servicios secretos y las sanciones pronunciadas por la Comisión Nacional de Informática y Libertades, autoridad de aplicación de la ley. La ley fue modificada en varias oportunidades: Loi n° 88-227 du 11 mars 1988 (Journal officiel du 12 mars 1988); Loi n° 92-1336 du 16 décembre 1992 (Journal officiel du 23 décembre 1992); Loi n° 94-548 du ler juillet 1994 (Journal officiel du 2 juillet 1994); Loi n° 99-641 du 27 juillet 1999, (Journal officiel du 28 juillet 1999); Loi n° 2000-321 du 12 avril 2000, (Journal officiel du 13 avril 2000).; Loi n° 2002-303 du 4 mars 2002, (Journal officiel du 5 Mars 2002); Loi n° 2003-239 du 18 mars 2003 (Journal officiel du 19 mars 2003); Loi n° 2004-801 du 6 août 2004 (Journal officiel du 7 août 2004); Loi n° 2006-64 du 23 janvier 2006 (Journal officiel du 24 janvier 2006).

[31] Esta Comisión, creada por el art.6, tiene potestad reglamentaria y funciones de supervisión e información al público. Es una autoridad administrativa independiente integrada por 16 miembros, entre los cuales están representantes del Parlamento, del Consejo de Estado, de la Corte de Casación y del Tribunal de Cuentas (art.8).

físicas, y es la Comisión Nacional de Informática y Libertades la que, entre otras funciones, autoriza la habilitación de los registros del sector público.

La ley reglamenta asimismo el denominado derecho de acceso, previéndose el acceso directo del individuo a los registros, con la salvedad o excepción de aquellos que no lo permitan por razones de defensa y seguridad del estado, a los cuales tendrán acceso por intermedio de la comisión.

La ley francesa, al igual que la ley federal alemana, previó sanciones de multa y prisión para quienes infringieran sus normas.

Las reformas más significativas del año 2004 se centraron en el tratamiento de las infracciones, las correspondientes a la protección de datos, la biometría, los servicios secretos y las sanciones pronunciadas por la Comisión Nacional de Informática y Libertades.[32]

3.2.4. Austria

La Ley Federal sobre Protección de Datos Informáticos de índole personal se sancionó el 18 de noviembre de 1978. Incorporó normas de jerarquía constitucional y otorgó a la protección de datos personales el carácter de derecho fundamental de la persona, fuera ésta física o jurídica.

Con relación a los bancos de datos personales de carácter público, la ley expresamente los autorizó a la registración de datos cuando existiese una norma que lo previera en forma expresa o ello le resultare indispensable para el cumplimiento de los fines legítimos de que se trate.

Las entidades privadas deben solicitar su inscripción en el Registro de Procesamiento de Datos, previa aprobación de la denominada Comisión de Protección

[32] Ley 2004-801del 06/08/2004. Además debe tenerse en cuenta, entre otras las siguientes normas: Decreto 2005-1309 del 20/10/2005, sobre Medidas generales de aplicación de la ley, modificada en 2004; Decreto 82-525 del 16/06/1982, sobre el ejercicio del derecho de acceso; Circular del 12/03/1993, sobre las modalidades de aplicación del derecho de acceso en el sector público y el Reglamento Interno de la CNIL del 23/05/2006.

de Datos.

La citada Comisión es un organismo independiente, con potestad reglamentaria y judicial, cuyas resoluciones no pueden ser anuladas por vía administrativa, y contra las que sólo procede un recurso ante el Tribunal en lo Contencioso Administrativo. Tiene a su cargo, entre otras funciones, el otorgamiento de autorización de Flujos de Datos Transfrontera.

La ley austríaca previó asimismo sanciones penales de distinto carácter para quienes violaren los preceptos por ella establecidos.

En el año 2000 Austria puso en vigencia una nueva ley de protección de datos, para adaptar su norma a la Directiva 95-46-CE.[33]

3.2.5. Dinamarca

Dos leyes de 1978 abordaron el tema de modo independiente, una orientada a la regulación de los bancos de datos en el ámbito del sector público y la otra a los gestionados por entes privados.[34]

En el año 2000 se aprobó una nueva legislación que reemplazó a estas leyes, para adecuarse a la Directiva 95-CE-46.[35]

3.2.6. Noruega

La Ley Nº 48 de 1978 estableció un sistema de licencias o autorizaciones previas aplicable a los registros, tanto automáticos como manuales, que contuvieran datos de personas físicas o jurídicas, pertenecieran éstas al sector público o privado.

---

[33] Datenschutzgesetz 2000 - DSG 2000, http://www.dsk.gv.at/indexe.htm/. Cf. Masciotra, ob.cit. supra, p. 57.

[34] Leyes de Registros de las Autoridades públicas de 08/06/1978: la concerniente al sector público nº 294 (PARA) y otra al sector privado nº 293 (PRA). Modificadas en 10/06/1987 y nuevamente en diciembre de 1994, con vigencia a partir de agosto de 1995. El 01/07/1996 entró en vigencia una ley sobre utilización de datos médicos, en la que se fijan las reglas que precisan cuando y como el empleador puede utilizar y recoger datos concernientes al trabajador.

[35] Ley Nº 429 del 31/05/2000, http://www.datatilsynet.dk/eng/index.html/

En el año 2000 esta norma también fue modificada para adecuarse a la Directiva 46-CE-95.[36]

3.2.7. Luxemburgo

La primera ley de protección de datos se sancionó en 1979[37]. Actualmente cuenta con una nueva norma desde el año 2002[38], adecuada a la Directiva 46-CE-95 y otra del año 2005 sobre comunicaciones electrónicas, que traspuso al derecho local la Directiva 2002-CE-58.[39]

3.2.8. Finlandia

La primera ley de protección de datos entró en vigencia en 1988[40]; fue modificada en 1999[41] y también en el año 2000, para adecuarse a la Directiva 46-CE-95.[42]

3.2.9. Islandia

La ley sancionada en 1981 fue sustituida en el año 2000 por la ley 77, para adecuarse a la Directiva 46-CE-95, y fue objeto de diversas modificaciones hasta el año 2003.[43]

---

[36] Noruega, Ley Nº 31, del 14/04/2000, relativa al procesamiento de datos personales (Personal Data Act), http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/lov-20000414-031-eng.pdf/

[37] ver Masciotra, ob.cit. supra, p.57.

[38] Ley del 02/08/2002, « Protection des personnes à l'égard du traitement des données à caractère personnel », http://www.legilux.public.lu/leg/a/archives/2002/0911308/0911308.pdf#page=2

[39] Ley del 30/05/2005 « relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle », http://www.legilux.public.lu/leg/a/archives/2005/0730706/index.html/

[40] Ley 471 de 1987. Cf. Masciotra, ob.cit. supra, p.62 y Padilla, ob.cit. supra.

[41] Ley 523/1999, http://www.tietosuoja.fi/uploads/hopxtvf.HTM/

[42] Ley de reformas Nº 986/2000, entró en vigencia el 01/12/2000. http://www.tietosuoja.fi/uploads/hopxtvf.HTM/

[43] "Act on the Protection of Privacy as regards the Processing of Personal Data, Nº 77/2000 del

3.2.10. Gran Bretaña

La primer ley de protección de datos personales fue de 1984, mediante la cual se reguló el uso de información tratada automatizadamente referida a personas físicas, trasladando así el Convenio de Estrasburgo a su legislación interna.

Se destacan los ocho principios consagrados en esta ley[44], que establecen: "1) La información contenida en el dato personal deberá ser obtenida y deberá ser procesada en forma justa de acuerdo a la ley; 2) Dicha información personal deberá ser poseída sólo por uno o más propósitos específicos y que estén dentro de la ley; 3) Dicha información personal no podrá se usada o revelada en cualquier forma que no sea la ya especificada; 4) Dicha información personal deberá, para ese propósito, ser adecuada, relevante y NO excesiva en relación a dicho propósito o propósitos; 5) Dicha información personal deberá ser precisa y donde sea necesario actualizarla; 6) La información personal que se posea para cualquier propósito, o propósitos no deberá ser conservada por más tiempo del necesario para cumplir dicho propósito o propósitos; 7) A un individuo se le debe permitir: a) En períodos razonables y sin demora indebida o gastos: (I) Ser informado de los datos que el operador posea en relación a su persona. (II) Acceder a cualquier información poseídas por el usuario u operador y, b) donde sea necesario o apropiado, hacer corregir o borrar dichos datos o información. El principio octavo, referido también a la Información personal poseída por usuarios respectos de servicios provistos por personas a cargo de oficinas de computadora, señala: 8) Medidas apropiadas de seguridad deberán tomarse contra el acceso no autorizado, o alteración revelación o destrucción de información personal y contra la pérdida accidental o destrucción de la información personal."

En 1998 el Reino Unido aprobó una nueva ley, que adaptó la legislación a la

---

10/05/2000, reformada por las leyes Nº 90/2001, 30/2002, 81/2002 y 46/2003, entró en vigencia el 01/01/2001. La ley Nº 90/2001 comenzó a regir el 15/06/2001, la Nº 30/2002, el 16/04/2002, la Nº 81/2002, el 17/05/2002 y la Nº 46/2003, el 14/03/2003, http://www.personuvernd.is/information-in-english/greinar//nr/438/

[44] cuya traducción agradecemos a Uicich, Rodolfo Daniel, en "Los bancos de datos y el Derecho a la intimidad", Editorial Ad Hoc, Buenos Aires, 1999, p.124; ver adde: Masciotra, ob.cit. supra, p.58.

Directiva 46-CE-95[45] y en el año 2003 sancionó una ley sobre privacidad en las comunicaciones electrónicas.[46]

3.2.11. Portugal

Aunque fue el primer país europeo que reconoció constitucionalmente la necesidad de proteger a las personas frente a los riesgos informáticos, como hemos señalado precedentemente, pasaron quince años para que aquellas disposiciones fueran desarrolladas legislativamente. Recién en abril de 1991 se dictó la ley 10 de "Protección de datos personales frente a la informática"[47]. Esta norma amplió los parámetros tuitivos de la Constitución; estableciendo que el uso de la informática debe procurarse de forma transparente y con estricto respeto por la reserva de la vida privada y familiar y de los derechos, libertades y garantías fundamentales del ciudadano; previó la creación de la autoridad de aplicación (Comisión Nacional de Protección de Datos Personales Informatizados); determinó que ninguna decisión judicial, administrativa o disciplinaria puede tomarse sobre la exclusiva base del perfil de personalidad del titular del registro del banco de datos; y, en síntesis, reprodujo los principios consagrados por el mencionado Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa.[48]

Esta norma fue modificada por la Ley de Protección de Datos Personales Nº 67/98 de 26 de octubre, que ha transpuesto la Directiva 95/46/CE al derecho interno [49]. En el sector de telecomunicaciones, la Ley Nº 41 del 18 de agosto de 2004, incorporó la Directiva 2000-CE-58[50]. El Decreto-Ley 7/2004, ha transpuesto la Directiva del Comercio Electrónico en el artículo 13 de la Directiva de las Comunicaciones

---

[45] http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm/
[46] The Privacy and Electronic Communications (EC Directive) Regulations 2003, http://www.opsi.gov.uk/si/si2003/20032426.htm/
[47] http://www.cnpd.pt/bin/legis/nacional/lei_1091.htm/
[48] Bazán, Víctor, "La protección de datos personales y el derecho de autodeterminación informativa en perspectiva de Derecho comparado", LLGran Cuyo, 2005 (junio), 453.
[49] http://www.cnpd.pt/bin/legis/nacional/lei_6798.htm/
[50] http://www.cnpd.pt/bin/legis/juris/decisoes/Lei41-2004.pdf/

Electrónicas[51]. Hay legislación específica sobre tratamiento de datos policiales de Schengen, Europol y Eurojust, que en concreto atribuyen a la Autoridad de Protección de Datos la competencia de instancia nacional de control[52]. Hay otras normas, tanto en Código Penal, como en legislación dispersa, que reglamentan materias relativas a protección de datos[53].

3.2.12. Hungría

En 1992 sancionó la ley LXIII de Protección de Datos Personales y de Acceso público a la información de interés público[54], que ha sufrido diversas modificaciones. Establece que el responsable del tratamiento de datos debe resarcir los daños ocasionados al titular de los datos cuando se violen las prescripciones de la ley, salvo fuerza mayor o culpa de la víctima.[55]

3.2.13. Bélgica

En la década de los ochenta sancionó varias leyes vinculadas con la protección de datos[56] y en 1991 dictó una ley de Protección de datos[57], sustituida en 1992[58]. En

---

[51] http://www.cnpd.pt/bin/legis/nacional/DL7.2004.pdf/
[52] Ley 68 de octubre de 1998, http://www.cnpd.pt/bin/legis/nacional/lei_6898.htm/
[53] http://www.cnpd.pt/bin/legis/leis_nacional.htm/
[54] http://abiweb.obh.hu/dpc/index.htm/
[55] Art. 18: “The data controller shall be liable for any damage suffered by data subjects as a result of an unlawful processing of their data or as a result of an infringement of the technical requirements of data protection. The data controller shall also be liable for any damage suffered by the data subject resulting from the actions of a technical data processor. The data controller shall be exempted from liability if he proves that the damage was the result of force majeure beyond the sphere of data processing. (2) No compensation shall be paid for the part of damage suffered by the damaged person as a result of his intentional or grossly negligent conduct.”. Cf. Masciotra, ob.cit. supra, p.62, citando a Guahnon, Silvia y Somer, Marcela, “Hábeas data: procedimiento aplicable. ¿Derecho a una tutela efectiva y temprana versus Derecho de defensa en juicio?”, Revista de Derecho Procesal Nº 5, Rubinzal Culzone, 2000, p.199.
[56] Regulación sectorial relativa a funcionarios públicos de 1982; Creación de la Comisión Consultiva para la Protección de la Vida Privada en 1982; Regulación sectorial relativa al censo de 1983; Creación del Registro Nacional de Personas Físicas en 1983; Regulación sectorial relativa al crédito de 1985; Regulación sectorial relativa a la seguridad social de l.990.
[57] 08/03/1991.
[58] Ley general de tutela de datos personales de 08/12/1992, que sustituye a la Ley

1994 aprobó la ley del 30 de junio relativa a la protección de la vida privada contra las escuchas y el registro de comunicaciones y telecomunicaciones, que comenzó a regir el 1 de febrero de 1995. La ley de 1992 sufrió diversas modificaciones y se ha adaptado a la Directiva 46-CE-95[59].

Hay que mencionar también la Ley de 1991 relativa al crédito[60] y en el año 2001 la relativa a las centrales de crédito a los particulares.[61]

3.2.14. España

Este país, que también fue pionero al incorporar el tema en su Constitución de 1978, recién en el año 1992 aprobó la Ley N° 5/92 denominada Ley Orgánica de Regulación del Tratamiento de Datos (LORTAD)[62].

Esta norma fue luego sustituida por la Ley 15/99 (LOPDP)[63], para adaptar la Directiva 46-CE-95 al derecho español. Ambas leyes constituyen el molde en el que se basó la actual ley argentina 25.326, por lo que más adelante haremos referencias más específicas a su articulado.

La Ley 34/2000 de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI)[64] y la Ley 32/2003 General de Telecomunicaciones[65] tienen puntos

---

8.3.1991

[59] puede consultarse el texto vigente a enero de 2006 en http://www.privacycommission.be/textes_normatifs.htm/ (en francés y holandés).

[60] Ley del 08/06/1991, http://www.privacycommission.be/textes_normatifs/12_06_1991.pdf/

[61] Ley del 10/08/2001, que reglamenta una materia del art.78 de la Constitución Belga, publicada en Monitor Belga (Moniteur Belge) del 25/09/2001, http://www.privacycommission.be/textes_normatifs/MB-BS25-9-01.pdf/

[62] Ley Orgánica 5/1992, 29/10/1992 (LORTAD - España), de Regulación del Tratamiento Automatizado de los Datos de carácter Personal (BOE, 31/10/1992), que hemos reproducido en Altmark, Daniel R. y Molina Quiroga, Eduardo, "Régimen Jurídico de los Bancos de Datos" (Informática y Derecho, Vol. 6, Editorial De Palma, 1998) p.347 y ss.

[63] Ley orgánica 15/1999, de 13/12!1999, de Protección de datos de carácter personal, según el cambio de denominación por artículo 79 Ley 62/2003, de 30/11/2003, https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Ley%2015_99.pdf/

[64] https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Ley_34-

de contacto con las normas antes citadas.

También debe tenerse en cuenta el Real Decreto 94/1999 de 11 de junio, por el que se aprobó el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal[66], el 428 de 1993 por el que se aprobó el estatuto de la Agencia Española de Protección de datos[67].

La Agencia Española de Protección de Datos ha dictado varias "Instrucciones", tales como la 1/1995 relativa a los servicios de información sobre solvencia patrimonial y crédito[68], a la que volveremos a referirnos; la 2/1995, sobre sobre "Medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal"[69]; y más recientemente, la 1/2006, del 8-11-2006 sobre "tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras[70], entre muchas otras.

Del mismo modo, tienen gran valor para nuestra materia las sentencias del Tribunal Constitucional Nº 290 del 30 de noviembre de 2000 sobre la

---

2002%20_LSSI_definitiva_1.pdf/

[65] https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/LGT.pdf/

[66] https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/A.8%29%20Real%20Decreto%20994-1999.pdf/

[67] https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/A.5%29%20Real%20Decreto%20428-1993.pdf/. Este decreto fue modificado por el Real Decreto 156/1996, https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/A.6%20Real%20Decreto%20156-1996.pdf/

[68] https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/A.12%29%20Instucci%F3n%201-1995%20de%201%20de%20marzo%20de%20la%20APD%20.pdf/

[69] https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/A.13%29%20Instrucci%F3n%202-1995%20de%204%20de%20mayo%20de%20la%20APD%20sobre%20garant%EDa%20de%20los%20datos%20personales.pdf/

[70]https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Instruccion_1_2006_videovigilancia.pdf/

inconstitucionalidad de varios artículos de la derogada LORTAD[71], en el que se destaca el voto particular del magistrado Manuel Jiménez de Parga y Cabrera, afirmando la existencia de un nuevo derecho que llama "libertad informática", y la Nº 292 de la misma fecha, pero referida a planteos de inconstitucionalidad de la ley 15/1999[72], en la que se mencionó concretamente a la autodeterminación informativa como el derecho fundamental que consagra el art. 18.4 de la Constitución española.

Más recientemente, se dictó el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobó el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal.[73]

3.2.15. Italia

Se cita como antecedente la ley del 20 de mayo de 1970 Nº 30 "Estatuto de los trabajadores", cuyo artículo 4 prohíbió el uso "de instalaciones audiovisuales y de otros dispositivos para finalidades de control a distancia de la actividad de los trabajadores"; y el artículo 8 que prohíbió "efectuar indagaciones sobre las opiniones políticas, religiosas o sindicales del trabajador, así como sobre hechos no relevantes para los fines de la valoración de la aptitud profesional del trabajador".[74] Se suele citar también la ley 121 del 1 de abril de 1981 sobre nuevo ordenamiento de la Administración de la seguridad social, referida a los bancos de datos del Ministerio del Interior[75].

La Ley 675/96 de 31 de diciembre de 1996 sobre protección de datos personales[76] introdujo los lineamientos de la Directiva 46-CE-95. La Ley 676 del

---

[71] http://www.tribunalconstitucional.es/STC2000/STC2000-290.htm/
[72] En este caso la demanda fue contra los artículos 21.1 y 24.1 y 2 de la citada ley 15/1999, http://www.tribunalconstitucional.es/STC2000/STC2000-292.htm/
[73] BOE Nº 17, 19/01/2008, http://www.boe.es/aeboe/consultas/bases_datos/doc.php?coleccion=iberlex&id=2008/00979/
[74] http://informatica-juridica.com/legislacion/italia.asp/
[75] ídem nota anterior.
[76] "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali", publicada en el Boletín Oficial, 08/01/1997 y que entró en vigor el 08/05/1997. Texto consolidado al 28/12/2001 en http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FLa+legge+n.+675/

mismo año autorizó al Gobierno a reglamentar la citada ley 675.

Actualmente existe el denominado “Código en materia de protección de los datos personales”, aprobado por el decreto legislativo N° 196 del 30 de junio de 2003, con vigencia a partir del 27 de febrero de 2004, consolidado con la ley del 26 de febrero de 2004[77].

3.2.16 Otras legislaciones

Sin agotar con esta enumeración la totalidad de leyes europeas, podemos mencionar que Grecia aprobó su ley 2.472 de Protección de Datos en 1997[78].

Irlanda, en 1988 sancionó su Ley de Protección de Datos[79], en aplicación del Convenio de Estrasburgo de 1981 y en el año 2003 la reformó para adaptarla a la Directiva 46-CE-95[80].

Polonia, cuya Constitución ya hemos mencionado, aprobó su Ley de Protección de Datos Personales en agosto de 1997.[81] En el año 2002 se creó un organismo responsable de la protección de los datos personales, habiéndose modificado la Ley sobre la protección de los datos personales en agosto de 2001, lo que ha provocado la aproximación de su legislación al acervo comunitario. El Convenio del Consejo de Europa de 1981 para la protección de las personas respecto del tratamiento automático de los datos personales se ratificó en mayo de 2002 y entró en vigor en septiembre de 2002.

La República Checa sancionó su ley de Protección de Datos Personales en el

---

[77] http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana%2FII+Codice+in+materia+di+protezione+dei+dati+personali/

[78] http://www.dpa.gr/Documents/Eng/Law%202472-97-en-amended.doc/ (en inglés).

[79] Ley Nº 25 de Protección de datos del 13/07/1988, http://www.dataprotection.ie/viewdoc.asp?Docid=64&Catid=47&StartDate=1+January+2006&m=l/

[80] http://www.dataprotection.ie/viewdoc.asp?Docid=68&Catid=47&StartDate=1+January+2006&m=l/

[81] http://www.giodo.gov.pl/data/filemanager_en/61.doc/, cuya última reforma sería de 2006

año 2000[82]. La Bailía de Guersney, en el año 2001[83]. Chipre aprobó su ley en el año 2001, reformada en 2003 y una norma sobre comunicaciones electrónicas en 2004.[84] Bulgaria, aprueba su primera ley en el año 2002, pero el texto vigente data de 2005.[85]

En la actualidad, todos los países europeos cuentan con normas similares.

3.3. Síntesis

Los países europeos, como se ha visto, han adaptado sus legislaciones internas a la Directiva del Parlamento Europeo y el Consejo de Ministros de la Unión Europea, en el marco de la Comunidad Europea de 1995.

Las principales coincidencias las encontramos en el reconocimiento de un conjunto de principios y reglas específicas para el tratamiento de los datos de carácter personal, enunciados en el Convenio de Estrasburgo de 1981, y que con mayor o menor grado de detalle han sido incorporados a las normas nacionales.

En una breve reseña de estos principios mencionamos la existencia de una autoridad ú órgano de control especial, con diverso rango y características según los países, pero con la exigencia de independencia del órgano ejecutivo; los principios de licitud, calidad, consentimiento, conocimiento o información y participación, instrumentados mediante los derechos de acceso, actualización, rectificación y supresión, que comentaremos en particular en el capítulo 6.

Sin perjuicio de ello, cabe aclarar que no todas las leyes se ocupan particularmente de los informes crediticios, situación que ha preocupado más a los países latinoamericanos, y desde otra perspectiva a Estados Unidos.

Finalmente, la normativa comunitaria europea procura armonizar la protección de la intimidad y otros derechos personales, con la particular evolución hacia la

---

[82] http://www.uaipit.com/multilingue/documentosImpr.jsp/
[83] http://www.dataprotection.gov.gg/
[84] sus textos en inglés en: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument/
[85] http://www.cpdp.bg/en_zakon.html/

autodeterminación informativa que hemos señalado, y la libre circulación de los datos personales y las mercaderías. Desde este punto de vista, no siempre la conciliación de ambos objetivos se ha inclinado a favor de la protección de datos.

La aceptación de las exigencias de Estados Unidos luego de los atentados a las Torres Gemelas se produjo, de algún modo, con la Directiva 2006/24/CE de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones[86], que modificó la Directiva 2002/58/CE (relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas), tema que excede los alcances de este trabajo, pero es válido aclarar que se estableció, en esta última directiva, que "se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado (pero) no se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas".

[86] DO 105/54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:ES:PDF/

Capítulo 4. Derecho comparado. Legislación de Estados Unidos

Sumario: Leyes federales, La ley sobre Informes de crédito. Ley de protección de la vida privada. Freedom of Information Act. Consumer Credit Reporting Reform Act. Fair Credit Billing Act (FCBA). Equal Credit Opportunity Act (ECOA). Family Education Rights Act (FERPA). Electronic Fund Transfer Act (EFTA). Privacy Protection Act 1980. Counterfeit Access Device and Computer Fraud and Abuse Act (CFAA). Cable Communications Policy Act (CCPA). Electronic Communication Privacy Act (ECPA). Computer Security Act (CSA). Telephone Consumer Protection Act (TCPA). Cable Television Consumer Protection and Competition Act (CTCPCA). Driver´s Privacy Protection Act (DPPA). Legislación estatal. Acuerdo de "Puerto Seguro". Situación actual

4.1. Leyes federales

La normativa sobre tratamiento de datos personales en Estados Unidos se caracteriza por ser sectorial, es decir que no existe una norma de aplicación general al estilo de las promovidas por la Unión Europea, que se han analizado en los dos capítulos anteriores. Por el contrario, hay tantas regulaciones legales como contextos justifiquen su existencia, con la especificidad que sea requerida por la naturaleza de los datos, las finalidades de su tratamiento o de la entidad titular de la base.

Algunas leyes regulan la protección de los datos en contextos específicos tales como los servicios postales, las comunicaciones electrónicas, los datos médicos, de crédito, los servicios financieros, el uso de grabaciones magnetoscópicas, etc.. Otras, en cambio, contienen preceptos que inciden en la protección de datos personales en determinado ámbito: ley federal de Procedimiento Administrativo, ley de Comunicación por Cable, ley de Reforma Tributaria, ley de Interferencias de las Telecomunicaciones, entre otras[1].

[1] Conf. entre otros: Masciotra, ob.cit. supra, p.63; Lucas Murillo de la Cueva, Pablo, "El derecho a la autodeterminación informativa", p. 125 y sigtes. y Bazán, Víctor, ob.cit. supra; Puente de la Mora, ob.cit, supra; Palazzi, Pablo A.,"Habeas data y protección de datos en Latinoamérica", http://comunidad.derecho.org/congreso/ponencia20.html/

Además, casi todos los Estados cuentan con leyes de alcance sectorial.

4.1.1. La ley sobre Informes de crédito

La *Fair Credit Reporting Act* (FCRA) fue sancionada el 26 de octubre de 1970[2], y podemos considerarla el primer antecedente normativo en la materia.

Aunque esta ley no menciona en ningún momento los sistemas de tratamiento automatizado de datos, sus previsiones sobre la recogida, conservación y transmisión a terceros de informes sobre la solvencia personal, profesional o económica de las personas y los derechos que a los afectados reconoce para su protección, inauguran una técnica que, posteriormente, se aplicará también a la tutela de las informaciones personales introducidas y tratadas en computadoras.

Esta ley promueve que las agencias de informes de consumidor, incluyendo las agencias de crédito (*credit bureaus*) y las especializadas (como agencias que brindan información sobre historial de firma de cheques, expedientes médicos e historial de alquiler) operen observando que la información sea exacta, justa y respete la privacidad[3].

El sistema exige que cuando se utilice un informe de crédito u otro tipo de informe de consumidor para denegar una solicitud de crédito, seguro o empleo, o para

---

[2] Corresponde a la Sección (§) 1681, del Título 15, capítulo 41, subcapítulo III del Código de Estados Unidos (U.S. Code), subsecciones o parágrafos 601 a 625, que podríamos traducir como “Ley de información (o divulgación) justa (o adecuada) del crédito”. Su primera consideración dice más o menos lo siguiente “el sistema de actividades bancarias es dependiente sobre la divulgación justa y exacta del crédito. Los informes de crédito inexactos deterioran directamente la eficacia del sistema de actividades bancarias, y los métodos injustos de la divulgación de crédito minan la confianza pública que es esencial para el funcionamiento continuado del sistema de actividades bancarias”. Ha sufrido diversas modificaciones desde su sanción original. Puede consultarse su texto actualizado y otras normas relacionadas en http://www4.law.cornell.edu/uscode/15/1681.html/

[3] En los sitios de protección al consumidor se la presenta como la norma que “controla la manera en que las agencias crediticias mantienen sus antecedentes de crédito (la manera en que usted paga sus cuentas) y cómo los prestamistas los usan”, vgr.: La Comisión Federal de Comercio (FTC) mantiene un sitio en Internet, en español, donde se brinda información y asesoramiento a los consumidores http://www.ftc.gov/credit/espanol_loans.htm/

emprender otra acción contra el concernido, se le debe informar incluyendo el nombre, dirección y teléfono de la agencia que proporcionó esa información.

El consumidor tiene derecho a solicitar y obtener toda la información que sobre él exista en los archivos de una "agencia de informe del consumidor", o agencias de información sobre consumidores previa identificación, que puede incluir su número de Seguro Social. En muchos casos, la divulgación de esta información es gratuita[4].

Las puntuaciones de crédito son resúmenes numéricos sobre la calificación del consumidor basadas en información de las agencias de crédito. Éste puede solicitar una puntuación de crédito de agencias de informe del consumidor que crean puntuaciones o distribuyen las puntuaciones utilizadas en préstamos de bienes raíces residenciales, con cargo, pero en algunas transacciones hipotecarias, el prestamista brinda gratuitamente esta información.

El consumidor tiene derecho, si cree que existe información incompleta o inexacta, a que la agencia de informe del consumidor, investigue la presentación, salvo cuando se la considere frívola o intrascendente.

La información inexacta, incompleta o no verificable debe ser retirada o corregida, dentro de treinta (30) días, sin perjuicio de la facultad de la agencia de informe del consumidor para seguir reportando información, si ha verificado su exactitud.

Las agencias de informe del consumidor no pueden reportar información negativa que haya ocurrido hace más de siete (7) años, ni quiebras ocurridas hace más de diez (10) años.

---

[4] Tiene derecho a una divulgación gratuita si es demandado debido a información consignada en un informe de crédito; o cuando es víctima de un robo de identidad y se coloca una alerta de fraude en su expediente; o cuando su expediente contiene información no exacta como resultado de fraude; también cuando el consumidor recibe asistencia pública; o no está empleado pero prevé solicitar empleo en 60 días. Asimismo, para septiembre de 2005, todos los consumidores tendrán derecho a una divulgación cada 12 meses si así lo solicitan a cada agencia de crédito nacional y de las agencias nacionales de informe del consumidor especializadas.

Una agencia de informe del consumidor puede proporcionar información solamente a personas que realmente la necesiten, por ejemplo, para considerar una solicitud de crédito o de seguro, empleo, locación de vivienda u otro negocio. La *FCRA* especifica quiénes son las personas que tienen una necesidad válida de acceso.

No se puede dar información al empleador, o a un posible empleador, sin consentimiento escrito previo otorgado por el consumidor al empleador.[5]

Las ofertas "preevaluadas" de crédito y seguro deben incluir un número de teléfono sin cargo al que puede llamar cuando una persona desea eliminar su nombre y dirección de las listas en las que se basan estas ofertas.[6]

Se puede accionar judicialmente en caso de infracción a la *FCRA* por parte de una agencia de informe del consumidor o, en algunos casos, de un usuario de informes de consumidor o proveedor de información a una agencia de informe del consumidor.

Las víctimas de robo de identidad y el personal militar en actividad tienen derechos adicionales.

4.1. 2. Ley de protección de la vida privada

A partir del escándalo de *Watergate*, ante el temor sobre el uso que el gobierno federal podría hacer de los ordenadores y sistemas informatizados y a fin de proteger a los ciudadanos de una posible violación de su privacidad por parte de aquél, el Congreso sancionó el 31 de diciembre de 1974 la Ley de Privacidad o *Privacy Act*.[7]

La *Privacy Act* de 1974[8], tiene por objetivo proteger la privacidad de los individuos identificados en sistemas de información llevados por entes y órganos

---

[5] El consentimiento escrito generalmente no es requerido en la industria de camiones
[6] Puede optar por no figurar en las listas de las agencias de crédito llamando al 1-888-5-OPTOUT (1-888-567-8888).
[7] Conf. Masciotra, ob.cit.supra, especialmente nota 90.
[8] Public Law 93-579, (93rd Congress, S. 3418) de 31/12/1974 (U.S. Code, cap 5,552a) llamada Privacy Act of 1974, modificada varias veces, por última vez en 1988 (Computer Matching Act), http://www.usdoj.gov/oip/privstat.htm/

federales. En su exposición de motivos se menciona que "... el creciente uso de ordenadores y de una tecnología compleja de la información si bien es esencial para el eficiente funcionamiento de las Administraciones Públicas, ha aumentado grandemente el detrimento que para la privacidad individual puede derivarse de cualquier captación, conservación, uso y difusión de información personal".

Dicha normativa autoriza por primera vez a las personas a conocer información sobre sí mismas contenidas en los archivos de las agencias federales y a impugnar las mismas, corregirlas o enmendarlas.

Sus disposiciones contienen las siguientes prerrogativas: autorizar que un ciudadano tenga acceso a la información sobre su persona que aparezca en los archivos de una agencia federal y a corregirla o enmendar esa información; impedir que una agencia que posea datos sobre una persona los ponga a disposición de otra dependencia sin el consentimiento de dicha persona; exigir que las agencias federales tengan en sus archivos aquellos datos que sean necesarios, legales, precisos y actualizados, y divulgar la existencia de todos los bancos de datos y archivos que contienen información sobre los ciudadanos; prohibir que las agencias conserven datos relativos al ejercicio por un individuo de su derecho a acogerse a la Primera Enmienda, a no ser que exista una autorización legal, que la persona interesada lo autorice o se trate de un caso que tenga que ver con actividades relacionado con el cumplimiento de la ley; autorizar que cualquier persona pueda tener acceso a un interdicto con vista a corregir o enmendar un dato contenido en los archivos de una agencia, y autorizar a que dicha persona sea recompensada por los daños sufridos a consecuencia de un acto de negligencia intencional cometido por una agencia. Prohíbe que las agencias vendan o alquilen datos como el nombre o la dirección de un individuo para incluirlos en listados postales.[9]

Se exceptúan de su divulgación varios archivos como los de la Agencia Central de Inteligencia (CIA), los archivos de las agencias de cumplimiento de la ley (agencias policiales o de seguridad, como el FBI), o los archivos del Servicio Secreto. También escapan a la regla las informaciones estadísticas, el nombre de las personas que

[9] cf. Masciotra, ob.cit. supra.

suministran informaciones usadas para determinar si una persona cumple con los requisitos para trabajar para el gobierno federal; materiales de prueba federales y archivos históricos del Archivo Nacional.

Alcanza al sector privado, cuando se encuentra vinculado contractualmente al público para el tratamiento de datos por su encargo, mediante la regulación de la captación, conservación, uso y difusión de información por éstos, prescindiendo del soporte en que se contiene, de modo que la ley resulta aplicable sea que las operaciones de tratamiento se realicen por medios informáticos o manuales.

La ley asegura que la revelación de los datos por el órgano de la Administración Federal podrá tener lugar sólo mediando petición o consentimiento del individuo a quien conciernen, salvo excepciones fundadas en necesidad de orden público[10].

Se reconoce al titular derecho de acceso, que incluye el detalle de las revelaciones del registro[11].

Asimismo, el órgano debe asegurar el acceso del individuo a los registros que le conciernen, así como una copia de ellos y permitirle solicitar la modificación de ellos, en su caso. Igualmente, el individuo concernido en el registro puede pedir la revisión administrativa de la negativa de rectificación y se le debe asesorar sobre las disposiciones aplicables a la revisión judicial de tal decisión.

---

[10] Se exceptúa requerir el consentimiento cuando la difusión responda a los fines para los cuales se recogió la información; o cuando se trate de información con destino a los tribunales, el congreso, los archivos nacionales, servicios de estadística o relativos a infracciones de tránsito.

[11] El derecho de acceso tiene limitaciones en el caso de los registros llevados por la CIA, el FBI, los servicios de inmigraciones y los registros llevados en razón de la lucha contra el tráfico de drogas. Cons. también Bazán, Víctor, “La protección de datos personales y el derecho de autodeterminación informativa en perspectiva de Derecho comparado”, LL Gran Cuyo, 2005-junio, 453.

4.1.3. Freedom of Information Act

Esta ley sancionada en 1966[12], también conocida como *FOI Act* o *FOIA*, establece cierto control sobre la información personal que colectan las agencias federales y como la usan. La ley garantiza tres derechos primarios: a) el derecho de cada individuo a ver sus propios documentos, sujetos a las excepciones revistas en la ley; b) el derecho del individuo a corregir su documento, si el registro es incorrecto, irrelevante, inoportuno o incompleto; y c) el derecho a demandar al gobierno por violaciones a la ley, incluyendo aquellos casos en que el gobierno permite a otros ver un documento personal, excepto si esta específicamente permitido por la ley.

Esta ley es un estatuto que establece el proceso por el cual todo individuo puede solicitar acceso a registros o información de las agencias federales. Las agencias federales, como la Comisión para la Igualdad de Oportunidades en el Empleo, están obligadas a divulgar sus archivos si han recibido una solicitud por escrito para la revisión de los mismos, salvo cuando los documentos solicitados estén protegidos por una de las nueve excepciones y tres exclusiones contenidas en la Ley FOIA. La norma no se aplica a los registros en poder del Congreso, los tribunales o gobiernos estatales y locales. Cualquier solicitud para revisar registros en poder de los gobiernos estatales y locales debe ser dirigida directamente a las agencias de gobierno estatal o local apropiadas[13].

4.1.4. Consumer Credit Reporting Reform Act

La ley de Reforma de los Informes de Crédito de Consumidores de 1996 modifica la *Fair Credit Reporting Act* de 1970 (*FCRA*). Mejora del proceso de notificación y reconoce a los sujetos el derecho de acceso a sus informes de crédito. También impone nuevas restricciones a los revendedores de informes de crédito de consumo. Los consumidores pueden obtener la indemnización de los daños y perjuicios, incluidas las costas.

---

[12] U.S. Code, Título V, arts. 552 y sigts., modificada en 2002, http://www.usdoj.gov/oip/foiastat.htm/
[13] http://www.eeoc.gov/es/foia/index.html

4.1.5. La Fair Credit Billing Act (FCBA)

Esta ley se refiere a la facturación de las transacciones de crédito renovable[14] (open end, en inglés), tales como tarjetas de crédito y cuentas de cargo renovables o rotatorias - como por ejemplo las cuentas de crédito de las tiendas por departamento, excluyéndose los contratos de ventas a plazos y prevé procedimientos de resolución de disputas para los "errores de facturación"[15].

Mientras la factura se encuentre en disputa, el acreedor no puede amenazar la calificación de crédito ni reportarlo como moroso al consumidor. No obstante, el acreedor puede informar que se está impugnando o cuestionando su factura.

4.1.6. Equal Credit Opportunity Act (ECOA)

La ley de acceso equitativo al crédito[16], prohíbe la discriminación crediticia por razones de sexo, raza, estado civil, religión, origen nacional, edad, o recepción de asistencia pública. Los acreedores pueden solicitar esta información (excepto religión) en ciertos casos, pero no pueden utilizarla para discriminar al decidir si otorgarle o no el crédito.

La *ECOA* protege a los consumidores que tratan con compañías que extienden créditos en forma regular, incluyendo bancos, pequeñas compañías financieras y de préstamo, tiendas minoristas y por departamentos, compañías de tarjetas de crédito, y cooperativas de crédito. Todos los que participan en la decisión de otorgar un crédito, incluyendo agentes de bienes raíces que arreglan la financiación, deben obedecer

---

[14] Public Law 93-495, 28/10/1974, 93rd Congreso, H.R.11221, http://www.ftc.gov/os/statutes/fcb/fcb.pdf/

[15] Estos errores pueden obedecer por ejemplo a: cargos no autorizados. La ley federal limita su responsabilidad por cargos no autorizados a un monto de $50; cargos con fecha o monto erróneo; cargos por bienes y servicios no aceptados o que no fueron entregados o prestados tal como acordado; errores de cálculo; falta de registro de pagos u otros créditos sobre una cuenta, como por ejemplo las devoluciones; falta de envío de facturas al domicilio; cargos para los cuales el consumidor solicitó una explicación o prueba de compra por escrito junto con un error reclamado o un pedido de explicación.

[16] Título 15, Capítulo 41, Subcapítulo IV, US Code 1691, http://www.usdoj.gov/crt/housing/documents/ecoafulltext_5-1-06.htm/

esta ley. Las empresas o negocios que solicitan el crédito también están protegidas por esta ley.

Los consumidores tienen derecho a que la asistencia pública confiable sea considerada de la misma manera que otro ingreso, y fundamentalmente, a que frente a la negativa de crédito, el afectado pueda conocer los motivos.

Además, la ley prohíbe a los acreedores discriminar a los solicitantes de crédito que ejercen de buena fe los derechos otorgados por la ley.

4.1.7. Family Education Rights Act (FERPA)

La ley de Derecho a la privacidad familiar en el ámbito educativo de 1974[17]es una ley federal que protege la privacidad de los datos que obran en el legajo o expediente del estudiante. Se aplica a todas las escuelas que reciban fondos de un programa del Departamento de Educación de los E.E.U.U..

La *FERPA* da a los padres ciertos derechos con respecto a los expedientes de la educación de sus hijos, y transfiere estos derechos al estudiante cuando él o ella alcanza la edad de 18 años o asiste a una escuela más allá del nivel de la “High School” secundaria. Los estudiantes a quienes se han transferido estos derechos se denominan “estudiantes elegibles.”

Los padres o los estudiantes elegibles tienen el derecho de examinar los legajos o expedientes mantenidos por la escuela referidos a la educación del estudiante

Las escuelas no están obligadas a expedir copias de esta documentación a menos que sea imposible para que los padres o los estudiantes elegibles revisen los expedientes (por ejemplo, por razones de gran distancia).

Los padres o los estudiantes elegibles tienen derecho a solicitar la corrección de datos cuando éstos sean inexactos o engañosos. Si la escuela decide no enmendar

[17] § 1232g de 20 U.S.C.; La parte 99 de 34 CFR.

el dato se puede exigir una audiencia luego de la cual, si se mantiene la negativa se faculta al afectado a incorporar al legajo una declaración con su opinión sobre la información disputada.

Los establecimientos educativos necesitan el permiso escrito del padre o del estudiante elegible para difundir cualquier información del expediente de la educación de un estudiante. Sin embargo, *FERPA* permite que las escuelas divulguen esos expedientes, sin consentimiento, en ciertos casos (§ 99.31 de 34 CFR), tales como funcionarios de la escuela con interés educativo legítimo; otras escuelas a las cuales un estudiante se está transfiriendo; funcionarios encargados de la evaluación del estudiante; los responsables de ayuda financiera a un estudiante; organizaciones que conducen ciertos estudios para o a nombre de la escuela; organizaciones de acreditación. Tampoco es necesario el consentimiento previo cuando debe cumplirse con una orden judicial o una citación legal publicada; o cuando es requerida por funcionarios competentes en casos de emergencias de salud y de seguridad o por el Estado o las autoridades locales, dentro de un sistema juvenil de la justicia, conforme a ley específica del estado.

En cambio, es posible publicar sin consentimiento lo que se conoce como “directorio” que comprende el nombre de un estudiante, dirección, número de teléfono, fecha y lugar del nacimiento, los honores y las concesiones, y las fechas de asistencia o cursada. Sin embargo, las escuelas deben informar a los padres y estudiantes elegibles sobre la información del directorio y permitir padres y a estudiantes elegibles pedir que no se divulgue la información del directorio sobre ellos. Las escuelas deben notificar a padres y a estudiantes elegibles anualmente de sus derechos según la FERPA. Los medios reales de la notificación (letra especial, inclusión en un boletín de PTA, manual del estudiante, o artículo periodístico) se dejan a la discreción de cada escuela.

4.1.8. Electronic Fund Transfer Act (EFTA)

Esta ley de 1978 sobre transferencias electrónicas de fondos[18] establece la

[18] US Code Título XV, Capítulo 41, Subcapítulo VI § 1693.

obligación de las instituciones financieras que efectúen transferencias electrónicas u otros servicios bancarios por ese procedimiento, de informar a sus clientes del acceso de terceras personas a sus bancos de datos.

4.1.9. Privacy Protection Act 1980

La ley de 1980 regula la tutela especial que se establece en favor de periodistas o informadores, limitando las facultades de los agentes públicos dedicados a la persecución de los delitos, en relación con el registro de sus materiales de trabajo[19].

4.1.10. Counterfeit Access Device and Computer Fraud and Abuse Act (CFAA)

Es una ley federal sancionada en 1984[20] que tipifica conductas relacionadas con abusos y fraudes informáticos. Originalmente se centró en el acceso no autorizado o fraudulento a datos contenidos en computadoras vinculados con tarjetas de crédito, y se ha ido extendiendo hacia otras figuras de fraude y acceso no autorizado a bases de datos.

4.1.11. Cable Communications Policy Act (CCPA)

La ley de Protección de la Privacidad en la televisión por cable de 1984[21] tutela la información personal de clientes de los abastecedores de servicio de cable, incorporando pautas de las recomendaciones de la OCDE de 1980.

Las compañías de televisión por cable deben informar por escrito sus políticas de privacidad a cada suscriptor (cliente) en el momento de inicio del contrato de servicio y por lo menos una vez al año después de eso[22].

---

[19] http://www.informatica-juridica.com/legislacion/estados_unidos.asp/
[20] Public Law. 98-473, título 18, Sección 1030, US Code, aprobada el 12/10/1984. Fue modificada en 1986 y 1990.
[21] US Code Título 47, Capítulo 5 V-A del Subcapítulo Parte IV § 551.
[22] La política de privacidad debe especificar: a) la naturaleza de la información personalmente identificable que es o puede ser recogida, y sus destinos; b) la

Estas empresas deben obtener el previo consentimiento escrito o electrónico del suscriptor antes de recoger cualquier información personal. El consentimiento no se requiere para obtener la información "necesaria para prestar servicios de cable", lo que constituye una excepción demasiado abierta, ni para detectar usos no autorizados (piratería).

El acceso de la información personal sin consentimiento también se permite conforme a un orden judicial. El suscriptor debe ser notificado, y ofrecerle la posibilidad de cuestionar la orden. Los accesos pueden no incluir generalmente la información sobre las selecciones particulares del suscriptor de la programación video.[23]

Los proveedores de servicio de cable deben destruir la información personal cuando no se necesite más para los propósitos para los cuales fue recogida y no haya pedidos pendientes de acceso. Deben tomar medidas apropiadas para prevenir el acceso desautorizado de la información personal de los clientes.

Se pueden reclamar daños y perjuicios incluidos los punitivos.

La *CCPA* incluye específicamente "otros servicios" tales como "comunicaciones de la radio y del alambre," y podría aplicarse a la información sobre clientes de las conexiones de banda ancha del Internet del cable.

4.1.12. Electronic Communication Privacy Act (ECPA)

Ésta es la ley de privacidad en las comunicaciones electrónicas de 1986[24]. Prohíbe la interceptación de mensajes mandados por medio de esta tecnología, define todo lo relativo a comunicaciones electrónicas (correo electrónico, transmisiones vía satélite, telefonía celular, etc.), establece las sanciones civiles y penales por infringir la

---

"naturaleza, la frecuencia y el propósito" de cualquier acceso que se pueda hacer de tal información, incluyendo la identificación de las personas a quienes esos accesos pueden ser hechos; c) cuánto tiempo la información se puede mantener por el abastecedor de servicio de cable; d) donde y cómo el suscriptor puede tener acceso a la información sobre él o ella misma; y e) el derecho del suscriptor de interponer un reclamo legal si los requisitos de la ley no se siguen.

[23] Otra ley proporciona las protecciones para la información sobre las selecciones de los individuos de materiales de video alquilados.

[24] Public Law 99-508, 21/10/1986.

normativa, etc.

4.1.13. Computer Security Act (CSA)

Es una ley de 1987[25] que regula quién protege la información de los sistemas informáticos y el desarrollo de la criptografía en el Gobierno de USA. El Instituto Nacional para los Estándares y la Tecnología (*NIST*), una división del Ministerio de Comercio, es responsable de la seguridad de los sistemas informáticos sin clasificar, no militares, del gobierno. El papel de la Agencia de Seguridad Nacional (*NSA*) fue limitado a proporcionar asistencia técnica en el ámbito civil de la seguridad, considerando que era inadecuado que una agencia de inteligencia militar tuviera control sobre la difusión de la información sin clasificar.

Esta ley fue una reacción al decreto del Presidente Reagan (NSDD)[145] de 1984 que otorgó a la NSA control sobre toda la información “sensible pero sin clasificar” de los sistemas informáticos del gobierno.

4.1.14. Telephone Consumer Protection Act (TCPA)

La Ley de protección del consumidor de servicios telefónicos de 1991[26], protege a los consumidores contra llamadas no deseadas de comercialización telefónica, restringe las horas de las llamadas y el uso de los marcadores automáticos en la comercialización telefónica.

4.1.15. Cable Television Consumer Protection and Competition Act (CTCPCA)

Es una ley de 1992[27] que prohíbe la venta o publicación de la información correspondiente a los suscriptores de televisión por cable;

---

[25] Public Law 100-235.
[26] 47 USCC & 227 (Law. Co-op. 1994).
[27] 47 USCC & 551 (Law. Co-op. 1994).

4.1.16. Driver´s Privacy Protection Act (DPPA)

La norma fue sancionada en 1994[28]" para proteger la privacidad de la información personal sobre los automotores, prohibiendo la difusión o uso por cualquier Estado de la información personal sobre un individuo obtenido por los registros automotores. La última modificación exige a las oficinas estatales obtener el permiso de la persona antes de que la información de su legajo automotor se pueda vender o informar a terceras personas.

La ley fue cuestionada en su constitucionalidad y con motivo de la demanda entablada por Carolina del Sur[29], la Corte Federal sostuvo que el esquema regulatorio restringe la capacidad de los Estados de la Unión para revelar la información personal sobre cualquier individuo obtenida por el registro estadual del automotor sin su consentimiento. Agregó que esta prohibición no se aplicaba si los conductores prestaban su consentimiento a la divulgación de esos datos, el que debe ser expreso. Pero lo importante a los fines en comentario es que afirmó que esta ley de protección a la privacidad del conductor (LPPC) no es incompatible con los principios del federalismo norteamericano inherentes a la división de poderes entre los Estados y el Gobierno Federal -Enmienda décima de la Constitución de Estados Unidos- pues no exige que los Estados, en tanto entes soberanos, apliquen la regulación sobre sus propios ciudadanos, sino que regula a aquéllos en tanto propietarios de bases de datos y, por lo tanto, no viola los principios constitucionales del federalismo, pues la materia legislada constituye “cosa en el comercio interestadual" y, por ende, se halla sujeta a regulación por el Congreso en virtud de lo dispuesto por la Cláusula del comercio, art. 1° de la Constitución de los Estados Unidos.[30]

---

[28] Esta norma de Derecho Público Nº 103-322 codificada según la enmienda prevista por Public Law 106-69.

[29] SC Estados Unidos, 12/01/2000, “Janet Reno, Procuradora General de los Estados Unidos y otros, apelantes e. Charlie Condon, Procurador General del Estado de Carolina del Sur y otros”. El fallo en inglés en: http://supct.law.cornell.edu/supct/html/98-1464.ZO.html/

[30] Publicado también en LA LEY 2000-D, 404, con nota de Flores, Oscar, “La Corte Suprema Norteamericana y una sentencia que, acotando el poder de los Estados, afianza el derecho a la privacidad".

4.2. Legislación estatal

Los Estados tienen autoridad para hacer cumplir la FCRA, y muchos Estados tienen su propia legislación de informe del consumidor. En algunos casos, los derechos del consumidor pueden ser más amplios en virtud de la ley estatal.

Las legislaciones estatales también protegen la intimidad personal en diversas situaciones. Las áreas cubiertas comprenden los registros bancarios, las suscripciones a televisión por cable, los informes de crédito, los registros de empleo, los registros oficiales, los datos genéticos e historiales médicos, los registros de seguro, los historiales académicos, las comunicaciones electrónicas y el alquiler de vídeos.

Tanto las leyes federales que hemos reseñado, como las leyes estatales, permiten que los consumidores impongan límites a lo que los bancos y otras compañías financieras pueden hacer con su información financiera personal.

Por ejemplo la ley de California[31] es más avanzada respecto a los límites de revelación de la información financiera personal. Exige que las empresas de servicios financieros pidan autorización al concernido antes de compartir su información con empresas externas que no ofrezcan productos o servicios financieros. Las compañías financieras deben notificar anualmente a sus clientes sus derechos a la privacidad. La ley de California requiere que los avisos sean fáciles de leer y entender. También permite avisar a un banco y otras instituciones financieras el deseo de no compartir la información financiera personal con compañías externas que ofrezcan productos o servicios financieros, o con las empresas poseídas o controladas por su empresa financiera (o sea, las afiliadas). En caso de silencio se entienen que la compañía podrá compartir su información con otros.

Si el consumidor considera que se ha violado su privacidad puede presentar una queja ante el Procurador General del Estado de California o ante una dependencia estatal o federal que regule las empresas financieras. La dependencia, previa investigación, puede tomar medidas contra la empresa financiera.

---

[31] Ley de Privacidad del Estado California, 1992.

Las principales leyes de privacidad financiera del Estado de California en esta materia son la Ley de la Privacidad de Información Financiera (California Financial Information Privacy Act) secciones 4050 a 4060 del Código Financiero[32]; la Financial Services Modernization Act, (GLB) (Ley de Modernización de Servicios Financieros) 15 U.S. Code 6801-6810.[33]

4.3. Acuerdo de "Puerto Seguro".

La legislación estadounidense se caracteriza por promover que los propios interesados sean quienes velen por el cumplimiento de la normativa relativa al tratamiento de los datos personales que les conciernen ya sea a través del ejercicio de los derechos que se reconocen al titular de los datos, o bien mediante la formulación de códigos deontológicos y adopción de disposiciones reglamentarias por los órganos responsables de sistemas de registro. El Estado asegura su posición de gendarme mediante el establecimiento de excepciones fundadas en necesidades de orden público, prescindiendo de la consagración de una autoridad de control pública que vele por el cabal cumplimiento de la legislación.[34]

Este modelo de autoregulación y autocontrol, unido al mosaico normativo de normas federales y estaduales aparece en franca oposición al favorecido por los Estados miembros de la Unión Europea, y no se armoniza con la pretensión de un nivel de protección adecuado en las transferencias transfronterizas de datos personales desde Europa a los Estados Unidos. Ello motivó extensas rondas de negociación que condujeron a los llamados "Acuerdos de Puerto Seguro" (*Safe Harbor Agreement*), mediante los que se ha procurado conciliar ambas opciones legislativas.

---

[32] http://www.privacy.ca.gov/lawenforcement/laws.htm#five/
[33] http://www.ftc.gov/privacy/glbact/glbsub1.htm/
[34] El sistema de autocontrol promovido por Estados Unidos es objeto de serios cuestionamientos en su seno; así Andrew Shapiro, de la Universidad de Harvard, además de rechazar el actual estado de desarrollo de la protección de la privacidad – especialmente de los datos personales– y repudiar un enfoque mercantilista como solución, ha abogado por la creación de un organismo federal que coordine la protección de la privacidad a nivel nacional como en el extranjero, o bien, en su defecto, cuando menos encargar a alguna entidad existente todas las políticas relacionadas con la materia. Cf. Shapiro, Andrew, "The control revolution" (1999)."El mundo en un clic", trad. Francisco Ramos, Grijalbo. Barcelona, 2001, pp. 259 – 268, 348 – 351.

A mediados del 2000, el Departamento de Comercio de los Estados Unidos publicó los denominados *Safe Harbor Privacy Principles*, traducidos como Principios de Puerto Seguro, texto que contempla los principios a que deben sujetarse las entidades estadounidenses para obtener el visto bueno de la Unión Europea, a fin de asegurar una política de protección de datos adecuada, que brinde privacidad y confidencialidad homologables a los estándares europeos, tras lo cual podrán recibir cesiones de datos personales provenientes de los Estados miembros de la Unión Europea sin problemas ni sanciones para cedente o cesionario.[35]

Por su adhesión a *Safe Harbor* los organismos y entidades asumen ciertos principios rectores del tratamiento de datos, a saber: notificación e información a las personas, previas a la recogida de datos que les conciernen; derecho de opción para divulgación a terceros o usos incompatibles con el objeto inicial de la recogida, ya sea en listas de exclusión o aceptación, según la naturaleza de los datos; se condiciona la transferencia ulterior de datos a terceros a la adopción de los principios de *Safe Harbor*; se impone a las entidades tratantes de datos la obligación de implementar medidas de seguridad y la obligación de velar por la calidad de los datos; reconocimiento de los derechos de acceso y rectificación a las personas concernidas; y, se establece la necesidad de que las entidades tratantes adopten mecanismos que brinden garantías para la aplicación de los principios, tales como recursos independientes, procedimientos de seguimiento y medios para subsanar infracciones y sancionarles, en su caso.

Se aclara que estos principios no son obligatorios para las empresas o entidades de Estados Unidos, ya que previamente deben aceptar voluntariamente la aplicación del Acuerdo, mediante autocertificación de su compromiso al respecto, la que debe ser notificada al Departamento de Comercio. Dicha notificación debe renovarse anualmente e incluye información básica relativa a la entidad u organización

[35] Para una revisión de la materia pueden consultarse el texto definitivo y anexos de Safe Harbor, así como los trabajos preparatorios elaborados por el Departamento de Comercio de los Estados Unidos, todos ellos disponibles en http://www.export.gov/safeharbor/ , en tanto que las observaciones, dictámenes e informes formuladas por el Grupo deTrabajo previsto por la Directiva 95/46/CE a las diversas versiones de Safe Harbor está disponible en su página Internet: http://europa.eu.int/comm/internal_market/privacy/index_en.htm/

adherente, el tratamiento de datos personales provenientes de Europa que efectúa y una descripción de las políticas de protección a la vida privada a que somete el procesamiento de aquellos. La verificación de las prácticas de protección de la vida privada, así como su conformidad con los principios de Safe Harbor puede ser efectuada por terceros o por la propia entidad.

Los compromisos asumidos por las entidades adscritas a Safe Harbor no son extensivos al tratamiento de toda la información personal, sino sólo a aquellos datos transmitidos desde la Unión Europea a partir del momento en que se adhiere al Acuerdo.

Adicionalmente, *Safe Harbor* contempla hipótesis de tratamiento de datos personales a los cuales no le son aplicables sus principios, tales como aquel efectuado en el marco de actividades periodísticas; una aplicación parcial de sus disposiciones al tratamiento de datos obtenidos en el contexto de una relación laboral; y previsiones ante la fusión o absorción de las entidades adheridas por otras.

La autoridad de aplicación es la *Federal Trade Commission* (Comisión Federal de Comercio), que goza de facultades ante actos o prácticas desleales o fraudulentos que constituyen un modelo de conducta continuado e inadecuado, en tanto ellos se relacionen con el comercio. Sin embargo, en principio, la FTC carece de competencia cuando la información está destinada a otros fines, así como en actividades específicas, tales como las financieras, de telecomunicaciones, transporte, aéreas y otras, evento en el cual guarda, a lo sumo, competencia residual o concurrente con otras entidades (*Federal Reserve Board, Office of Thrift Supervision, National Credit Union Administration Board* y los Departamentos de Transporte y Agricultura, por mencionar algunas).

Safe Harbor despertó inicialmente cierto optimismo en los especialistas, en especial porque había conjugado el régimen normativo europeo con la autorregulación estadounidense, aparentemente en términos satisfactorios; experiencia susceptible de proyectarse a otras experiencias en las cuales los sistemas de ambos bloques

manifiestan distancia.[36]

Sin embargo, el tiempo permitió apreciar los reales efectos del acuerdo: la pluralidad de disposiciones legales aplicables, el mosaico de instituciones comparecientes como autoridades de aplicación, las restringidas facultades conferidas a éstas para velar por el cumplimiento, así como los márgenes de autoregulación, la fiabilidad de la autocertificación y el escaso número de entidades y organismos que han hecho propios los principios de *Safe Harbor*,[37] han generado cierto grado de preocupación por la exigua eficacia del Acuerdo entre las autoridades competentes de los Estados miembros de la Unión Europea, quienes afrontan nuevas negociaciones con Estados Unidos con miras a obtener un adecuado nivel de protección para los datos personales transmitidos allende el Atlántico[38].

4.4. Situación actual

Como hemos reseñado, desde el inicio de la década de los setenta, el Congreso de los Estados Unidos ha aprobado numerosas leyes para proteger la privacidad en varios sectores, además de las mencionadas, pueden citarse las denominadas Right to Financial Privacy Act de 1978, Computer Matching and Privacy Protection Act de 1988, Employee Polygraph Protection Act de 1988, Video Privacy Protection Act de 1988, Health Insurance Portability and Accountability Act de 1996, Children´s Online Privacy Protection Act de 1998, Gramm-Leach Bliley Act de 1999, entre otras.

Sin embargo, no toda la legislación emitida por el Congreso en los Estados

---

[36] Muñoz Machado, Santiago, "La regulación de la red. Poder y Derecho en Internet", Taurus. Madrid, 2000, pp. 181 – 189.

[37] Las proyecciones iniciales estimaban que a un año de haberse adoptado Safe Harbor cuando menos un millar de entidades y organismos estadounidenses se acogerían a los principios y obligaciones previstas en él; sin embargo, a la fecha, estando próximos a cumplir tres años desde su adopción, el número de adhesiones apenas si rebasa las trescientas. Información disponible en http://www.export.gov/safeharbor/

[38] Cerda Silva, Alberto, “Autodeterminación informativa y leyes sobre protección de datos”, en Revista chilena de Derecho Informático Nº 3 Diciembre 2003. Universidad de Chile. Facultad de Derecho., http://www.derechoinformatico.uchile.cl/CDA/der_informatico_completo/...)

Unidos está formulada para proteger la privacidad de los ciudadanos. Cierto número de leyes o estatutos han estipulado la recolección gubernamental de la llamada información sensible, es decir, aquella que tiene que ver con la raza, el sexo, la filiación sindical, etc., o que facilitan el uso de técnicas de investigación por parte de las autoridades de gobierno, entre estas podemos mencionar las siguientes disposiciones: Bank Secrecy Act de 1970, Communications Assistance for Law Enforcement Act de 1994, Personal Responsability and Work Opportunity Reconciliation Act de 1996.

Luego de los atentados del 11 de setiembre de 2001, la conocida como Patriot Act (por la sigla de *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USAPA)* [39] de 2001[40], ha modificado en forma sustantiva la legislación vigente en torno a la privacidad en línea. La norma introduce cambios importantes a diversos estatutos de la legislación federal de los Estados Unidos (United State Code) [41]. Se ha dicho que, "impone cambios legislativos con respecto a aspectos tan diversos que van desde el lavado de dinero, prácticas

[39] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001", que podríamos traducir como "Ley que unifica y fortalece a América al Proporcionar las Herramientas Apropiadas para interceptar u obstruir al Terrorismo". Su texto en español puede consultarse en: http://www.interamericanusa.com/articulos/Leyes/US-Patriot%20Act.htm/

[40] Puente de la Mora, ob.cit. supra.

[41] Según el EPIC (Electronic Privacy Information Center) esta ley afecta a las siguientes normas federales: Wiretap Statute (Title III), http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002510----000-.html/; Electronic Communications Privacy Act; Computer Fraud and Abuse Act; http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001030----000-.html/ Foreign Intelligence Surveillance Act, http://www4.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001801----000-.html/; Family Education Rights and Privacy Act, http://www4.law.cornell.edu/uscode/html/uscode20/usc_sec_20_00001232---g000-.html/; Pen Register and Trap and Trace Statute, http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00003121----000-.html/; Money Laundering Act, http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00000981----000-.html/; Immigration and Nationality Act, http://www4.law.cornell.edu/uscode/html/uscode08/usc_sup_01_8.html/; Money Laundering Control Act; Bank Secrecy Act, http://www4.law.cornell.edu/uscode/html/uscode31/usc_sup_01_31_08_IV_10_53_20_II.html/; Right to Financial Privacy Act y Fair Credit Reporting Act.

crediticias y servicios bancarios y financieros, comunicaciones por medios electrónicos, educación de la familia, espionaje e inteligencia, migración, así como intervención de comunicaciones telefónicas, etc."[42]

Las implicaciones con respecto a la privacidad en línea son considerables, ya que este estatuto incrementa la facultad de los organismos de impartición y administración de justicia para autorizar la instalación de equipos de intervención telefónica y dispositivos de rastreo, así como la instalación de dispositivos que canalicen, envíen y señalen la información de las computadoras. Dicha ley también "aumenta las facultades del gobierno para obtener información financiera personal, así como estudiantil, sin necesidad de comprobar sospecha o hechos constitutivos de delitos, simplemente con la certificación que posiblemente se obtendrá es relevante para una investigación criminal que actualmente se lleve a cabo"[43].

[42] Sitio oficial de Electronic Privacy Information Center EPIC, http://www.epic.org/privacy/terrorism/usapatriot/. Cf. Puente de la Mora, ob.cit y nuestro acceso a dicho sitio el 29/01/2007.
[43] Idem nota supra.

Capitulo 5. Derecho comparado. Constituciones y de Leyes América Latina y otros países.

Sumario: Constituciones. Brasil. Colombia. Perú. Paraguay. Ecuador. Venezuela. Guatemala. Nicaragua. Bolivia. Honduras. Leyes nacionales. Brasil. Chile. Ecuador. Paraguay. Perú. Venezuela. México. Uruguay. Colombia. El Salvador. Panamá. Costa Rica. Otros países. Canadá. Organización de Estados Americanos (OEA).Legislación de otros países fuera del continente americano. Australia. Cooperación Económica de Asia-Pacífico (APEC). Sintesis.

5.1. Constituciones

En el ámbito latinoamericano, varios países han consagrado constitucionalmente la protección de los datos personales.

5.1.1. Brasil

La Constitución de 1988[1]*, dispone en su artículo artículo 5 inc. LXXIII:* "Se concederá "habeas data": a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo".También prevé, en el inciso LXXVII, que son gratuitas las acciones de "habeas corpus" y "habeas data" y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía. El artículo 108, dice que es competencia de los Tribunales Regionales Federales: I procesar y juzgar, originariamente: c) los "mandados de seguranca" y los "habeas data" contra actos del propio Tribunal o de los jueces federales".

5.1.2. Colombia

La Constitución de 1991[2] *establece:* "Artículo 15. Todas las personas tienen

[1] su texto en español: http://www.constitution.org/cons/brazil.htm/
[2] su texto en español: http://pdba.georgetown.edu/Constitutions/Colombia/colombia.html/

derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. 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. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley."

5.1.3. Perú

La Constitución Política de 1993 dispone en su artículo 2, en tres incisos, los derechos que relacionamos con la protección de datos: "5: A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria pueden levantarse a pedido 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.- 6: A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.- 7: Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley."

En el inciso 3 del artículo 200 incorpora la acción de Hábeas Data, modificando así lo previsto por la Constitución de 1991: "3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Artículo 2º, incisos 5 y 6 de la

Constitución.[3]

5.1.4. Paraguay

La Constitución de 1992[4] prevé en su artículo 135, bajo el título "Del Habeas Data": "Toda persona puede acceder a la información y a los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos". El artículo 30 referido a las señales de comunicación electromagnética, indica en su parte final: "Las autoridades asegurarán que estos elementos no sean utilizados para vulnerar la intimidad personal o familiar y los demás derechos establecidos en esta Constitución." El artículo 33 está referido al derecho a la intimidad.

El artículo 28, más orientado a lo que se conoce como *"derecho a réplica",* declara: "Se reconoce el derecho de las personas a recibir información veraz, responsable y ecuánime. Las fuentes públicas de información son libres para todos. La ley regulará las modalidades, plazos y sanciones correspondientes a las mismas, a fin de que este derecho sea efectivo. Toda persona afectada por la difusión de una información falsa, distorsionada o ambigua tiene derecho a exigir su rectificación o su aclaración por el mismo medio y en las mismas condiciones que haya sido divulgada, sin perjuicio de los demás derechos compensatorios."

5.1.5. Ecuador

La Constitución de 1998[5] dispone en su artículo 94: "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma,

---

[3] Incisos modificados por el Artículo único de la Ley 26470, publicada el 12/06/1995, http://www.congreso.gob.pe/constitucion.htm/. Antes de la reforma, el texto decía: "La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2°, incisos 5,6 y 7 de la Constitución."

[4] http://pdba.georgetown.edu/Constitutions/Paraguay/para1992.html/

[5] Registro Oficial No. 1, 01/08/1998, http://pdba.georgetown.edu/Constitutions/Ecuador/ecuador98.html/

o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional."[6]

5.1.6. Venezuela

La Constitución de 1999[7] se refiere al tema en varios varios artículos*: El artículo 28 dice:* "Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes 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 de las fuentes de información periodística y de otras profesiones que determine la ley". *El artículo 60 reza:* "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."

Por su lado, el artículo 281, que refiere las atribuciones del Defensor o Defensora del Pueblo, en su inciso 3 lo autoriza a "Interponer las acciones de inconstitucionalidad, amparo, habeas corpus, habeas data y las demás acciones o recursos necesarios para ejercer las atribuciones señaladas en los ordinales anteriores, cuando fuere procedente de conformidad con la ley."

---

[6] Puccinelli
[7] Publicada en Gaceta Oficial, 30/12/1999, No. 36.860, http://pdba.georgetown.edu/Constitutions/Venezuela/ven1999.html/

5.1.7. Guatemala

La Constitución de 1993[8] *en su artículo 31, bajo el título "Acceso a archivos y registros estatales" establece:* "Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos".

Esta norma debe articularse con el artículo 24, que bajo el rótulo "Inviolabilidad de correspondencia, documentos y libros", establece: "La correspondencia de toda persona, sus documentos y libros son inviolables. Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. Se garantiza el secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna. Los libros, documentos y archivos que se relacionan con el pago de impuestos, tasa, arbitrios y contribuciones, podrán ser revisados por la autoridad competente de conformidad con la ley. Es punible revelar el monto de los impuestos pagados, utilidades, pérdidas, costos y cualquier otro dato referente a las contabilidades revisadas a personas individuales o jurídicas, con excepción de los balances generales, cuya publicación ordene la ley. Los documentos o informaciones obtenidas con violación de este artículo no producen fe ni hacen prueba en juicio."

5.1.8. Nicaragua

La Constitución de 1987[9]*, en su artículo 26, dispone*: "Toda persona tiene

---

[8] Constitución de 1985, reformada en 1993, http://pdba.georgetown.edu/Constitutions/Guate/guate93.html/

[9] Esta Constitución Política de la República de Nicaragua ha sido reformada parcialmente por Ley No. 192 del 01/02/1995; ley 330 del 18/01/2002 y Ley 527 del 08/04/2005, http://pdba.georgetown.edu/Constitutions/Nica/nica05.html/. El texto del artículo continúa en estos términos: "El domicilio sólo puede ser allanado por orden escrita de juez competente, excepto: si los que habitaren en una casa manifestaren que allí se está cometiendo un delito o de ella se pidiera auxilio; si por incendio, inundación u otra causa semejante, se hallare amenazada la vida de los habitantes o de la propiedad; cuando se denunciare que personas extrañas han sido vistas en una morada, con indicios manifiestos de ir a cometer un delito; en caso de persecución actual e

derecho: 1. A su vida privada y la de su familia. 2. A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo. 3. Al respeto de su honra y reputación. 4. A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información."

5.1.9. Bolivia

La Constitución de 1967 con la reforma de 2002[10], establece en su artículo 23[11] la "Acción de Habeas Data", con el siguiente desarrollo: "I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de Habeas Data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya. II. Si el tribunal o juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado. III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo. IV. El recurso de Habeas Data no procederá para levantar el secreto en materia de prensa. V. El recurso de Habeas Data se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional

---

inmediata de un delincuente; para rescatar a la persona que sufra secuestro. En todos los casos se procederá de acuerdo a la ley. La ley fija los casos y procedimientos para el examen de documentos privados, libros contables y sus anexos, cuando sea indispensable para esclarecer asuntos sometidos al conocimiento de los tribunales de justicia o por motivos fiscales. Las cartas, documentos y demás papeles privados substraídos ilegalmente no producen efecto alguno en juicio o fuera de él. (Artículo reformado por Ley 192 de 1995).

[10] Constitución de 1967 con reformas introducidas por la Ley 1585 del 12/08/1994, texto concordado de 1995 sancionado por Ley 1615 del 06/02/1995, reformas introducidas por Ley 2410 del 08/08/2002, reformas introducidas por Ley 2631 del 20/02/2004, y reformas introducidas por Ley 3089 del 06/07/2005, http://pdba.georgetown.edu/Constitutions/Bolivia/consboliv2005.html/

[11] Ley 2631 de 20/02/2004, http:// www.uc3m.es/uc3m/inst/MGP/JCI/revista-05notnor-boli.htm/

previsto en el Artículo 19º de esta Constitución."

5.1.10. Honduras

La Constitución de 1982, reformada en 2003[12] ha introducido en el Título IV, sobre Garantías constitucionales, Capítulo I, bajo la denominación "Del Habeas corpus, Habeas data y el Amparo"[13], en el artículo 182: "El Estado reconoce la garantía de Hábeas Corpus o Exhibición Personal, y de Hábeas Data. En consecuencia en el Hábeas Corpus o Exhibición Personal, toda persona agraviada o cualquier otra en nombre de ésta tiene derecho a promoverla; y en el Hábeas Data únicamente puede promoverla la persona cuyos datos personales o familiares consten en los archivos, registros públicos o privados de la manera siguiente: ... 2. El Hábeas Data: Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en caso de que fuere necesario, actualizarla, rectificarla y-o enmendarla. Las acciones de Hábeas Corpus y Hábeas Data se ejercerán sin necesidad de poder ni de formalidad alguna, verbalmente o por escrito, utilizando cualquier medio de comunicación, en horas o días hábiles o inhábiles y libre de costas. Únicamente conocerá de la garantía del Hábeas Data la Sala de lo Constitucional de la Corte Suprema de Justicia, quien tendrá la obligación ineludible de proceder de inmediato para hacer cesar cualquier violación a los derechos del honor, intimidad personal o familiar y la propia imagen. Los titulares de los órganos jurisdiccionales no podrán desechar la acción de Hábeas Corpus o Exhibición Personal e igualmente tienen la obligación ineludible de proceder de inmediato para hacer cesar la violación a la libertad y a la seguridad personal. En ambos casos, los titulares de los órganos jurisdiccionales que dejaren de admitir estas acciones constitucionales, incurrirán en responsabilidad penal y administrativa. Las autoridades que ordenaren y los agentes que ejecutaren el ocultamiento del detenido o que en cualquier forma quebranten esta garantía incurrirán en el delito de detención ilegal."

---

[12] La Constitución de Honduras ha sufrido numerosas reformas. Si texto actualizado hasta el Decreto 36 del 04/05/2005 en: http://pdba.georgetown.edu/Constitutions/Honduras/hond05.html/

[13] Denominación modificada por decreto 243/2003.

5.1.11. México

La Constitución Política de los Estados Unidos Mexicanos, en el tema que nos ocupa, fue reformada en el año 2009, incorporándose en su artículo 16, como segundo párrafo, el siguiente texto: *"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*"[1]

Esta modificación fue precedida por otra, que introdujo en el artículo 73, sobre las facultades del Congreso de la Unión, la de "legislar en materia de protección de datos personales en posesión de particulares"[2].

Al momento de escribir estas líneas no se habían dictado las leyes reglamentarias de estas dos importantes reformas al texto constitucional mexicano, para lo que hay que considerar que en el último caso, se estableció un plazo de doce meses para que el Congreso aprobara la legislación pertinente.

5.2. Leyes nacionales

Sobre esta materia existen leyes en varios países latinoamericanos, con la particularidad que, en algunos casos, la norma es una consecuencia de las previsiones constitucionales que hemos mencionado, en otros casos, no existen alusiones explícitas a la protección de datos, pero sí se han sancionado leyes y en otros casos sólo hay disposiciones en el texto constitucional.

5.2.1. Brasil

La Ley 9507 de 1997[14] reglamenta el derecho de acceso a las informaciones y el procedimiento de la acción de habeas data. El artículo 7º de dicha norma establece que (se concede) hábeas data: "I. para asegurar el conocimiento de informaciones relativas a la persona del impetrante, obrantes en registros o bancos de entidades gubernamentales o de carácter público; II. para la rectificación de datos, cuando no se prefiera hacerlo por proceso sigiloso, judicial o administrativo; III. para la anotación en los asientos del interesado, de contestación o explicación sobre dato verdadero pero justificable y que esté en pendencia judicial o amigable."

El procedimiento está regulado en varios artículos, de la siguiente manera: "Art. 2°. El requerimiento será presentado al órgano o entidad depositaria del registro o banco de datos y será aceptado o rechazado en el plazo de cuarenta y ocho horas. Parágrafo único. La decisión será comunicada al requirente en veinticuatro horas. Art. 3°. Al recibir el pedido, el depositario del registro o del banco de datos fijará día y hora para que el requirente tome conocimiento de las informaciones. Art. 4°. Constatada la inexactitud de cualquier dato a su respecto, el interesado, en petición acompañada de documento comprobatorio, podrá requerir su rectificación. § 1°. Hecha la notificación en el máximo de diez días después de la entrada del requerimiento, la entidad u órgano depositario de registro o de la información dará conocimiento al interesado. § 2°. Aunque no se constate la inexactitud del dato, si el interesado presenta explicación o contestación sobre el mismo justificando la posible diferencia sobre el hecho objeto del dato, tal explicación será anotada en el catastro del interesado. Art. 8°. La petición inicial, que deberá contener los requisitos de los arts. 282 a 285 del Código de Procedimiento Civil, será presentada en dos vías, y los documentos que constituyan la primera serán reproducidos por copia en la segunda. Parágrafo único. La petición inicial deberá ser instruida con prueba: I. de la negativa al acceso a las informaciones o del transcurso de más de diez días sin decisión; II. de la negativa de hacer la rectificación o del transcurso de más de quince días, sin decisión; o III. de la negativa de hacer la anotación a que se refiere el § 2° del art. 4° o del transcurso de más de

[14] Publicada el 12/11/1997. Ver Puccinelli, Oscar, "El habeas data en Brasil", http://www.astrea.com.ar/files/prologs/doctrina0080.pdf/, publicado en Puccinelli, "El hábeas data en Iberoamérica", Bogotá, Temis, 1999, p. 295.

quince días sin decisión. Art. 9°. Al despachar la inicial, el juez ordenará que se notifique al demandado del contenido de la petición, entregándole la segunda vía presentada por el impetrante, con las copias de los documentos, a fin de que, en el plazo de diez días, preste las informaciones que juzgara necesarias. Art. 10. La inicial será desde luego rechazada, cuando no fuera el caso de hábeas data, o si le faltara alguno de los requisitos previstos en esta ley. Parágrafo único. Contra el despacho que rechaza la inicial cabrá el recurso previsto en el art. 15. Art. 11. Hecha la notificación, el secretario de la causa adjuntará a los autos copia auténtica del oficio dirigido al demandado y la prueba de su entrega a éste o de la negativa, sea de recibirlo, sea de dar recibo. Art. 12. Vencido el plazo al que se refiere el art. 9°, y oído el representante del ministerio público dentro del plazo de cinco días, los autos serán remitidos al juez para que adopte la decisión, que será proferida en cinco días. Art. 13. En la decisión, si juzgara procedente el pedido, el juez fijaría día y horario para que el demandado: I. presente al impetrante las informaciones a su respecto, obrantes en registros o bancos de datos; o II. presente en juicio la prueba de la rectificación o de la anotación hecha en los asientos del impetrante. Art. 14. La decisión será comunicada al demandado, por correo, con aviso de recepción, o por telegrama, radiograma o telefonema, conforme lo requiera el impetrante. Parágrafo único. Los originales, en el caso de transmisión telegráfica, radiofónica o telefónica deberán ser presentados a la agencia expedidora, con la firma del juez debidamente certificada. Art. 15. De la sentencia que conceda o deniegue el hábeas data cabe apelación. Parágrafo único. Cuando la sentencia concediera el hábeas data, el recurso tendrá efecto meramente devolutivo. Art. 16. Cuando el hábeas data fuera concedido y el presidente del tribunal al que competa el conocimiento del recurso ordenara al juez la suspensión de la ejecución de la sentencia, de ese acto cabrá agravio ante el tribunal que preside. Art. 17. En los casos de competencia del Supremo Tribunal Federal y de los demás tribunales cabrá a los relatores la instrucción del proceso. Art. 18. El pedido de hábeas data podrá ser renovado si la decisión denegatoria de éste no hubiera apreciado el mérito. Art. 19. Los procesos de hábeas data tendrán prioridad sobre todos los actos judiciales, excepto el hábeas corpus y el mandato de *segurança.* En la instancia superior deberán ser llevados a juzgamiento en la primera sesión que siga el día en que, hecha la distribución, fueran concluidos al relator. Parágrafo único. El plazo para la conclusión no podrá exceder de veinticuatro horas, a contar de la distribución. Art. 20. El juzgamiento del hábeas data compete: 1. Originariamente: a) al Supremo Tribunal Federal, contra actos del presidente de la República, de las mesas de la

Cámara de los Diputados y del Senado Federal, del Tribunal de Cuentas de la Unión, del procurador general de la República y del propio Supremo Tribunal Federal; b) al Superior Tribunal de Justicia, contra actos de ministro de Estado o del propio tribunal; c) a los tribunales regionales federales contra actos del propio tribunal o de juez federal; d) a juez federal, contra acto de autoridad federal, exceptuados los casos de competencia de los tribunales federales; e) a tribunales estaduales, según lo dispuesto en la Constitución del Estado; f) a juez estadual, en los demás casos. ll. En grado de recurso: a) al Supremo Tribunal Federal, cuando la decisión denegatoria fuera proferida en única instancia por los tribunales superiores; b) al Superior Tribunal de Justicia, cuando la decisión fuera proferida en única instancia por los tribunales regionales federales; c) a los tribunales regionales federales, cuando la decisión fuera proferida por juez federal; d) a los tribunales estaduales y a los del Distrito Federal y Territorios, conforme dispusieron la respectiva Constitución y la ley organizativa de la justicia del distrito federal. III. Mediante recurso extraordinario al Supremo Tribunal Federal, en los casos previstos en la Constitución. Art. 21. Son gratuitos los procedimientos administrativos para acceso a informaciones y rectificación de datos y para anotación de justificación, así como la acción de hábeas data."

Esta norma, de carácter eminentemente procesal, guarda profunda semejanza con la ley 1533 del 31 de diciembre de 1951, que reglamenta el procedimiento del *mandado de segurança*[15].

De la sentencia que concede o niega el hábeas data, cabrá el recurso de apelación. En el procedimiento previsto para el hábeas data solo hay lugar para recursos voluntarios, no repitiéndose la previsión del art. 12 de la ley 1533/91, que prevé el doble grado de jurisdicción obligatorio (reexamen necesario) de las decisiones que concedieran el mandato de *segurança*. Los plazos de los recursos en el procedimiento del hábeas data, por ausencia de expresa previsión en la referida ley, son los mismos previstos en el Código Procesal Civil, siendo duplicados para la hacienda pública y para el ministerio público (C. de P. C., art. 188). Están legitimados para la interposición del recurso de apelación: el impetrante; el ministerio público; el demandado y las entidades gubernamentales, de la administración pública directa e

[15] Puccinelli, ob.cit. supra.

indirecta, así como las instituciones, entidades o personas jurídicas privadas que presten servicios para el público o de interés público, siempre que detenten datos referentes a las personas físicas o jurídicas, a que pertenezca el demandado[16].

La ley excluye el efecto suspensivo de la sentencia que concede el hábeas data pero el presidente del tribunal al cual competiera el conocimiento del recurso puede ordenar al juez la suspensión de la ejecución de la sentencia. De esa forma, como regla general, el juez de primer grado está imposibilitado de conceder efecto suspensivo al recurso de apelación de la sentencia que concediera el hábeas data, lo cual no impide, por ejemplo, la suspensión de los efectos del hábeas data por acto del presidente del tribunal que debe motivar su decisión y su resolución puede ser recurrida ante el tribunal que la preside. Siendo así, la suspensión de la ejecución provisoria de la sentencia que conceda el hábeas data no podrá ser obtenida por medio del recurso de apelación, de cualquier otro recurso o acción genérica, ni por el mandato de *segurança*, toda vez que la propia ley estipula la medida posible de forma taxativa y expresa: despacho del presidente del tribunal[17].

Asimismo, con base en el art. 125 n° 1 de la Carta Magna, cada Estado miembro establecerá en el ámbito de la justicia estadual la competencia para el proceso y juzgamiento del hábeas data"[18].

De acuerdo a lo informado por la Agencia Española de Protección de datos en diciembre de 2004[19], el senado de la República brasileña ha admitido un proyecto de de ley de Protección de datos del Senador Sérgio Zambiasi, (proyecto del senado número 321/04).

Las líneas básicas del proyecto del senador Zambiasi[20] establecen como ámbito de aplicación la protección, tratamiento y uso de los datos de las personas

---

[16] Ídem nota supra.
[17] Ídem nota supra.
[18] Ídem nota supra.
[19] https://www.agpd.es/index.php?idSeccion=353/: "Se inicia la tramitación de una Proposición de Ley de Protección de Datos en Brasil."
[20] https://www.agpd.es/upload%2FPROJETO%20DE%20LEI%20DO%20SENADO%20N.pdf/

naturales y jurídicas de derecho público y privado (Art. 1º); entre los principios aplicables al tratamiento de los datos personales establece los de: licitud,buena fe, finalidad determinada, adecuación y actualización periódica de las informaciones, conservación de los datos por plazo determinable, consentimiento del titular, acceso del titular al banco de datos.(Art. 4º). Aclara los principios aplicables a determinadas categorías de datos (datos sensibles) (Art. 5º). Consagra los derechos básicos del titular de los datos: respecto a las libertades y garantías fundamentales, derecho de acceso, información previa, rectificación, consentimiento, cancelación, oposición, prescripción en cinco años, materia crediticia, facilitación de la defensa de derechos en procesos judiciales (Art. 7º). Organiza la supervisión por una autoridad independiente: el proyecto prevé la creación -mediante disposición reglamentaria- de una autoridad administrativa, federal, estadual, DF o municipal (Art. 15).[21]

La Agencia española apunta que es un proyecto en el que han contribuido decisivamente los miembros de la Red Iberoamericana de Protección de Datos de aquél país, es el primero de ámbito federal en materia de protección de datos y constituye un importante paso en el desarrollo de este derecho fundamental en la región[22].

La ley 8078/90, Código de Defensa de los Consumidores[23], establece en su artículo 43, que “El consumidor, sin perjuicio de lo dispuesto en el artículo 86, tendrá acceso a las informaciones existentes en registros, fichas, datos personales y de consumo archivados a su respeto, así como a las respectivas fuentes de información. Párrafo 1. Los registros y datos sobre los consumidores deben ser objetivos, claros, verdaderos y en lenguaje de facil entendimiento, y no pueden contener informaciones negativas referentes a un periodo superior a cinco años. Párrafo 2. La apertura de registro, ficha, archivo y datos personales y de consumo deberá ser comunicada por escrito al consumidor caso no solicitada por él. Párrafo 3. Siempre que encuentre alguna divergencia en sus datos y registros el consumidor podrá exigir su inmediata

[21] según información relevada el 31-01-2007, en la página del senador Zambiasi, el proyecto está en tratamiento en las Comisiones de Constitución, Justicia y Ciudadanía, http://www.senado.gov.br/sf/atividade/Materia/Detalhes.asp?p_cod_mate=71080/
[22] https://www.agpd.es/index.php?idSeccion=353/
[23] Código de defensa del consumidor de Brasil, Ley 8078 del 11/09/1990, http://www.procon.sc.gov.br/legislacao_02.htm/

corrección, debendo el archivista en el plazo de cinco días hábiles comunicar la alteración a los eventuales destinatarios de las informaciones incorrectas. Párrafo 4. Los bancos de datos y registros relativos a consumidores, los servicios de protección al crédito y equivalentes serán considerados entidades de carácter público. Párrafo 5. Ocurriendo prescripción relativa a la cobranza de deudas del consumidor, no podrán ser ofrecidas por los respectivos Sistemas de Protección al Crédito cualquier información que pueda impedir o dificultar nuevo acceso al crédito junto a los proveedores."

El artículo 44, por su parte dispone que "Los órganos públicos de defensa del consumidor mantendrán registros actualizados de las reclamaciones fundamentadas en contra proveedores de productos y servicios, debendo divulgarlos pública y anualmente. La divulgación indicará si la reclamación fue atendida o no por el proveedor. Párrafo 1. - Es posible el acceso de cualquier interesado a esas informaciones para fines de orientación y consulta. Párrafo 2. - Se aplican a este artículo, en lo que sea conveniente, las mismas reglas mencionadas en el artículo anterior y las del párrafo único del artículo 22 de este Código.

Podrían incluirse en el plexo normativo brasileño otras normas[24], tales como la ley 9.296/96[25] y la ley 10.217/01[26] que reglamentan la intercepción de comunicaciones telefónicas y electrónicas como también el tratamiento de esos datos. La Ley Complementaria 105/01, que permite que autoridades administrativas quiebren el secreto bancario, cuando existan hipótesis de delitos graves, sin autorización judicial[27].

En mayo de 2009, la Cámara de Diputados de Brasil aprobó un proyecto de ley destinado a regular los bancos de datos de protección del crédito y las relaciones

[24] ver III Encuentro Iberoamericano de Protección de Datos, Cartagena de Indias, Colombia, 24 al 28/05/2004: "Cuadro comparativo desarrollos normativos nacionales en materia de protección de datos", en https://www.agpd.es/upload/TERCERApropuestadecuadrodenormativas.pdf/
[25] reglamenta el inciso XII parte final del art. 5º de la Constitución de Brasil, 24/07/1996, https://www.planalto.gov.br/casacivil/site/static/le.htm/
[26] sancionada el 11/04/2001, https://www.planalto.gov.br/casacivil/site/static/le.htm/
[27] sancionada el 10/01/2001, https://www.planalto.gov.br/casacivil/site/static/le.htm/. La ley está pendiente de Acción Directa de Inconstitucionalidad al 24.05.2004.

comerciales[28], que ha pasado en revisión al Senado.

5.2.2. Chile

La Ley 19.628 sobre “Protección de la vida privada” de 1999[29] contiene veinticuatro artículos, divididos en un Título Preliminar (Disposiciones generales, arts. 1 a 3), cinco Títulos (I. De la utilización de datos personales, arts. 4 a 11; II. De los derechos de los titulares de datos, arts. 12 a 16; III. De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, arts. 17 a 19; IV. Del tratamiento de datos por los organismos públicos, arts. 20 a 22; y V. De la responsabilidad por las infracciones a esta ley, art. 23), y un Título Final (art. 24). En su última disposición transitoria aclara que las normas que regulan el Boletín de Informaciones Comerciales creado por el Decreto Supremo de Hacienda 950, de 1928, seguirán aplicándose en todo lo que no sean contrarias a las disposiciones de esta ley[30].

En el ámbito sanitario, el art. 24 de la Ley mencionada modificó al artículo 127 del Código Sanitario estableciendo: "Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo. Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los

---

28 Proyecto de ley 836-E-2003, http://www.camara.gov.br/sileg/integras/658894.pdf/

29 Promulgada el 18/08/1999 y publicada el 28/08/1999, http://www.anfitrion.cl/actualidad/20ulle/19628.html/

30 Peyrano, Guillermo F., "Bancos de datos" y tratamiento de datos personales. Análisis de algunas problemáticas fundamentales (Parangón de las previsiones de la ley argentina 25.326 con las disposiciones de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal” española y con la ley Nro.19.628 sobre "Protección de datos de carácter personal" de la República de Chile).”, fuera publicado en http://www.derecho.org/

médicos que las expidieron, ni datos que sirvan para identificarlos".

El Decreto N° 779, del 24 de agosto de 2000, ha reglamentado el Registro de Bancos de Datos Personales a cargo de organismos públicos[31], función que cumple el Registro Civil de Chile[32].

La Ley 19.812[33] modificó la Ley 19.628 en varios de sus artículos relacionados con informes crediticios, y prohíbe la comunicación de datos relativos a obligaciones extinguidas por algún medio legal o que, estando impagas, su monto por capital sea inferior a $2.000.000 (2600€, aproximadamente), entre otras disposiciones.

En materia laboral, la mencionada ley introdujo un nuevo inciso sexto al artículo 2 del Código del Trabajo que dice: "Ningún empleador podrá condicionar la contratación de trabajadores a la ausencia de obligaciones de carácter económico, financiero, bancario o comercial que, conforme a la ley, puedan ser comunicadas por los respon sables de registros o bancos de datos personales; ni exigir para dicho fin declaración ni certificado alguno. Exceptúanse solamente los trabajadores que tengan poder para representar al empleador, tales como gerentes, subgerentes, agentes o apoderados, siempre que, en todos estos casos, estén dotados, a lo menos, de facultades generales de administración; y los trabajadores que tengan a su cargo la recaudación, administración o custodia de fondos o valores de cualquier naturaleza."

La Ley 19.759[34] agrega el siguiente primer inciso al art. 5 del Código del Trabajo: "El ejercicio de las facultades que la ley le reconoce al empleador tiene como límite el respeto a las garantías constitucionales de los trabajadores, en especial cuando pudieran afectar la intimidad, la vida privada o la honra de estos." En base a esta última norma, la Dirección del Trabajo emitió un Oficio Ordinario 0260/0019 del 24 de enero de 2002, determinando que el empleador puede regular las condiciones, frecuencia y oportunidad del uso de los correos electrónicos de la empresa, pero en ningún caso podrá imponerse del contenido de los correos electrónicos del trabajador.

---

[31] su texto puede consultarse en http://www.habeasdata.org/ChileLeydePrivacidad/
[32] http://www.registrocivil.cl/f_institucion.html/ ó https://www.registrocivil.cl/OficinaInternet/servlet/MuestraPagina/
[33] 11/06/2002: http://www.anfitrion.cl/actualidad/20ulle/02061319812.html/
[34] 27/09/2001: http://www.anfitrion.cl/actualidad/20ulle/01100519759.html

5.2.3. Ecuador

La Ley 67 sobre Comercio electrónico y firma electrónica[35] dedica varios artículos a la protección de datos. Así el art. 9 reza: “Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.”

El artículo 32 sobre “Protección de datos por parte de las entidades de certificación de información acreditadas”[36], establece que “Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.”

En un “glosario”, que corresponde a la cláusula novena, explica: “el derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.” Sobre “Datos personales”, señala que “son aquellos datos o información

[35] puede descargarse en http://www.cpsr-peru.org/bdatos/ecuador/privacidad/Ley2002-67ecuador.pdf/view/ ó en http://www.corpece.org.ec/documentos/ley/ley_ce.doc/

[36] que forma parte del capítulo III “De las entidades de certificación de información”,

de carácter personal o íntimo, que son materia de protección en virtud de esta ley." "Datos personales autorizados" son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular."

Finalmente el art. 64, incorpora a continuación del numeral 19 del artículo 606 del Código Penal) el siguiente texto: "... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.".

También debe mencionarse la Ley de Control Constitucional[37], que atribuye al Tribunal Constitucional competencia para entender, entre otras materias, en los recursos de hábeas data (art. 12 inc. 3). El capítulo II está dedicado al Hábeas data, y en los artículos 34 a 45 se reglamenta el procedimiento.

El artículo 34 establece que "Las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener acceso a documentos, bancos de datos e informes que sobre sí mismas o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les esté por dar, podrán interponer el recurso de hábeas data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta Ley, por parte de las personas que posean tales datos o informaciones."

El artículo 35 dispone que el hábeas data tendrá por objeto: a) Obtener del poseedor de la información que éste la proporcione al recurrente, en forma completa, clara y verídica; b) Obtener el acceso directo a la información; c) Obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y, d) Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado, o no la ha divulgado.

[37] sancionada el 02/07/1997, http://www.uc3m.es/uc3m/inst/MGP/JCI/02-ecuador-leycontrolconstitucionalidad.htm/

En el año 2005, se aprobó la Ley 13 de “Burós de Información crediticia”[38], con el objeto de regular la constitución, organización, funcionamiento y extinción de los burós de información crediticia, cuya actividad exclusiva será la prestación de los se servicios de referencia crediticia. Volveremos sobre esta norma más adelante.

5.2.4. Paraguay

La Ley 1.682 de 2000 regula “la información de carácter privado” y fue modificada por la ley 1.969 del año 2002.[39]

La norma se plantea “regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general el tratamiento de datos personales, contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares” y aclara que “no se aplicará en ningún caso a las bases de datos ni a las fuentes de informaciones periodísticas ni a las libertades de emitir opinión y de informar.” (art. 1)

Más adelante ampliaremos el análisis de otros artículos.

5.2.5. Perú

La Ley 26.301[40] fue la primera norma luego modificada y complementada por otras normas. La ley 27.489 del 27 de junio de 2001, rige el funcionamiento de las centrales privadas de información de riesgos y la protección al titular de la información, regula el suministro de información de riesgos en el mercado, garantizando el respeto a los derechos de los titulares de la misma, reconocidos por la Constitución Política del Perú y la legislación vigente, promoviendo la veracidad, confidencialidad y uso apropiado de dicha información (arts. 9°, 10°, 12°, 13º, 14º. 15º, 16º, 7º, 18° (18.1,

---

[38] http://www.habeasdata.org/Ecuador-Ley-de-Buros-de-informacion-Informes-crediticios/

[39] La ley 1.682 es del 28/12/2000. La ley 1.969, del 23/08/2002, Gaceta Oficial Paraguay 06/09/2002, http://www.leyes.com.py/todas_disposiciones/2002/leyes/ley_1969_02.htm/.

[40] Ley 26.301 referida a la aplicación de la Acción Constitucional de Hábeas Data (El Peruano. Normas Legales, Lima, 08/05/1994, pág.122.750).

18.2).

La Ley 28.237 aprueba el Cód. Procesal Constitucional[41] y regula específicamente al hábeas data como proceso constitucional, en los artículos 61 a 65, además de las normas pertinentes a tal figura contenidas en los arts. 1° a 24 que componen el Título I del Código, bajo el siguiente rótulo: "Disposiciones generales de los procesos de hábeas corpus, amparo, hábeas data y cumplimiento".

Se citan también la ley de firmas y certificados digitales 27.269[42] y su modificatoria 27.310[43]; la ley que incorpora los delitos informáticos al Código Penal 27.309[44]; la ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y utilización de la firma electrónica 27.291[45]; la ley de notificación por correo electrónico 27.419[46]; la ley de microformas digitales Decreto Legislativo 681, Ley 26.612[47] y Decreto legislativo 827; y la ley de transparencia y acceso a la información pública 27.806[48]. Podemos agregar la Ley 28.493 sobre correo electrónico no deseado (Ley anti-spam).[49]

5.2.6. Venezuela

La ley orgánica de Amparo sobre derechos y garantías constitucionales[50] no

---

[41] publicada el 31/05/2004 y en vigor desde el 01/12/2004, http://www.congreso.gob.pe/ntley/Imagenes/Leyes/28237.pdf/

[42] publicada el 28/05/2000. Puede descargarse en: http://www.congreso.gob.pe/ntley/LeyNume.asp/

[43] publicada el 17/07/2000 modificada por art. 11, ley 27.269, ver web site nota anterior

[44] publicada el 17/07/2000, ver web site supra.

[45] publicada el 24/06/2000, ver web site supra:

[46] publicada el 07/02/2001, modifica el Código Procesal Civil peruano. ver web site supra.

[47] publicada el 21/05/1996, modifica el D. Leg 681, mediante el cual se regula el uso de tecnologías avanzadas en materia de archivo de documentos e información. ver sitio web citado supra.

[48] publicada el 03/08/2002, Ley de transparencia y acceso a la información pública. ver sitio web citado supra.

[49] 26/05/2005 puede consultarse en: http://lac.derechos.apc.org/?apc=21875se_1&x=4941757/

[50] http://www.mipunto.com/venezuelavirtual/leyesdevenezuela/leyesorganicas/leyorganica_deamparosobrederechosy_garantiasconstitucionales.html/

menciona expresamente a la protección de datos personales pero puede mencionarse la "Ley especial contra los Delitos Informáticos"[51], cuyo Capítulo III, relativo a los Delitos contra la Privacidad de las Personas y de las Comunicaciones, tipifica como delitos varias conductas referidas a la violación a la privacidad de los datos de carácter personal, las comunicaciones y su revelación indebida.

El artículo 20 titulado "Violación de la Privacidad de la Data o Información de Carácter Personal" establece: "Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero."

El artículo 21, referido a la "Violación de la Privacidad de las Comunicaciones", estipula que "Toda persona que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias".

Por último, el artículo 22, sobre "Revelación Indebida de Data o Información de Carácter Personal", establece que: "Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad".

[51] aprobada el 06/09/2001: http://www.tsj.gov.ve/legislacion/ledi.htm/

La Sala Constitucional del Tribunal Supremo de Justicia de Venezuela ha señalado, a propósito del ya citado artículo 28 de la Constitución, que “En el caso que se le niegue a una persona natural o jurídica el manejo de las bases de datos que contienen información sobre sí mismas o sobre bienes de su propiedad, lo procedente a los fines de intentar la protección de sus derechos, es incoar una acción de amparo que resuelva efectivamente la situación jurídica transgredida a través de su restitución; no obstante, si nos encontramos con el caso de que la información ya se conoce y el particular considera que la misma resulta errónea o inexacta, éste cuenta con la acción de habeas data para hacer valer, de ser procedente, el derecho que tiene a la constitución de una nueva situación jurídica, que no será mas que la corrección o eliminación de los datos que considera falsos o desactualizados.”[52] Y aclara que “(en Venezuela), la tendencia jurisprudencial, en especial la dictada por esta Sala, es concebir al habeas data como una acción constitucional garante del derecho que tiene todo ciudadano de rectificar, actualizar o destruir la información que resulte lesiva de sus derechos”.

Asimismo, ha explicado que “el llamado habeas data en general, no funciona en relación a expedientes personales de orden laboral que reposan en un archivo, a datos sueltos que alguien tenga sobre otro, anotaciones en diarios o papeles domésticos o comerciales, sino que funciona con sistemas no solo informáticos de cualquier clase de ordenación de información y datos sobre las personas o sus bienes, con fines de utilizarlos en beneficio propio o de otros, y que real o potencialmente pueden serlo en forma perjudicial contra aquellos a que se refiere la recopilación, se trata, por lo tanto, de bancos de datos, no referidos a alguien en particular, con independencia de que estén destinados a producir informaciones al público. Los registros objeto del habeas data, como todo registro, son compilaciones generales de datos sobre las personas o sus bienes ordenados de forma tal que se puede hacer un perfil de ellas, de sus actividades, o de sus bienes; los registros oficiales y los privados, objeto de la norma, tienen un sentido general, ellos están destinados a inscribir documentos, operaciones, actividades entre otros de las personas en determinados campos o temas, por lo que se trata de codificaciones de series de

[52] TSJ Venezuela, Sala Constitucional, 28/06/2006, expediente GP01-O-2004-000026, en http://www.tsj.gov.ve/decisiones/scon/Junio/1281-260606-05-1964.htm/

asuntos que forman patrones, matrices y asientos temáticos". "Así pues, los archivos electrónicos llevados por el Cuerpo de Investigaciones Científicas Penales y Criminalísticas, ya han sido considerados por esta Sala como recopilaciones de datos susceptibles de ser impugnados a través de la acción de habeas data".[53]

5.2.7. México

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[54] regula algunos aspectos de la protección de datos personales. El artículo 1º señala que la norma "tiene como finalidad proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal.", y en el artículo 2 establece que "Toda la información gubernamental a que se refiere esta Ley es pública y los particulares tendrán acceso a la misma en los términos que ésta señala". Aunque estos artículos parecen limitar el ámbito de la ley, diversos artículos han permitido construir una especie de estructura general de protección de los datos personales, tal como se muestra a continuación.

El artículo 3, entre otras definiciones, entiende por "Datos personales" a "La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad". y como "Sistema de datos personales" al conjunto ordenado de datos personales que estén en posesión de un sujeto obligado por la ley. El artículo 4, en uno de sus incisos, define como objetivo de la norma "Garantizar la protección de los datos personales en posesión de los sujetos obligados".

---

[53] En este caso, el actor solicitaba la eliminación de antecedentes penales que le impedían obtener trabajo, aunque el recurso fue rechazado por que los registros habían sido borrados -por un amparo anterior- e incumplimiento de requisitos formales de la Ley Orgánica de Tribunales.

[54] Sancionada en 2002 y en vigencia desde 2003. Texto actualizado en: http://www.diputados.gob.mx/LeyesBiblio/doc/244.doc/

El artículo 8 establece: “El Poder Judicial de la Federación deberá hacer públicas las sentencias que hayan causado estado o ejecutoria”, pero aclara que “las partes podrán oponerse a la publicación de sus datos personales”.

Además, contiene un capítulo específico (el cuarto), titulado “Protección de datos personales”, que abarca los artículos 20 a 26. El primero de ellos señala que “Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán: I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el artículo 61; II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido; III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el artículo 61; IV. Procurar que los datos personales sean exactos y actualizados; V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

El artículo 21 determina: “Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.”, aunque se acepta que “no se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos: II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran; III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos; IV. Cuando exista una

orden judicial; V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y VI. En los demás casos que establezcan las leyes".(art. 22)

Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto (IFAI) o de las instancias equivalentes previstas en el artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales (art. 23). Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante. La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el artículo 27 (art. 24).

El artículo 25 otorga un derecho de rectificación en: "Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones.

Finalmente, establece (artículo 26) que contra la negativa de entregar o corregir datos personales, procederá la interposición del recurso a que se refiere el Artículo 50. También procederá en el caso de falta de respuesta en los plazos a que se refieren los artículos 24 y 25.

El Instituto Federal de Acceso a la Información Pública (IFAI)[55] tiene una sección especial dedicada a la protección de datos personales[56], lo que no excluye que se hayan presentado varias iniciativas legislativas en procura de una ley específica.[57]

Existe también una ley especial para regular las Sociedades de Información Crediticia[58], que contiene cincuenta y ocho artículos, divididos en un Título Primero, capítulo único sobre Disposiciones Generales (arts. 1 a 4), el Título Segundo, con 5 capítulos: I De las sociedades de información crediticia (arts. 5 a 19); II De la base de datos (arts. 20 a 24); III De la prestación del servicio de información crediticia (arts. 25 a 37); IV De la protección de los intereses del cliente (arts. 38 a 50); V De las sanciones (arts. 51 a 56); VII Quitas y estructuras (arts. 57 y 58) y 5 artículos transitorios. Volveremos a comentar esta norma más adelante.

Además, pueden mencionarse, entre otras, las siguientes normas:

La Ley Federal de Responsabilidades de los Servidores Públicos[59], establece la obligación de los funcionarios para utilizar la información reservada a la que tenga acceso exclusivamente para los fines a que están destinados. Por otra parte, los servidores públicos tienen el deber de cuidar y custodiar la información a su cuidado, así como evitar su mal uso, destrucción, ocultamiento o utilización indebida.

El artículo 76 bis de la Ley Federal de Protección al Consumidor[60] regula lo que denomina “derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos”. “Artículo 76 bis: Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra

---

[55] http://www.ifai.org.mx/
[56] http://www.ifai.org.mx/datos_personales/
[57] ver por ejemplo Reyes Krafft, Alfredo Alejandro, “Protección de datos personales en México. Génesis legislativa” (Revista Derecho Informático - Alfa Redi 100, noviembre 2006) http://www.alfa-redi.com/rdi-articulo.shtml?x=7846/
[58] Sancionada el 27/12/2001, ver texto en: http://www.juridicas.unam.mx/
[59] Diario Oficial de la Federación del 13/03/2002. http://www.diputados.gob.mx/LeyesBiblio/doc/240.doc/
[60] http://www.diputados.gob.mx/LeyesBiblio/doc/113.doc/

tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente: I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente; II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos; III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones; IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella; V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor; VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población."

El artículo 210 del Código Penal Federal[61] dispone que "se impondrán de treinta a doscientas jornadas de trabajo en favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto."

[61] http://www.diputados.gob.mx/LeyesBiblio/doc/9.doc/

5.2.8. Uruguay

La Ley 17.838, de “Protección de Datos Personales a ser utilizados en Informes Comerciales”, y acción de "Habeas Data"[62] fue sancionada en 2004. Tenía dos partes, una dedicada a los informes comerciales, y la segunda que regulaba el derecho a la información a través del hábeas data, creando una autoridad de control, con 26 artículos.

En agosto de 2008, el Congreso uruguayo aprobó una nueva norma, bajo el número 18.331[63], cuyo artículo 1º declara que “el derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República[64].”

La ley uruguaya ampara por extensión a las personas jurídicas, en cuanto corresponda y es de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.

Se excluyen las bases de datos mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas; 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 y las bases de datos creadas y reguladas por leyes especiales.

Establece como principios generales del tratamiento de datos personales, los de legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad, que servirán también de criterio interpretativo para

---

[62] Sancionada el 24/09/2004 y publicada D.O. 01/10/2004 No. 26599, http://www.parlamento.gub.uy/Leyes/Ley17838.htm/

[63] Ley 18.331 de Protección de Datos Personales y Acción de "Habeas Data", 06/08/2008, D.O. Nº 27549, 18/08/2008, http://www.inau.gub.uy/biblioteca/documentos/Ley%20N%2018331.pdf/ y http://sip.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331&Anchor=/

[64] Art. 72 de la Constitución de la República Oriental del Uruguay: “La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno”.

resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes.

La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la ley y las reglamentaciones que se dicten en consecuencia. Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública. (Art. 6º. Principio de legalidad)

Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley. Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario. Cuando se constate la inexactitud o falsedad de los datos, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley. (Art. 7º. Principio de veracidad).

Esta norma presenta grandes similitudes con el Art. 4º de la LPDPA.

Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención y deberán ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados. La reglamentación determinará los casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo con la legislación específica, se conserven datos personales aun cuando haya perimido tal necesidad o pertinencia. (Art. 8º. Principio de finalidad).

Tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular. (Art. 8º).

El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse. El

referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 12 de la presente ley.

No se exigirá el previo consentimiento cuando los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación; se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; se trate de listados cuyos datos se limiten,en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento, y en el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma; cuando deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento; o se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico. (Art. 9º. Principio del previo consentimiento informado).

El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad. (Art. 10º. Principio de seguridad de los datos).

Aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros. Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia

competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular. Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos. (Art. 11. Principio de reserva).

La responsabilidad por la violación de las disposiciones de la ley recae en el denominado “Responsable de la base de datos o del tratamiento”, que es definido como la persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento (Art. 12. Principio de responsabilidad).

La ley otorga a los los titulares de los datos los derechos de información frente a la recolección de datos; de acceso, rectificación, actualización, inclusión o supresión (Arts. 13 a 15) y el derecho a la impugnación de valoraciones personales**.**

Este último consiste en que las personas no pueden verse sometidas a una decisión con efectos jurídicos que les afecte de manera significativa, que se base en un tratamiento automatizado o no de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad. En este caso, el afectado tendrá derecho a obtener información del responsable de la base de datos tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto. La valoración sobre el comportamiento de las personas, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado. (Art. 16).

Esta redacción supera en amplitud y claridad a la del Art. 20 de la LPDPA, ya que no la limita al ámbito de decisiones administrativas e incluye la inversión de la carga de la prueba.

Los operadores que exploten redes públicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos personales, adoptar las medidas técnicas y de gestiones adecuadas para preservar la seguridad en la explotación de su red o en

la prestación de sus servicios, con el fin de garantizar sus niveles de protección de los datos personales que sean exigidos por la normativa de desarrollo de esta ley en esta materia. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar. Esta regulación es sin sin perjuicio de lo previsto en la normativa específica uruguaya sobre telecomunicaciones relacionadas con la seguridad pública y la defensa nacional. (Art. 20**)**´

En materia de datos relativos a la actividad comercial o crediticia, el Art. 22 establece que "queda expresamente autorizado el tratamiento de datos personales destinados a brindar informes objetivos de carácter comercial, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor o en las circunstancias previstas en la presente ley. Para el caso de las personas jurídicas, además de las circunstancias previstas en la presente ley, se permite el tratamiento de toda información autorizada por la normativa vigente."

El plazo de caducidad de la registración se establece, cuando se trata de personas físicas en cinco años contados desde su incorporación, autorizándose que si al vencimiento de dicho plazo la obligación permanece incumplida, el acreedor pueda solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años. El nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original. Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción.

También se dispone que "los responsables de las bases de datos se limitarán a realizar el tratamiento objetivo de la información registrada tal cual ésta le fuera suministrada, debiendo abstenerse de efectuar valoraciones subjetivas sobre la misma."

Cuando se haga efectiva la cancelación de cualquier obligación incumplida

registrada en una base de datos, el acreedor deberá en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo al responsable de la base de datos o tratamiento correspondiente. Una vez recibida la comunicación por el responsable de la base de datos o tratamiento, éste dispondrá de un plazo máximo de tres días hábiles para proceder a la actualización del dato, asentando su nueva situación.

La autoridad de aplicación es la Unidad Reguladora y de Control de Datos Personales, que funciona como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica. Estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos.

Actúa asistido por un Consejo Consultivo estará integrado por cinco miembros: una persona con reconocida trayectoria en la promoción y defensa de los derechos humanos, designado por el Poder Legislativo, el que no podrá ser un Legislador en actividad; un representante del Poder Judicial; un representante del Ministerio Público; un representante del área académica y un representante del sector privado, que se elegirá en la forma establecida reglamentariamente.

La acción de protección de datos personales o Habeas data está regulada en los Arts. 37 a 45.

Esta ley derogó la 17.838 y debía ser reglamentada dentro de los 180 días de su promulgación.

Constituye, con la ley colombiana, la legislación más moderna de Sudamérica.

5.2.9. Colombia,

Con anterioridad a la ley aprobada en 2007 y declarada aplicable a fines de

2008, la Corte Constitucional había efectuado una interesante regulación pretoriana[65].

El 16 de octubre de 2008 la Corte Constitucional emitió la sentencia[66] mediante la cual efectuó la revisión de constitucionalidad del Proyecto de ley Estatutaria 27/06 del Senado y 221/07 Cámara, "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicio y las provenientes de terceros países y se dictan otras disposiciones".

La norma se conoce con el 1266/2008 de "Habeas Data" de Colombia[67] tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales, y se aplicará a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada. La norma recoge los denominados "Principios de Administración de Datos", entre los que se encuentran el principio de veracidad; el principio de finalidad; el principio de circulación restringida; el principio de temporalidad de la información; y el principio de seguridad.

Designa a la Superintendencia de Industria y Comercio para ejercer la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales que se regula.

Sin perjuicio de esta última norma existían diversas normas sectoriales que se ocupaban del tema. Así en el ámbito de la Administración de Justicia, el artículo 95 de la Ley 270 de 1996 (Estatutaria de la Administración de Justicia)[68] ordena que los

---

[65] Bajo la voz “autodeterminación informativa”, pueden consultarse los fallos relacionados en http://www.constitucional.gov.co/corte/

[66] Sentencia C 1011/08, en expediente PE 029 http://vlex.com/vid/colombia-ley-proteccion-datos-50034442.

[67] Publicada en el Diario Oficial 47.219 del 31/12/2008, http://basedoc.superservicios.gov.co/basedoc/leyes.shtml?x=69964/

[68] Diario Oficial 42.745, 15/03/1996. Texto actualizado en: http://www.cajpe.org.pe/rij/bases/legisla/colombia/ley51.HTM/

procesos que se tramiten con soporte informático garantizarán (...) “la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley”.

La Ley 527 de 1999 sobre “Comercio Electrónico y firmas digitales”[69], establece que las “Entidades de Certificación”, están obligadas a “garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor” (Literal c del artículo 32).

El artículo 31 de la ley 863 el 29 de diciembre de 2003[70], por la cual se establecen normas tributarias, aduaneras, fiscales y de control para estimular el crecimiento económico y el saneamiento de las finanzas públicas, modifica el artículo 799-1 del Estatuto Tributario, disponiendo lo siguiente: "Información a las centrales de riesgo. La información relativa al cumplimiento o mora de las obligaciones de impuestos, anticipos, retenciones, tributos y gravámenes aduaneros, sanciones e intereses, podrá ser reportada a las centrales de riesgo por la Dirección de Impuestos y Aduanas Nacionales. Tratándose de contribuyentes morosos, se reportará su cuantía a partir del sexto (6) mes de mora. Una vez cancelada la obligación por todo concepto, esta entidad deberá ordenar la eliminación inmediata y definitiva del registro en la respectiva central de riesgo." Esta norma fue declarada inconstitucional (“inexequible”) por Sentencia C-993/04, del 12/10/2004 de la Sala Plena de la Corte Constitucional[71]; se entendió que una norma que permite al organismo recaudador reportar la existencia de deudas fiscales a centrales de riesgo privadas debió ser tramitada a través de una Ley Estatutaria y no por intermedio de una Ley Ordinaria; por lo demás, el artículo afectó el núcleo esencial del Derecho Fundamental del habeas data, protegido por el art. 15 de la Constitución Colombiana.

La Resolución 575 del 9/12/2002 de la Comisión de Regulación de

---

[69] Su texto en http://www.corpece.org.ec/documentos/ley/colombia/ley_colombia_527-99.html/

[70] Su texto en http://www.actualicese.com/normatividad/2003/leyes/L863-03/L863-03.html/

[71] Expediente D-5134, demanda de inconstitucionalidad contra el Art. 31 de la Ley 863 de 2003. Actor: Karin Irina Kuhfeldt Salazar, http://www.habeasdata.org/colombia/ y en http://www.constitucional.gov.co/corte/

Telecomunicaciones (CRT)[72], dispone lo siguiente: “Reporte a Centrales de Riesgo. Los operadores de telecomunicaciones pueden remitir a una entidad que maneje y/o administre bases de datos, la información sobre la existencia de deudas a favor del operador, así como solicitar información sobre el comportamiento del suscriptor o usuario en sus relaciones comerciales, siempre y cuando el hecho generador de esa obligación sea la mora del mismo en el cumplimiento de sus obligaciones y el titular otorgue su consentimiento expreso para pasar información crediticia a un banco de datos al momento de la suscripción del contrato. El reporte a las centrales de riesgo debe ser previamente informado al suscriptor o usuario, con señalamiento expreso de la obligación en mora que lo ha generado, el monto y el fundamento de la misma. Dicha comunicación debe efectuarse con una antelación de por lo menos 10 días a la fecha en que se produzca el reporte. El reporte a las centrales de riesgo no podrá realizarse mientras no quede en firme la decisión sobre las reclamaciones pendientes que tenga el suscriptor o usuario. Los operadores deben reportar el pago a la central de riesgo a más tardar 10 días después del momento en que cese la mora. (Art. 7.1.11.)

La misma norma establece (articulo 7.1.2 Inviolabilidad de las comunicaciones) que los operadores de telecomunicaciones deben adoptar todas las medidas de seguridad requeridas para garantizar la inviolabilidad de las comunicaciones y de los datos personales de los usuarios. El secreto de las telecomunicaciones se extiende a las comunicaciones de voz, datos, sonidos o imágenes y a la divulgación o utilización no autorizada de la existencia o contenido de las comunicaciones. Salvo orden judicial competente, los operadores de telecomunicaciones no pueden permitir, por acción u omisión, la interceptación o violación de las comunicaciones que cursen por sus redes. Si la violación proviene de un tercero, el operador de servicio de telecomunicaciones debe tomar de inmediato las medidas necesarias para que la conducta cese y denunciar ante las autoridades competentes la presunta violación. Para efectos de la prevención y control de fraude en las telecomunicaciones, los operadores pueden intercambiar información sobre los usuarios.

En el sector bancario rigen Instrucciones impartidas por la Superintendencia

[72] http://gecti.uniandes.edu.co/docs/Res%20575%2002%20CRT.pdf/

Bancaria a las entidades financieras respecto del tratamiento de datos personales de los clientes, tales como la Circular Básica Contable y Financiera de la Superintendencia Bancaria[73], cuyo Capítulo II contienen las reglas relativas a la gestión del riesgo crediticio, que comentaremos más adelante.

5.2.10. El Salvador

La Constitución establece en el artículo 2, inciso segundo, que se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Entre las obligaciones de los proveedores de servicios de crédito, bursátiles o servicios financieros en general con los consumidores de los referidos servicios, el art. 19 de la ley de Protección al consumidor[74] menciona la de "proporcionar a solicitud del consumidor que sea prestatario, su historial crediticio, gratuitamente dos veces al año, y pagando una comisión, si el interesado lo requiere más veces que las indicadas; salvo que existan procesos judiciales pendientes entre proveedor y consumidor" (inc. i) e "informar por escrito al solicitante de un crédito, si éste lo requiere, los motivos por los cuales se le hubiese denegado el crédito solicitado" (inc. l).

El art. 21 dispone que "Las entidades especializadas en la prestación de servicios de información estarán obligadas a permitir al consumidor el acceso a la información de sus datos, así como a solicitar la actualización, modificación y eliminación de los mismos, de forma gratuita. Asimismo, tendrán la obligación de corregir la información falsa, no actualizada o inexacta en un plazo máximo de diez días contados a partir de la recepción de la solicitud del interesado.

Las entidades especializadas a las que se refiere el presente artículo, no podrán obtener ninguna clase de información personal del consumidor, si no es con la debida autorización de éste, y únicamente en las condiciones en que la misma haya sido conferida.

---

[73] Circular Externa 100/1995, http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/cir100.htm/
[74] Decreto 776/2005, http://www.defensoria.gob.sv/descargas/ley_proteccion_consumidor.pdf/

A su vez, el art. 42 que tipifica las infracciones leves, incluye como tal "Incumplir la obligación relativa a proporcionar el historial crediticio del consumidor a solicitud de éste, de acuerdo a lo establecido en el Art. 19, literal i); a menos que hubieren procesos judiciales pendientes entre proveedor y consumidor".

Entre las normas anteriores al articulado referido, se destaca el Reglamento General de la Ley Penitenciaria[75].

El artículo 19 sobre privacidad de datos del interno, determina: "La administración penitenciaria podrá dar información respecto a datos personales de internos, previo consentimiento por escrito de éste, a organismos o instituciones gubernamentales que justifiquen la utilidad de esta información, salvo a los jueces y al ministerio público cuando la información sea necesaria para el cumplimiento de sus propias funciones. Las transferencias internacionales de datos personales podrán efectuarse cuando se preste cooperación o auxilio policial, judicial o penitenciario de acuerdo a lo que regulen los tratados o convenios suscritos y ratificados por el estado de El Salvador. El destino de éstas deberá confirmarse."

El artículo 20, (datos personales especialmente protegidos) establece: "Los datos de carácter personal del interno, relativos a opiniones políticas, convicciones religiosas o filosóficas y sobre su salud, solamente podrán ser entregados o difundidos a personas, instituciones u organismos de carácter público o privado del país o del extranjero, previo consentimiento por escrito del interno; salvo que por razones de interés general lo disponga alguna ley. Cuando se solicite este tipo de datos, incluso por apoderado del interno, deberá presentarse a la administración la autorización en que conste el consentimiento del mismo, para poder accesar a aquéllos."

El artículo 21 (rectificación o complementación de datos personales) dice: "El interno podrá solicitar a la administración la rectificación o complementación de los datos personas o la información que conste en su expediente y en los registros o ficheros penitenciarios, cuando éstos sean inexactos o incompletos, presentando la documentación probatoria correspondiente. de la rectificación o complementación

[75] Decreto 95 del 14/11/2000, http://www.oas.org/juridico/spanish/gapeca_sp_docs_slv2.pdf/

efectuada deberá informarse al interesado a más tardar quince días después de presentada la solicitud al director del centro penitenciario."

El artículo 22 (garantía de confidencialidad de los datos e informaciones) estipula: "Los funcionarios y empleados responsables de los expedientes, registros o ficheros penitenciarios, deberán adoptar las medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos e informaciones que aquéllos contienen, así como para evitar su alteración, pérdida o acceso no autorizado; y estarán obligados, junto con quienes trabajen con esos datos e informaciones, a guardar confidencialidad sobre los mismos, incluso después que haya terminado la relación del interno con la administración penitenciaria, respondiendo penalmente por los delitos que cometieren en el manejo de la información".

5.2.11. Panamá

No hay una norma general de protección de datos, pero existen normas sectoriales.

Ley 6 de 22 de enero de 2002[76] dicta normas para la transparencia en la gestión pública y establece la acción de habeas data, que sólo es procedente ante las entidades públicas o privadas que, por concesión, brinden servicios públicos. Puede ser ejercida por un tercero interesado, sin necesidad de sustentar justificación o motivación alguna (habeas data indirecto). La acción se tramita con el mismo procedimiento que la acción de Amparo de garantías constitucionales. Los perjudicados tiene el derecho a que la información incorrecta o desfasada o irrelevante se corregida o eliminada. Fue reglamentada por Decreto Ejecutivo 124 de mayo de 2002[77].

La Ley 24 de mayo de 2002[78] por la cual se regula el servicio de información sobre solvencia de crédito, se aplica a la actividad de las personas, públicas o privadas, naturales o jurídicas, que se dediquen a manejar datos sobre solvencia

[76] G.O. 24.476, 23/01/2002, http://www.bibliojuridica.org/libros/3/1156/30.pdf/
[77] G.O. 24.557, 22/05/2002,
[78] G.O. 24.559, 23/05/2002,
http://www.asamblea.gob.pa/NORMAS/2000/2002/2002_522_0698.PDF/

económica o historial de crédito por cualquier medio tecnológico o manual.

Esta ley ha sido modificada por la ley 14 de 2006[79], que ha sustituido, entre otros artículos, el referido a "calidad de los datos", en los siguientes términos: "Artículo 4. Calidad de los datos. Los datos sobre historial de crédito, brindados por los consumidores o clientes o por los agentes económicos, los manejados por las agencias de información de datos y los generados por transacciones de carácter económico, financiero, bancario, comercial o industrial, deberán ser exactos y actualizados, de forma que respondan con veracidad a la situación real del consumidor o cliente. Con este propósito, los datos que manejen y comuniquen los agentes económicos y las agencias de información de datos reflejarán el movimiento de los pagos, los abonos y las cancelaciones de las obligaciones del consumidor o cliente, así como cualquier otra información producto del tratamiento de los datos de este, que faciliten la comprensión y el análisis de su historial de crédito".

5.2.12. Costa Rica

Si bien no tiene una norma específica sobre protección de datos, cuenta con una abundante jurisprudencia de la Sala Constitucional de la Suprema Corte de Justicia[80]. Es frecuentemente citada como precedente una sentencia de 1999[81] en la que se afirmó: "los derechos de intimidad y de autodeterminación informativa tienen como núcleo fundamental de protección la persona humana, son derechos de defensa e implican ante todo un derecho de autodeterminación. El reconocer a la persona el derecho de controlar la información que le corresponde, el derecho de impedir que terceros obtengan conocimiento o manejen dicha información y el derecho de rectificación ha surgido ante la necesidad de evitar que un tercero pueda ejercer un control sobre la persona, control que la colocaría en situación de objeto o en situaciones que resulten contrarias a la dignidad de la persona humana."

---

[79] http://www.asamblea.gob.pa/NORMAS/2000/2006/2006_547_1508.PDF/
[80] Sistema Costarricense de Información Jurídica (SCIJ), http://200.91.68.20/scij/busqueda/jurisprudencia/jur_repartidor.asp/
[81] Suprema Corte de Justicia de Costa Rica, Sala Constitucional, resolución N° 5802-99 27/07/1999, citada entre otros por el Dictamen de la Procuraduría General 76 de 21/02/2005, publicado en: http://www.pgr.go.cr/Scij/Busqueda/Normativa/Pronunciamiento/pro_ficha.asp?param6=1&nDictamen=13006/, entre otros.

Esta doctrina jurisprudencial se ha mantenido, refiriéndose a la autodeterminación informativa, a la calidad de los datos, y en general sigue los mejores principios en la materia.[82]

En otro pronunciamiento sobre la publicación de datos crediticios en el sitio web del Poder Judicial[83] la Sala Constitucional ha señalado sobre el derecho a la autodeterminación informativa, que "la ampliación del ámbito protector del Derecho a la intimidad surge como una respuesta al ambiente global de fluidez informativa que se vive. Ambiente que ha puesto en entredicho las fórmulas tradicionales de protección a los datos personales, para evolucionar en atención a la necesidad de utilizar nuevas herramientas que permitan garantizar el derecho fundamental de los ciudadanos a decidir quién, cuándo, dónde y bajo qué y cuáles circunstancias tiene contacto con sus datos. Es reconocido así el derecho fundamental de toda persona física o jurídica a conocer lo que conste sobre ella, sus bienes o derechos en cualquier registro o archivo, de toda naturaleza, incluso mecánica, electrónica o informatizada, sea pública o privada; así como la finalidad a que esa información se destine y a que sea empleada únicamente para dicho fin, el cual dependerá de la naturaleza del registro en cuestión. Da derecho también a que la información sea rectificada, actualizada, complementada o suprimida, cuando la misma sea incorrecta o inexacta, o esté siendo empleada para fin distinto del que legítimamente puede cumplir. Es la llamada protección a la autodeterminación informativa de las personas, la cual rebasa su simple ámbito de intimidad. Se concede al ciudadano el derecho a estar informado del procesamiento de los datos y de los fines que con él se pretende alcanzar, junto con el derecho de acceso, corrección o eliminación en caso el que se le cause un perjuicio ilegítimo.[84]" Y agrega: "El derecho de autodeterminación informativa tiene como base los siguientes principios: el de transparencia sobre el tipo, dimensión o fines del

---

[82] Entre otras podemos citar la sentencia 08996/2002 sobre informes de juicios por una empresa de informes crediticios;

[83] CSJ Costa Rica, Sala Constitucional, Sentencia 12695/2003, "R. M. A. vs. Presidente de la Corte Suprema de Justicia y el Jefe del Departamento de Tecnología de Información del Poder judicial", http://200.91.68.20/scij/busqueda/jurisprudencia/jur_repartidor.asp/

[84] reiterado en Sentencia 2006-09834 (Exp: 06-005927-0007-CO) del 07/07/2006, http://200.91.68.20/scij/busqueda/jurisprudencia/jur_repartidor.asp/, entre muchas otras.

procesamiento de los datos guardados; el de correspondencia entre los fines y el uso del almacenamiento y empleo de la información; el de exactitud, veracidad, actualidad y plena identificación de los datos guardados; de prohibición del procesamiento de datos relativos a la esfera íntima del ciudadano (raza, creencias religiosas, afinidad política, preferencias sexuales, entre otras) por parte de entidades no expresamente autorizadas para ello; y de todos modos, el uso que la información se haga debe acorde con lo que con ella se persigue; la destrucción de datos personales una vez que haya sido cumplidos el fin para el que fueron recopilados; entre otros."

En el mismo fallo, que reitera anteriores pronunciamientos se refiere que "La esfera privada ya no se reduce al domicilio o a las comunicaciones, sino que es factible preguntarse si es comprensible incluir "la protección de la información" para reconocerle al ciudadano una tutela a la intimidad que implique la posibilidad de controlar la información que lo pueda afectar. Lo expuesto, significa que el tratamiento electrónico de datos, como un presupuesto del desarrollo de nuestra actual sociedad democrática debe llevarse a cabo afianzando los derechos y garantías democráticas del ciudadano (arts. 24, 1, 28, 30, 33 y 41 de la Constitución). Es obvio, que el acceso a la información es un poderoso instrumento de progreso individual, y para el ejercicio de los derechos políticos y sociales. Pero también debe reconocerse que el progreso no significa que los ciudadanos deban quedar en situación de desventaja frente al Estado o a los particulares. El nuevo derecho a la intimidad debe ponderar los intereses en conflicto, entre el legítimo interés de la sociedad a desarrollarse utilizando la información, como la también necesidad de tutelar a la persona frente al uso arbitrario de sus datos personales. La tutela a la intimidad implica la posibilidad real y efectiva para el ciudadano de saber cuáles datos suyos están siendo tratados, con qué fines, por cuáles personas, bajo qué circunstancias, para que pueda ejercer el control correspondiente sobre la información que se distribuye y que lo afecta (arts. 24 de la Constitución y 13 inciso 1, de la Convención Americana de Derechos Humanos)." Y añade: "Ha quedado claro que la información que respecto de una persona sea almacenada, además de no poder ser de carácter estrictamente privado, debe ser exacta".

Remitiéndose a un fallo precedente[85] destaca que “siendo la exactitud uno de los requisitos de la información que las bases de datos pueden guardar de las personas, la falta de elementos suficientes para identificar unívocamente a la persona investigada, puede ocasionarle graves perjuicios. En ese sentido, el artículo 93 de la Ley Orgánica del Tribunal Supremo de Elecciones y del Registro Civil, número 3504, de diez de mayo de mil novecientos setenta y cinco y sus reformas, confiere a la cédula de identidad ese carácter. Por lo anterior, este tribunal considera que las empresas administradoras de datos personales tienen la obligación ineludible de verificar que las informaciones almacenadas a nombre de una persona hayan sido obtenidas de forma tal que no quepa duda acerca de la titularidad del afectado, es decir no basta con la advertencia que plantea la empresa recurrida de indicar al afiliado que corre por su cuenta verificar la titularidad de la persona consultada . En razón de lo que dispone el artículo 140 del Código Procesal Civil, en relación con el 243 de la Ley Orgánica del Poder Judicial, en el sentido de que los abogados y sus asistentes debidamente acreditados tienen acceso a los expedientes judiciales, las empresas encargadas de almacenar datos referentes a procesos jurisdiccionales están en la obligación de verificar la exactitud de los datos que registran, estableciendo con claridad –por medio de una revisión del legajo o de una certificación expedida en el despacho- el nombre completo y número de cédula del demandado, y sólo entonces incluirlo en sus registros. Si el afectado solicita por escrito la exclusión de los datos que a su nombre aparezcan y que sean inexactos por indeterminación de la cédula del deudor, la empresa protectora de crédito debe proceder a verificar la exactitud de las informaciones, en los términos antes dichos, o bien a eliminarlos de su base de datos…"

Finalmente, también puede mencionarse el artículo 10 de la Ley 7839 del Sistema de Estadística Nacional[86] que establece: “En todo caso, serán de aportación estrictamente voluntaria y sólo podrán recabarse previo consentimiento de los interesados, los datos susceptibles de revelar las opiniones políticas, las convicciones religiosas o ideológicas, la preferencia sexual y, en general, cuantas circunstancias puedan afectar la intimidad personal”.

---

[85] CSJ Costa Rica, Sala Constitucional, Sentencia 2000-01119, 01/02/2000
[86] http://asamblea.racsa.co.cr/ley/leyes/7000/7839.doc/

5.3. Otros países

5.3.1. Canadá

Existen dos leyes federales sobre privacidad: la *Privacy Act*[87] y la Ley de Protección de documentos e información electrónica. La primera entró a regir el 1 de julio de 1983, e impone a los departamentos gubernamentales y agencias federales respetar el derecho a la privacidad, limitando la recolección, el uso y el acceso de la información personal. Otorga el derecho de acceso y a solicitar la corrección de los datos personales que estén registrados en estas oficinas del gobierno federal.

La otra ley (*Personal Information Protection and Electronic Documents Act - PIPEDA*), de abril del año 2000[88], en vigencia desde el 1 de enero de 2001, establece los principios básicos a observar por las organizaciones del sector privado para poder recoger, utilizar o divulgar información personal en el curso de actividades comerciales. La ley otorga a los titulares de datos los derechos de acceso y rectificación de los datos personales que estas organizaciones pudieron haber recogido sobre ellos. Inicialmente, esta ley se aplicó solamente a la información personal sobre clientes o empleados recogida, utilizada o divulgada en el curso de actividades comerciales por el sector privado federal regulado, de organizaciones tales como bancos, líneas aéreas, y compañías de las telecomunicaciones. Actualmente se aplica a la información personal recogida, usada o divulgada por el sector minorista, empresas de publicidad, industrias, e incluso las organizaciones provincialmente reguladas. No rige con relación a los datos personales de empleados de dichas organizaciones provincialmente reguladas. El gobierno federal puede eximir a las organizaciones o actividades en las provincias que tienen sus propias leyes de protección de datos, si son substancialmente similares a la ley federal. La *PIPEDA* tiene vigencia en esas provincias para el sector privado federal regulado, y en transacciones interprovinciales e internacionales. El Comisionado Federal (*Privacy*

[87] http://www.privcom.gc.ca/legislation/02_07_01_01_e.asp#001/
[88] Personal Information Protection and Electronic Documents Act (PIPEDA) http://laws.justice.gc.ca/en/ShowFullDoc/cs/P-8.6///en/, entró en vigencia el 10/12/2000.

Commissioner) de Canadá es la autoridad de aplicación[89].

Cada provincia y territorio de Canadá tiene legislación sobre privacidad regulando la recolección, uso y acceso de la información personal realizados por agencias estatales. Terranova y Labrador han aprobado la legislación, pero no está todavía en vigor. Estas leyes otorgan en general el derecho de tener acceso y de corregir su información personal. Las infracciones se denuncian ante una comisión independiente o el ombudsman autorizado a recibir y a investigar quejas. Columbia Británica, Alberta y Quebec son las únicas provincias con leyes reconocidas como substancialmente similares a PIPEDA[90].

El Código Civil de Quebec, Canadá de 1991[91], regula la protección de datos personales en el Libro I "Personas", Título II, Capítulo 3 titulado "Respeto de la reputación de la privacidad", en los artículos 35 a 40. Existe una ley que desarrolla esta normativa[92]

5.4. Organización de Estados Americanos (OEA)

En la Organización de los Estados Americanos (OEA), existe un anteproyecto de Convención Americana para la Autodeterminación Informativa[93], cuyo artículo 1º reza: "Objeto y fin. El fin de la presente Convención es garantizar, en el territorio de cada Estado Parte a cualquier persona física o jurídica sean cuales fueren su nacionalidad, residencia o domicilio, el respeto de sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa con relación a su vida privada y demás derechos de la personalidad; asimismo, la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos

[89] Mediante la Decisión de la Comisión del 20/12/2001 se consideró que esta norma se adecua a la Directiva 95/46/CE. [notificada con el número C(2001) 4539] (2002/2/CE) Diario Oficial N° L 002, 04/01/2002, p. 0013 – 0016.
[90] ver índice de links en: http://www.privcom.gc.ca/prov/index_e.asp/
[91] http://www.lexum.umontreal.ca/ccq/en/. Ver Masciotra, ob.cit. supra, quien traduce los arts.37 a 41.
[92] An Act respecting the protection of personal information in the private sector (Quebec) .S.Q., chapter P-39.1, http://www.canlii.org/qc/laws/sta/p-39.1/20061117/whole.html/
[93] El anteproyecto se difundió en el año 2000 y originalmente lo tomamos de http://www.ulpiano.com/convencion.htm, página discontinuada. También lo cita http://lac.derechos.apc.org/legislacion/completo.shtml?x=9046/.

correspondientes a su persona o bienes."

En el capítulo de "Garantías judiciales", se prevé el derecho de toda persona a un "recurso" sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que los ampare contra actos que violen sus derechos fundamentales reconocidos por la Convención, la Constitución de los Estados Partes o la ley (art. 12.1). Para tal fin consagra el derecho de toda persona a controlar sus datos personales existentes en ficheros públicos o particulares, señalando que la garantía y el procedimiento judiciales para ejercer tal control es el hábeas data (art. 12.2). Además, y si bien defiere al derecho interno de los Estados la regulación de la naturaleza constitucional o común de tal recurso, indica que en todo caso éste debe ser su medio de amparar en forma expedita, rápida y eficaz los derechos de la persona ante los excesos informáticos automatizados o manuales (art. 12.3).

5.5. Legislación de otros países fuera del continente americano

5.5.1. Australia

Las dos leyes más importantes que regulan la protección de datos son la *FOIA* de 1982 y la *Privacy Act* de 1988.

La primera de ellas prevé que "cuando una persona considera que un documento a que ha accedido en términos de dicha ley es incompleto, incorrecto, desnaturalizado o engañoso y va a ser usado por la agencia con fines administrativos, puede solicitar su rectificación o una anotación de su solicitud de rectificación".[94]

La Ley Federal de Privacidad, 119 de 1988 (*Privacy Act*) contiene once principios sobre privacidad de la información (*IPPs*) que se aplican en la Commonwealth y rigen en los organismos públicos estatales. También tiene diez principios nacionales en materia de privacidad (*NPPs*) que rigen tanto en el sector privado como en todos los proveedores de servicios médicos. La parte IIIA de la Ley Federal de Privacidad regula los servicios de crédito y los informes que divulgan las agencias. La Comisión sobre Privacidad también tiene algunas funciones reguladoras

[94] Masciotra, ob.cit. supra.

en el marco de otras leyes, tales como la de Telecomunicaciones de 1997, la Ley Nacional de Salud de 1953, la ley de entrecruzamiento de datos para fines impositivos de 1990 (Cth) e incluso el Código Penal de 1914.[95]

Algunos estados de Australia han dictado también leyes protectoras de la privacidad, como Nueva Gales del Sur, Queensland, Victoria, Tasmania, Australia del Sur, Australia del Oeste, el Territorio del Norte y el distrito Capital.[96]

5.5.2. Cooperación Económica de Asia-Pacífico (APEC.

Los trabajos en materia de privacidad de APEC[97] se centraron en la creación de un Marco de Privacidad (APEC Privacy Framework) como un aspecto de protección de derechos humanos y libertades fundamentales, enfatizando, al mismo tiempo, que la falta de una legislación adecuada en la materia, atrae la desconfianza de los consumidores y los usuarios de comunicaciones, y de otras tecnologías de la información, lo cual finalmente entorpece el comercio y afecta la economía de las naciones.

Específicamente, su enfoque distintivo es concentrar su atención en el equilibrio entre la privacidad de la información y las necesidades de los negocios comerciales, convirtiéndose en el instrumento internacional de mayor importancia que orienta en la materia a los principales cuerpos normativos del mundo.

Estos principios son:

"Preventing Harm", o de prevención de daño. Debe reconocerse el interés del individuo a sus expectativas legítimas de privacidad, por lo que la legislación debe prevenir y sancionar el uso ilegítimo de la información.

"Notice", o de obligación de dar aviso. Los sujetos obligados por la legislación

---

[95] http://www.privacy.gov.au/act/index_print.htm/
[96] pueden consultarse en http://www.privacy.gov.au/privacy_rights/laws/index.html/
[97] http://www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html/

deben dar aviso en términos claros y entendibles a los titulares de la información, respecto de las prácticas de privacidad de los que gozará la información que compartan. Esto incluye i) La mención de que se recaban datos personales; ii) La descripción de para qué se recolecta la información, con qué propósitos o fines; iii) Los tipos de personas u organizaciones a quienes podría compartirse la información; iv) La identidad y domicilio de la persona que recolecta la información, incluyendo la posibilidad de que dicho sujeto obligado sea contactado para realizar consultas sobre sus prácticas y políticas de privacidad; y v) Las opciones que se ofrezcan al titular respecto del uso o divulgación de la información que proporcione.

"Collection Limitation" o de limitación a la recolección de información personal. La recolección de datos personales debe limitarse al alcance que sea relevante para los propósitos por los cuales se recaba la información.

En todo caso, la información debe obtenerse por medios lícitos y, cuando así lo requiera la ley, con conocimiento o consentimiento de sus titulares.

"Uses of Personal Information", o de usos de la información o datos personales. La información o datos personales que se recaben de sus titulares, debe ser usada de acuerdo con los propósitos que motivaron su recolección, o con propósitos compatibles, excepto en aquellos casos en que: i) Se cuente con el consentimiento del titular para fines diferentes; ii) El uso es necesario para proporcionar un servicio al titular, de acuerdo con relaciones previas entre el receptor y el titular; o iii) Cuando así lo requiera la ley.

"Choice" o de presentación de opciones. Los titulares deben recibir opciones claras y entendibles respecto del alcance que puede darse en el uso de sus datos, para fines distintos de aquellos por los cuales se recaba la información. Estas opciones o restricciones no deben existir cuando la información se recabe de fuentes de acceso público.

"Integrity of Personal Information" o de preservación de la integridad de datos personales. La información personal que se mantenga de los individuos por parte de los sujetos obligados, debe ser adecuada, completa y actual, de acuerdo con los propósitos para los cuales se recaba.

"Security Safeguards", o de salvaguardas de seguridad. Los sujetos obligados en el contexto de la ley que mantengan registros de datos personales deben manejarlos con estándares humanos y técnicos razonables que protejan la privacidad de la información, y que prevenga su destrucción, uso, modificación o divulgación no autorizados.

"Access and Correction", o de acceso y derecho de corrección. Los titulares de información personal deben tener derecho a: *(i)* Obtener confirmación por parte de los sujetos obligados por la ley, respecto de si tienen o no información personal que les concierna; *(ii)* Que se les haga saber la información que tengan en su conocimiento, en un tiempo y a un costo razonable, con medios adecuados que les permita entenderla; y (*iii*) Controvertir la exactitud de la información y, en su caso, solicitar su rectificación.

"Accountability" o de responsabilidad. Todo sujeto obligado en el contexto de la ley, debe ser responsable de la observancia de las disposiciones legales o regulatorias tendentes a la protección de la privacidad y uso legítimo de datos personales.

En mi opinión, este capítulo también debería terminar con un parágrafo que brevemente marque las características comunes encontradas en la legislación de América Latina, o como mínimo, señalar que los países en los que la cuestión ha merecido una regulación más específica, mas general, etc.

5.6. Síntesis

Varias constituciones de los países de América Latina, con enfoques a veces distintos, han incorporado el derecho a acceder y en su caso obtener su rectificacion o modificación, de los datos personales, ya sea bajo la vía procesal del denominado hábas data, como una variante de la tutela del derecho a la intimidad, o con mayor grado de desarrollo, en los términos del moderno concepto de autodeterminación informativa.

Este proceso es relativamente reciente y se inicia a fines de los ochenta en Brasil y se ha ido desarrollando en mediados de la última década del siglo pasado, en Colombia, Perú, Paraguay, Ecuador, Venezuela, Guatemala, Nicaragua, Bolivia y Honduras, por lo menos hasta el momento de escribir este documento.

En cuanto a las legislaciones nacionales, su orientación es más diversa. Brasil ha reglamentado el procedimiento de habeas data, pero luego ha incorporado en el Código de defensa del consumidor reglas asimilables al principio de calidad de los datos.

Las normas de Chile, Colombia, Paraguay y Uruguay al estilo de la ley argentina, efectúan una regulación general del tratamiento de datos personales.

Perú no solo ha reglamentado el habeas data, sino que ha sancionado normas en materia de centrales de informes crediticios, lo mismo que México.

Panamá, Venezuela, El Salvador y Panamá en cambio, han destinado su legislación, con diverso alcance, a los informes crediticios o de solvencia.

Aunque el proceso latinoamericano está menos extendido que el europeo, el tema de la protección de datos está presente en la agenda de la mayoría de los países, independientemente de la existencia o no de legislación específica.

En tal sentido, la Red Iberoamericana de Protección de Datos, constituída en 2003, a impulso de la Agencia Española de Protección de Datos, en su VI encuentro, llevado a cabo en el 2008[98] aprobó una declaración que reproducimos a continuación y que da cuenta de lo expresado precedentemente.

La mencionada declaración aprobada en la ciudad de Cartagena (Colombia) en mayo de 2008, dice así:

"El derecho fundamental a la protección de datos personales presenta como uno de sus rasgos más característicos el de la amplitud de sus efectos. Esta característica es consecuencia de que el tratamiento y uso de la información personal se produce en todo tipo de actividades públicas o privadas desde el nacimiento de la persona. Y afecta a todas las facetas de la persona entre las que destacan su perfil

98 https://www.agpd.es/portalweb/internacional/red_iberoamericana/encuentros/VI_Encuentro/index-ides-idphp.php/

educativo, socioeconómico, laboral, sanitario, ideológico, religioso o cultural. E incluso permite deducir perfiles derivados de sus hábitos como usuario de nuevos desarrollos tecnológicos.

Por otra parte, el tratamiento de datos personales se ha multiplicado vertiginosamente en el marco de un mundo globalizado. El desarrollo económico global lleva consigo un nuevo impulso de los flujos internacionales de datos que son tratados en entornos geográficos con regulaciones diversas que ofrecen distintos niveles de garantía a las personas.

Junto a ello el desarrollo tecnológico y de nuevos servicios de la sociedad de la información ha ampliado las opciones de intercambio de información entre las personas y de acceso a la misma poniendo en jaque los criterios tradicionales de garantía de la protección de datos y la privacidad, que deben adaptarse a los nuevos retos que se plantean.

La globalización ha incidido, también, en el desarrollo de nuevas formas de criminalidad y, especialmente, en la lucha contra el terrorismo generando mayores exigencias de seguridad que deben hacerse compatibles con el respeto a los derechos fundamentales.

El tratamiento masivo y selectivo de la información personal en el marco descrito debe ser legítimo, proporcionado a las finalidades que lo justifican y llevarse a cabo con garantías de confidencialidad y seguridad que impidan el acceso a la información por terceros no autorizados.

Las personas deben estar informadas sobre quienes y para qué se utilizan sus datos personales.

Y tienen que poder reaccionar frente a usos ilegítimos ejerciendo sus derechos. En particular, esta capacidad reactiva debe permitirles evitar el mantenimiento secular y universal en la red de la información que les afecta. Para ello deben poder solicitar su tutela efectiva por parte de instituciones apropiadas.

Dar una respuesta adecuada para la protección de la información personal hace necesario impulsar la adopción de estándares internacionales que ofrezcan a las personas, cualquiera que sea el lugar en que se traten sus datos, garantías del

siguiente tenor:

1. Los datos personales deben ser obtenidos y tratados de modo leal y lícito, respetando, como regla general, el poder de decisión de la persona sobre la información que le afecta.

2. Las personas han de ser educadas en la protección de sus datos y estar informadas sobre quién y para qué fines se tratan sus datos.

3. Los fines del tratamiento de datos serán específicos y concretos.

4. El tratamiento de datos ha de ser proporcionado a los fines que lo justifican.

5. Los datos personales deben ser exactos y veraces.

6. Es preciso identificar categorías de datos que por su mayor sensibilidad exijan una protección reforzada.

7. Es preciso garantizar la confidencialidad y la seguridad de la información personal.

8. Las personas deben tener la posibilidad de conocer qué información se trata, rectificarla si es inexacta, obtener su cancelación si es innecesaria y oponerse a su tratamiento.

9. Las limitaciones a las anteriores garantías han de fundarse en razones de interés público.

10. Debe preverse una autoridad que permita que estas garantías sean efectivas."

La Red Iberoamericana de Protección de Datos, consciente de la urgencia de avanzar en esta dirección, ha debatido en el VI Encuentro celebrado en Cartagena de Indias (Colombia) sobre los nuevos retos que están planteados con participación de instituciones, expertos y representantes de entidades privadas de países iberoamericanos y de otras áreas.

Asimismo ha constatado los avances normativos impulsados en diversos

países latinoamericanos para dotarse de nuevas garantías en la protección de los datos personales. Iniciativas que suponen un impulso adicional en el proceso de alcanzar estándares de protección de un mundo global.

En el mismo sentido, el Convenio 108 del Consejo de Europa, abierto a la ratificación de Estados no europeos, sigue siendo un referente para garantizar una protección adecuada de la información personal.

La Red Iberoamericana de Protección de Datos hace un llamamiento a las conferencias internacionales relacionadas con la protección de datos y la privacidad, cualquiera que sea su ámbito geográfico, para que incluyan en su agenda el impulso a unos estándares de protección de datos que puedan culminar en la adopción de un instrumento jurídico común por parte de las Organizaciones internacionales competentes".

Capítulo 6. Principios rectores del tratamiento de los datos personales

Sumario. Licitud. Calidad. Consentimiento. Conocimiento o información. Derecho de acceso. Derechos de actualización, rectificación y supresión. Elaboración de perfiles. Cesión de datos.

El ya mencionado Convenio 108 de Estrasburgo estableció un conjunto de principios básicos para la protección de los datos de carácter personal, bajo el rótulo de "calidad de los datos"[1].

Estos principios han sido mantenidos y actualizados en la más reciente normativa europea, que es la Directiva 95/46 del Parlamento Europeo y del Consejo, relativa a la "Protección de las personas físicas en lo que respecta al Tratamiento de Datos personales y a la libre circulación de estos datos"[2].

6.1. Licitud

En virtud de esta normativa, los Estados europeos deben prever que los datos personales sean "tratados de manera leal y lícita"; y que sean "recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines", aclarando que "no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y

---

[1] Especialmente en el Art. 5º. Calidad de los datos.- Los datos de carácter personal que sean objeto de un tratamiento automatizado: a) se obtendrán y tratarán leal y legítimamente; b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; d) serán exactos y si fuera necesario puestos al día; e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

[2] Directiva 95/46/CE del Parlamento Europeo y del Consejo, 24/10/1995, relativa a la "Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", Diario Oficial N° L 281, 23/11/1995, p. 0031 – 0050. En Legislación comunitaria vigente: documento 31995L0046, cons. http://europa.eu.int/

cuando los Estados miembros establezcan las garantías oportunas"[3].

En nuestro país este principio ha sido receptado en la ley 25.326 con la siguiente redacción: “La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley” (art. 4º inciso 2).

6.2. Calidad.

El Convenio 108 también establece que los datos deben ser "adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente"[4]. Deben ser "exactos y, cuando sea necesario, actualizados, debiendo tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados"[5].

En la Argentina, la ley 25.326 ha reproducido este concepto del siguiente modo: “Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para

---

[3] Artículo 6 (principios relativos a la calidad de los datos).- “1. Los Estados miembros dispondrán que los datos personales sean: a) tratados de manera leal y lícita; b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas; c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos. 2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.”

[4] Artículo 6 inciso c) ut supra transcripto.

[5] Artículo 6 inciso d) ut supra transcripto.

los que se hubieren obtenido" (art. 4º inciso 1) y "Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario" (art. 4º inciso 4).

Los datos deben ser conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente, aunque se admite que "los Estados miembros establezcan las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos".

Es importante destacar que los responsables del tratamiento, es decir la persona física o jurídica que gestiona u opera el procesamiento de la información, son quienes están encargados de garantizar el cumplimiento de estos principios de calidad[6].

6.3. Consentimiento

El consentimiento del titular de los datos ha sido considerado un pilar del sistema de protección de datos personales[7], toda vez que constituye la condición justificante de las operaciones de tratamiento a que pueden ser sometidos los datos[8], sin la cual las mismas quedan teñidas de ilicitud.

La Directiva 46/95, ya citada, se ocupa de este principio bajo el rótulo de

---

[6] Artículo 6 inciso e) ut supra transcripto.

[7] Peyrano, Guillermo F., "El principio del consentimiento en el sistema de protección de datos personales. Condiciones de validez y posibilidad de revocación del consentimiento prestado. El derecho de oposición", Zeus, t. 92, 7/7/2003, año XXX, http://www.editorial-zeus.com.ar, Sección Colección Zeus - Doctrina, documento nº 00562. En el mismo sentido, Gozaíni, Osvaldo Alfredo "El consentimiento para el uso de los datos personales", LA LEY, 2001-C, 781.

[8] "Los "datos" en sí mismos, serían representaciones de aspectos de la realidad física, de las ideas, de los sentimientos, de las sensaciones, etc., que los integrantes de la especie se traspasan unos a otros, y que dado que se transmiten utilizándose los referidos "códigos comunes" de comunicación, son comprendidos o interpretados en similar sentido por emisores y receptores" (Peyrano, Guillermo F., "Datos sensibles: perfiles y regulaciones. El impacto del desarrollo tecnológico", El Derecho, boletín Nº 10.651, 13/12/2002.

“principios relativos a la legitimación del tratamiento de datos [9]

Se ha expresado que “su importancia radica en que constituye el medio o la modalidad a través de la cual el interesado tiene oportunidad de elegir el nivel de protección que le dará a la información sobre su persona; por eso, debe tratarse de una expresión de voluntad consciente e informada”[10].

Esta facultad de elegir el “nivel de protección” sobre las informaciones personales encuentra su justificación en el derecho a la “autodeterminación informativa”, reconocido como un auténtico derecho, incluso de rango constitucional, en el derecho europeo[11].

La afirmación de este derecho trae aparejado “que todo registro de datos debería estar subordinado al consentimiento de la persona identificada o identificable a

[9] Artículo 7: “Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca, o b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o d) es necesario para proteger el interés vital del interesado, o e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente.”

[10] Gils Carbo, Alejandra M., “Régimen Legal de las Bases de Datos y Hábeas Data”, Editorial La Ley, Buenos Aires, 2001, pág. 78.

[11] “El “derecho al dominio de los datos personales” (Recht auf “informationelle Selbstbestimmung”) ha sido considerado como un derecho constitucional garantizado (BverfG 15 diciembre 1983, BverfGE 65,1, 43)”, conforme Rigaux, François “Libre circulation des données et protection de la vie privée dans l’espace européen”, separata de “Festchrift für Ulrich Drobnig”, pág. 427. En relación a esta sentencia expresan del Peso Navarro y Ramos González que la misma “...señala que las limitaciones a este derecho a la autodeterminación informativa sólo son admisibles en el marco de un interés general superior y suscitan un fundamento legal basado en la Constitución. El legislador, en su regulación, debe observar el principio de proporcionalidad y tiene que adoptar, asimismo, precauciones de índole organizativa y de derecho procesal susceptible de contrarrestar el peligro de vulneración del derecho a la salvaguardia de la personalidad” (del Peso Navarro, Emilio y Ramos González, Miguel Ángel “LORTAD-Análisis de la Ley”, Ed. Díaz de Santos, Madrid, 1998, pág. 71).-

la cual se refieren las informaciones recogidas"[12].

El consentimiento del titular de los datos constituye la condición justificante de las operaciones de tratamiento de los datos de carácter personal (con las correspondientes excepciones previstas en la ley).

El consentimiento del titular de los datos debe ser libre, expreso e informado, quedando descartada la posibilidad de ser otorgado en forma tácita o presunta.

La ley privilegia la prestación de ese consentimiento en forma escrita, pero admite otros medios equiparables de acuerdo a las circunstancias.

La ausencia del soporte físico en el medio informático -propio de la manifestación por escrito (por lo usual, el soporte "papel")- hace que dicha manifestación no puede equipararse estrictamente a esta última, no obstante resultar posible su reproducción de esa forma.

Esa diferencia hace necesaria la adopción de los recaudos técnicos que permitan garantizar la autoría de la declaración de voluntad a fin de tener por válidamente prestado el consentimiento, como asimismo que se haya cumplido con los requisitos de "libertad" e "información" a su respecto, requeridos por la ley.

El recaudo de la "información" en el consentimiento, consiste en una puesta en conocimiento al titular de los datos, en una suerte de esclarecimiento de circunstancias relativas a esas informaciones, como igualmente de las relacionadas con las operaciones a que podrán ser sometidos, y de ciertos derechos que le reconoce la ley en relación a los mismos.

El consentimiento libre, expreso e "informado" es requerido para el "tratamiento" de los datos de carácter personal, comprendiendo por ende todas las operaciones involucradas en ese término. Las operaciones intermedias de almacenamiento, categorización, clasificación, etc., requerirán también del mismo, al igual que las referidas a la comunicación de estas informaciones (transferencia,

[12] Rigaux, François "Libre circulation des données et protection de la vie privée dans l'espace européen", separata de "Festchrift für Ulrich Drobnig", pág. 431.

cesión, etc.).

El sentido de esta exigencia finca en descartar la posibilidad de la obtención de conformidades, conseguidas sin la cabal conciencia de los titulares respecto de su contenido y alcances.-

El consentimiento prestado para el tratamiento de datos de carácter personal debe tener carácter revocable.-

Es necesario que el consentimiento sea inequívoco para que su tratamiento sea lícito. Esta es la regla adoptada por la Directiva 95/96 UE, la cual establece que los Estados miembros autorizarán el tratamiento de datos personales sólo si el interesado ha dado su consentimiento en forma inequívoca.

6.4. Conocimiento o información

La información de carácter personal que se recolecte debe ser puesta en conocimiento del sujeto concernido, y debe ser el resultado del empleo de medios lícitos, ya sea mediante el consentimiento del sujeto o por autorización legal.

6.5. Derecho de acceso

El derecho de acceso es concedido como un presupuesto de los derechos de rectificación, actualización, cancelación y confidencialidad.

El principio de la participación individual, consagra el derecho de acceso a los datos[13], que debe ser proporcionado "libremente, sin restricciones y con una

[13] El art. 8° del Convenio 108 establece: "Garantías complementarias para la persona concernida.- Cualquier persona deberá poder: a) conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero; b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de los datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos

periodicidad razonable y sin retrasos ni gastos excesivos"[14], implicando "la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, que se informe por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos" y "la comunicación, en forma inteligible, de los datos objeto de los tratamientos, y de toda la información disponible sobre el origen de los datos", así como "el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas".

6.6. Derechos de actualización, rectificación y supresión

La Constitución Nacional establece en su artículo 43 párrafo 3º que toda persona tiene además el derecho “en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización” de los datos personales contenidos en los ficheros ya comentados.

Estos derechos tienen ya vigencia en el derecho comparado, en las normas que hemos mencionado.

---

enunciados en los artículos 5º y 6º del presente Convenio; d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.”

[14] Artículo 12 Directiva (Derecho de acceso).- “Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: - la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; - el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos; c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.”

La ley francesa de 1978 (art. 3) establece que “Toda persona tiene derecho a conocer y rechazar las informaciones y los razonamientos usados en sistemas automatizados cuyos resultados la perjudiquen”.

La Directiva europea 46/1995 dispone en el marco del llamado “derecho de acceso” que los interesados tienen derecho a exigir la "rectificación, supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos"[15]. También significa la "notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado si no resulta imposible o supone un esfuerzo desproporcionado obtener información de la entidad responsable de los datos acerca de la existencia de datos que le conciernan"; "ser informado dentro de un tiempo razonable y de manera comprensible"; "oponerse a cualquier dato que le concierna y a que esa oposición quede registrada"; "obtener que los datos relativos a su persona, en caso de prosperar su oposición, sean suprimidos, rectificados o completados"; "ser informado de las razones por las cuales se deniega su derecho de acceso o éste no se le concede en lugar, tiempo y forma razonables; oponerse a toda negativa a darle las razones mencionadas precedentemente".

La ley española 15 de 1999, en su artículo 16, se ocupa del tema bajo el título “Derecho de rectificación y cancelación”[16].

---

[15] Artículo 12 inciso b) ut supra transcripto.

[16] Artículo 16 Ley 15/1999: “1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. 2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos. 3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. 4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación. 5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el

6.7. Elaboración de perfiles

La preocupación por el impacto de los denominados “perfiles virtuales” ha sido, conjuntamente con el derecho de acceso como manifestación de la autodeterminación informativa, el otro eje motivador de la normativa de protección de los datos personales.

Se lo describe como el derecho que tienen las personas a "no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc." [17]

Encontramos un antecedente de esta norma en la Ley francesa de 1978, cuyo artículo 2 estipula: “Ninguna decisión judicial, que implicara apreciación en cuanto al

---

interesado.” La Ley 78-17 francesa (art. 36): Art. 36. “El titular del derecho de acceso puede exigir que sean rectificados, completados, clarificados, puestos al día o eliminados, los datos concernientes que sean inexactos, incompletos, equívocos, obsoletos o cuya recolección, utilización, comunicación o conservación estén prohibidos. Cuando de hecho lo solicite al interesado, el servicio u organismo concerniente deberá entregar sin cargo copia del registro modificado. En caso de reclamo, la carga de la prueba incumbe al servicio ante el cual se haya ejercido el derecho de acceso, salvo que se haya establecido que las informaciones reclamadas hayan sido comunicadas por la persona a quien concierne o con su acuerdo. Cuando el titular del derecho de acceso obtenga una modificación del registro, la será reintegrado al valor de la tasa establecida en el art. 35.” La ley chilena lo contempla en el art. 12 que hemos transcripto supra.

[17] Artículo 15 Directiva (Decisiones individuales automatizadas) “1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc. 2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión: a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.”

comportamiento humano, podrá tener por fundamento la definición del perfil o de la personalidad del interesado dada por un sistema automatizado de informaciones. Ninguna decisión administrativa o privada que implique apreciación sobre un determinado comportamiento humano, podrá tener por único fundamento la definición del perfil o de la personalidad del interesado dada por un sistema automatizado de informaciones."

A su vez, el artículo 13 de la Ley 15-1999 española, antecedente directo de nuestra ley, establece que "1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. 2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. 3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto. 4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado."[18].

[18] El art. 12 de la LORTAD establecía: "Impugnación de valoraciones basadas exclusivamente en datos automatizados.- El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad."

Capítulo 7. Legislación argentina

Reforma constitucional de 1994. El habeas data en la constitución nacional. Constituciones provinciales. San Juan. Salta. La Rioja. Jujuy. San Luis. Córdoba. Río Negro. Tierra del Fuego, Antártica e Islas del Atlántico Sur. Provincia de Buenos Aires. Chubut. Chaco. Ciudad Autónoma de Buenos Aires. Santiago del Estero. Formosa. Tucumán. Neuquén. Reenvíos a la Constitución Nacional. Constituciones que no contemplan ni reenvían. Leyes provinciales. Santiago del Estero. Chaco. Chubut. Río Negro. Neuquén Mendoza. Tucumán. Misiones. San Juan. Ciudad Autónoma de Buenos Aires. Entre Ríos. Córdoba. Jurisprudencia relacionada.

La Constitucional Nacional de 1853-60, con las reformas de 1866, 1898 y 1957 no contenía una mención expresa al derecho a la intimidad, y menos aún a la protección de los datos personales, sin perjuicio de lo que hemos señalado en el capítulo primero.

Aún así, es posible encontrar anclaje para la protección de ciertos datos personales en varias disposiciones constitucionales: artículos 14 (publicar las ideas por la prensa sin censura previa), 18 (protección de la correspondencia epistolar y el domicilio), 19 (principio de reserva) y 33 (derechos y garantías no enumerados).

7.1. Reforma constitucional de 1994

El acuerdo político institucional, conocido como “Pacto de Olivos” se implementó mediante la Ley 24.309[1], que contenía el llamado “Núcleo de coincidencias básicas”, como anexo del artículo 2º. En esta disposición se establecían las materias que la Convencion Constituyente podía considerar. En el artículo 3º ap. “N” de dicho anexo se incorporó como tema (la) “Consagración expresa del habeas corpus y del amparo: Por incorporación de un artículo nuevo en el capítulo segundo de la Primera Parte de la Constitución Nacional.”

[1] Sancionada y promulgada el 29/12/1993. Publicada el 31/12/1993. http://infoleg.mecon.gov.ar/infolegInternet/anexos/0-4999/693/norma.htm/

Como podemos advertir, la institución del llamado “hábeas data” no estaba expresamente contemplado en la convocatoria, aunque el Consejo para la Consolidación de la Democracia[2] ya lo había propuesto, diciendo que en una futura reforma constitucional “debe consagrarse el derecho a la privacidad, principlamente con miras a que no se vea afectado por los avatares de la informática en materia de registros de datos.”[3]

La Convención Constituyente reunida en Santa Fe, en 1994, recibió aproximadamente veintisiete proyectos en los que se refería al “hábeas data”[4], y para darle cabida se resolvió incluir el tema en el párrafo tercero de lo que luego sería el actual artículo 43 de la Constitución Nacional.

La norma mencionada dice: "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 aquellos. No podrá afectarse el secreto de las fuentes de información periodística."

Como se verá luego, el tema no era una novedad ya que varias constituciones de las provincias argentinas durante la segunda mitad de la década del 80 introdujeron normas relacionadas con esta materia.

7.1.1. El habeas data en la constitución nacional

Como el artículo 43 ya citado está dedicado básicamente al amparo, ha sido frecuente considerar al denominado habeas data como una especie, o subespecie de

---

[2] Organismo especial asesor del gobierno del Presidente Raúl Alfonsín, creado mediante decreto Nº 2446/85, que fuera presidido por Carlos S. Nino, que produjo dos dictámenes sobre los puntos que deberían ser sometidos a una futura reforma constitucional

[3] “Reforma constitucional-Examen preliminar del Consejo para la consolidación de la Democracia”. Eudeba, Buenos Aires, 1986.

[4] Según lo manifestado por el Convencional Mariano Cavagna Martínez durante el debate.

ese instrumento procesal[5].

No compartimos esta visión pues al analizar los antecedentes del derecho comparado, extranjero y aún el público provincial, se advierte que estamos frente a un nuevo derecho dirigido a la protección de los datos personales, que es la autodeterminación informativa.

Esta afirmación no impide reconocer que, entre sus múltiples facetas, encuentren también tutela ciertos aspectos de la intimidad, el honor, la imagen o la identidad[6]. Es correcto prohibir que la información personal se emplee con fines discriminatorios, pero no es imprescindible acudir al amparo para alcanzar este objetivo.

El control sobre los datos acumulados y procesados en registros o bancos de datos públicos y privados, tiene tres dimensiones: la de conocer, la de acceder y rectificar, que los anglosajones denominan: *rigth to know*; *rigth to acces* y *rigth to correct*. Al derecho en sí, se lo conoció como habeas scriptum, entre nosotros como hábeas data, y tiene privilegio sobre el derecho de propiedad de la información[7].

Las acciones para ejercer los derechos de acceso, rectificación y actualización,

---

[5] CNCiv, sala F, 06/07/1995, “B. de S., D. A. v. Sanatorio G. A. s/amparo”, ED, 165-257; CNCiv, sala H, 25/09/1995, “Rossetti Serra, Salvador v. Dun & Brandstreet S.R.L.”, JA 1995-IV-355; STJ. Entre Ríos, sala 1ª, 08/11/1994, “R. R., J. E. v. Banco Francés del Río de la Plata”, JA 1996-III-1102, entre otros.

[6] CJ Salta, 02/11/1998. “Rocco, Juan C. c/ Banco Mayo Coop. Ltdo. LA LEY 1999-E, 904 y LL N.O.A, 199-234: ”La Constitución Nacional en su art. 43 prevé una fórmula amplia de hábeas data en la cual no se enuncia cuál es el bien jurídico que tutela -actúa frente a falsedades o discriminación-, permitiendo inferirlo en cada caso concreto. Sin embargo, al aludir su texto a la protección contra la discriminación, no estaría refiriéndose solamente a la igualdad, sino más bien a las posibles consecuencias persecutorias que pudieran pesar sobre las personas registradas de mantenerse ese dato tal como y donde está y, por otra parte, al permitir accionar sobre datos falsos, está protegiendo no sólo el valor verdad sino también toda la gama de afecciones a otros derechos que por vía de tal falsedad pueda sufrir la persona, como el honor, la reputación, la propia imagen, la identidad, etcétera.”; CNCiv, sala H, 25/09/1995, “Rossetti Serra, Salvador v. Dun & Brandstreet S.R.L.”, JA 1995-IV-355: ”La finalidad del hábeas data es impedir que en bancos o registros de datos se recopile información respecto de la persona titular del derecho que interpone la acción cuando dicha información está referida a aspectos de su personalidad que se hallan directamente vinculados a su intimidad.”

[7] Cf. Voto de Petracchi en “Urteaga”, ut supra citado.

que en definitiva integran lo que se conoce como “habeas data”, son parte de un estatuto más amplio, como hemos intentado explicar en el capítulo primero. En nuestra opinión hubiera sido más correcto establecer la garantía genérica de la protección de los datos personales, dejando abierto el camino a la estructuración de los medios procesales pertinentes por vía legislativa.

El texto constitucional, a nuestro juicio, ha confundido la forma con el fondo. Debió haber consagrado el plexo de derechos referidos a proteger los datos personales, y habilitar una vía procesal, por supuesto también expedita y rápida. La asimilación con la acción de amparo implicó el riesgo de desvirtuar la finalidad del instituto[8], situación que afortunadamente ha sido superada.

Mientras el amparo como remedio o vía procesal de naturaleza excepcional requiere que exista "ilegalidad o arbitrariedad manifiesta", el "hábeas data", en cambio, tiene una finalidad muy específica, que es otorgar a toda persona un medio procesal eficaz para poder conocer y controlar la información de carácter personal que le concierna y para evitar que terceras personas hagan un uso indebido de esa información.

En tal sentido, la Suprema Corte de Justicia de Mendoza ha sostenido que “Si bien según el texto constitucional el “hábeas data” es una especie de amparo, ello no implica que todo lo regulado por ley de amparo sea aplicable a aquél, pues el objeto perseguido procesalmente difiere en ambos casos. En efecto, para la procedencia del “hábeas data” no se requiere, en principio, arbitrariedad o ilegalidad manifiestas, dado que procede ante la mera falsedad en el contenido de los datos o la discriminación que de ellos pudiere resultar.” [9]

---

[8] Así por ejemplo, se puede apreciar este criterio en un fallo de la CNACAF, sala III, 22/12/1999, “M., M. c/ Fidelitas S. A. v otros”, LA LEY 2001-B, 791, con nota de Slaibe, María Eugenia y Gabot, Claudio, “La discriminación en los informes comerciales frente a la nueva regulación del "habeas data", en el que se sostuvo: “La admisión formal de la acción de habeas data requiere que el actor alegue que el registro cuestionado incluye información inexacta o que puede provocar discriminación, además de las previsiones constitucionales del amparo, tales como la necesidad de que el acto lesivo padezca de una arbitrariedad o ilegalidad manifiesta (del fallo de 1ª instancia).”

[9] SCJMdza, sala I, 17/11/1997, “Costa Esquivel, Oscar A. c/ CO. DE. ME.”, DJ, 1998-

El amparo tutela los derechos y garantías en general, excluida la libertad física, mientras que el "hábeas data" permite hacer efectivo un conjunto de derechos referidos a datos personales contenidos en registros operados o en poder de terceros. Estos derechos, básicamente, son el derecho de acceso, el de rectificación, actualización y cancelación, sin perjuicio del catálogo más amplio que hemos reseñado en materia de derecho comparado.

En uno de los primeros casos que resolvió la justicia civil se señaló que “Si hubiera querido limitar el hábeas data a la tutela exclusiva de la intimidad, se hubiera recurrido a un texto como el establecido para el hábeas corpus que especifica su aplicación cuando el derecho afectado es la libertad física. Por lo tanto, el hábeas data es un medio constitucional útil para la protección de *todos* los derechos y garantías establecidos por la Constitución, Tratados y leyes *cuando resultan violados por vía informática*.” [10]

En nuestra opinión, el texto constitucional debió habilitar a toda persona a "tomar conocimiento de los datos a ella referidos y de su finalidad", y como consecuencia de este derecho establecer la vía procesal para hacerlo efectivo. Esta interpretación correctora es fundamental, ya que resultaría contradictorio que debiera acreditarse la existencia de "ilegalidad o arbitrariedad manifiesta" por parte del titular u operador del banco de datos para que se pueda ejercer el derecho de acceso a los datos de carácter personal.

7.2. Constituciones provinciales

Varias constituciones provinciales, antes de la reforma constitucional de 1994, habían incorporado disposiciones que protegían los datos personales, con diversas fórmulas.

3-864.

[10] CNCiv, sala F, 06/07/1995, “B. de S., D. A. v. Sanatorio G. S.A. s/amparo”, ED 165-257:”...También es aplicable al supuesto de autos, en el cual la negativa del sanatorio accionado a brindar la información contenida en la historia clínica requerida, podría afectar la vida, la salud y la integridad personal (del dictamen del fiscal de Cámara)”.

7.2.1. San Juan

La Constitución de 1986[11] en su art. 26 (Registro de personas e informática) establece: “Todo ciudadano tiene derecho a tomar conocimiento de lo que de él conste en forma de registro y de la finalidad a que se destinan las informaciones, pudiendo exigir la rectificación de datos, así como su actualización.- No se puede utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se destine para fines estadísticos no identificables.”

7.2.2. Salta

La Constitución de 1986[12] dispone en su artículo 89 (Hábeas data): “Toda persona podrá interponer acción expedita de hábeas data para tomar conocimiento de los datos referidos a ella o a sus bienes, y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes. En caso de datos falsos, erróneos, obsoletos[13] o de carácter discriminatorio, podrá exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.”

7.2.3. La Rioja

La Constitución de 1986[14] previó en su artículo 30: “Son inviolables el domicilio, los papeles y registros de datos privados, la correspondencia epistolar y las comunicaciones de cualquier índole. Sólo pueden ser allanados, intervenidos, interceptados o registrados en virtud de orden escrita de Juez competente. La Ley limitará el uso de la informática para preservar el honor, la intimidad personal y familiar

---

[11] Sancionada el 26/4/1986 y publicada el 07/05/1986, http://www.legsanjuan.gov.ar/normas/Constitucion_ProvincialN.pdf/

[12] Sancionada el 02/06/1986 y reformada parcialmente el 07/04/1998, http://www.camdipsalta.gov.ar/conprov.htm/

[13] CJ Salta, 02/11/1998, “Rocco, Juan C c/ Banco Mayo Coop. Ltdo.”, LA LEY 1999-E, 904 y LL N.O.A, 199-234: “El art. 89 de la Constitución de la provincia de Salta que incorpora el hábeas data amplía la protección prevista en la Constitución Nacional en tanto dispone en su párrafo segundo la posibilidad de exigir la supresión, rectificación, confidencialidad o actualización de datos no sólo falsos, erróneos o de carácter discriminatorio, sino también obsoletos.”

[14] sancionada el 14/08/1986.

de los habitantes y el pleno ejercicio de sus derechos. El allanamiento de domicilio en horas de la noche es excepcional, debiendo el magistrado que lo dispone fundar la decisión. Las autoridades policiales sólo proporcionarán antecedentes penales de los habitantes en los casos previstos por la Ley."

En la reforma de 2002[15], se agregó un nuevo artículo, con el número "28 bis", bajo el título de "Habeas data", que dice: "Toda persona física o jurídica podrá interponer acción de hábeas data para garantizar su derecho de autodeterminación informativa, a cuyo fin está facultada para acceder a sus datos personales y los referidos a sus bienes, y al destino de tal información que se encuentren asentados en archivos, registros, bancos de datos u otros medios técnicos, electrónicos y ópticos, de carácter público o privado, de soporte, procesamiento y provisión de la información; y, en caso de falsedad o uso discriminatorio de tales datos, exigir la supresión, rectificación, actualización o el sometimiento a confidencialidad de los mismos. No podrá afectarse el secreto de las fuentes de información periodística."

7.2.4. Jujuy

El texto constitucional aprobado en 1986[16], establece en su artículo 23 (Protección de la intimidad de la honra y de la dignidad): "6. Todas las personas tienen derecho a tomar conocimiento de lo que constare a su respecto en los registros provinciales de antecedentes personales y del destino de esas informaciones, pudiendo exigir la rectificación de los datos. Queda prohibido el acceso de terceros a esos registros, así como su comunicación o difusión, salvo en los casos expresamente previstos en al ley. 7. Los registros provinciales de antecedentes personales harán constar en las certificaciones que emitan solamente las causas con condenas efectivas firmes dictadas contra el interesado , con excepción de las que debieran ser remitidas a los jueces. 8. El procesamiento de datos por cualquier medio o formas nunca puede ser utilizado para su registro y tratamiento con referencia a convicciones filosóficas, ideológicas o políticas, filiación partidaria o sindical, creencias religiosas o

[15] texto con las reformas de 1998 y 2002, http://www.larioja.gov.ar/servicios/documentos/constitucion2002.pdf/
[16] Sancionada el 22/10/1986 y publicada el 17/11/1986, http://www.jujuy.gov.ar/constitucion/index.htm/

respecto de la vida privada, salvo que se tratare de casos no individualmente identificables y para fines estadísticos."

7.2.5. San Luis

La Constitución de 1987[17] dispone en su Artículo 21 (Libertad de expresión y derecho de información): "Es inviolable el derecho que toda persona tiene de expresar libremente sus ideas y opiniones y de difundirlas por cualquier medio, sin censura de ninguna clase. Ninguna ley ni autoridad puede restringir la libre expresión y difusión de las ideas, ni trabar, impedir ni suspender por motivo alguno el funcionamiento de los talleres de impresión, difusoras radiales, televisivas y demás medios idóneos para la emisión y propagación del pensamiento, ni secuestrar maquinarias o enseres, ni clausurar sus locales, salvo por resolución judicial. Aquel que abuse de este derecho es responsable de los delitos comunes en que incurre a su amparo y de la lesión que cause a quiénes resulten afectados. Todos los habitantes de la Provincia gozan del derecho al libre acceso a las fuentes públicas de información. La libertad de expresión comprende también el derecho de las publicaciones a obtener los elementos necesarios a tal fin, y la facultad que tiene toda persona a la réplica o rectificación ante una referencia o información susceptible de afectar su reputación personal, la que debe publicarse gratuitamente, en igual forma y con el mismo medio utilizado. Una ley especial asegura la protección debida a toda persona o entidad contra los ataques a su honra, reputación, vida privada o familiar, cuando ésta es lesionada por cualquiera de los medios de difusión determinados en este artículo. Todos los habitantes de la Provincia tienen derecho a tomar conocimiento de los que de ellos conste en registro de antecedentes personales e informarse sobre la finalidad a que se destinan dichos registros y la fuente de información en que se obtienen los datos respectivos."

7.2.6. Córdoba

La Constitución de 1987[18], establece en su artículo 50 (Privacidad): "Toda

---

[17] Sancionada el 26/03/1987 y publicada el 08/04/1987, http://www.diputadossanluis.gov.ar/

[18] publicada el 29/04/1987, luego reformada en 2001, http://www.argentina.gov.ar/argentina/portal/documentos/cp_cordoba.pdf/

persona tiene derecho a conocer lo que de él conste en forma de registro, la finalidad a que se destina esa información y a exigir su rectificación y actualización. Dichos datos no pueden registrarse con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros, excepto cuando tengan un interés legítimo. La ley reglamenta el uso de la informática para que no vulnere el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos."

7.2.7. Río Negro

La Constitución de 1988[19], establece en su artículo 20 (Derecho a la privacidad): “La ley asegura la intimidad de las personas. El uso de la información de toda índole o categoría, almacenada, procesada o distribuida a través de cualquier medio físico o electrónico debe respetar el honor, la privacidad y el goce completo de los derechos, la ley reglamenta su utilización de acuerdo a los principios de justificación social, limitación de la recolección de datos, calidad, especificación del propósito, confidencialidad, salvaguarda de la seguridad, apertura de registros, limitación en el tiempo y control público. Asegura el acceso de las personas afectadas a la información para su rectificación, actualización o cancelación cuando no fuera razonable su mantenimiento.”

7.2.8. Tierra del Fuego, Antártida e Islas del Atlántico Sur.

La Constitución de 1991[20] establece en su artículo 45 (Privacidad): “Toda persona tiene derecho a conocer lo que de ella conste en forma de registro y la finalidad a que se destine esa información, y a exigir su rectificación y actualización. Estos datos no pueden registrarse con propósitos discriminatorios de ninguna clase ni ser proporcionados a terceros, excepto cuando estos tengan un interés legítimo.”

7.2.9. Provincia de Buenos Aires.

Simultánea a la reforma nacional, la reforma provincial de 1994[21] dispuso en su

---

[19] aprobada el 08/06/1988, http://www.legisrn.gov.ar/const_prov.htm/
[20] aprobada el 17/05/1991, http://www.legistdf.gov.ar/sitio/documentos/conspro/
[21] aprobada el 13/09/1994, http://www.gob.gba.gov.ar/legislacion/constitucion/cpppal.htm/

artículo 20: “Se establecen las siguientes garantías de los derechos constitucionales:...3. (Hábeas Data)- A través de la garantía del Hábeas Data, que se regirá por el procedimiento que la ley determine, toda persona podrá conocer lo que conste de la misma en forma de registro, archivo o banco de datos de organismo públicos, o privados destinados a proveer informes, así como la finalidad a que se destine esa información, y a requerir su rectificación, actualización o cancelación. No podrá afectarse el secreto de las fuentes y el contenido de la información periodística. Ningún dato podrá registrarse con fines discriminaciones ni será proporcionado a terceros, salvo que tengan un interés legítimo. El uso de la informática no podrá vulnerar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos. Todas las garantías procedentes son operativas. En ausencia de reglamentación, los jueces resolverán sobre la procedencia de las acciones que se promueven en consideración a la naturaleza de los derechos que se pretendan tutelar.”

7.2.10 Chubut

La Constitución de 1994[22] establece en su artículo 56 (Hábeas data): “Toda persona puede interponer acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o en los privados destinados a proveer informes y en caso de error, omisión, falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No puede afectarse el secreto de una fuente de información periodística.”

7.2.11. Chaco

La reforma de 1994[23], establece en el artículo 19: “Todos los derechos y garantías reconocidos, expresa o implícitamente, en esta Constitución, están protegidos en sus ejercicios por las siguientes acciones: ... (Habeas data) “Toda persona tiene derecho a informarse de los datos que sobre sí mismo, o sobre sus

[22] Aprobada el 15/10/1994, http://www.sup-trib-delsur.gov.ar/sup-trib-delsur/cbconst.htm/
[23] reforma aprobada el 27/10/1994, http://www.senadoctes.gov.ar/Constituciones-Pciales/constituci%F3n_provincia_chacoS.htm/

bienes, obren en forma de registros o sistemas oficiales o privados de carácter público; la finalidad a que se destine esa información, y a exigir su actualización, corrección, supresión o confidencialidad. Tales datos no podrán ser utilizados con fines discriminatorios de ninguna especie. No podrá afectarse el secreto de las fuentes de información periodística. Responsabilidad. Ningún juez podrá excusar la denegación de acciones contempladas en este artículo en el hecho de no haberse sancionado las leyes reglamentarias, en cuyo caso deberá arbitrar las medidas procesales adecuadas. Tampoco podrá negarse a entender en las acciones o resolverlas en violación de los plazos previstos. No podrán los funcionarios o empleados negarse al cumplimiento de la orden judicial respectiva. Si lo hicieren serán enjuiciados, y, en su caso, removidos".

7.2.12. Ciudad Autónoma de Buenos Aires

La Constitución de 1996[24] establece en su articulo 16: “Toda persona tiene, mediante una acción de amparo, libre acceso a todo registro, archivo o banco de datos que conste en organismos públicos o en los privados destinados a proveer informes, a fin de conocer cualquier asiento sobre su persona, su fuente, origen, finalidad o uso que del mismo se haga.- También puede requerir su actualización, rectificación, confidencialidad o supresión, cuando esa información lesione o restrinja algún derecho.- El ejercicio de este derecho no afecta el secreto de la fuente de información periodística.”

7.2.13 Santiago del Estero

La Constitución de 1997[25], en el capítulo de Garantías, ha regulado en el artículo 60 el Habeas data estableciendo: “Toda persona puede interponer acción de amparo para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o en los privados destinados a proveer informes y en caso de error, omisión, falsedad o discriminación, para exigir la

[24] aprobada el 01/10/1996, http://www.legislatura.gov.ar/1legisla/constcba.htm#_Toc0/
[25] aprobada el 23/12/1997, http://www.cervantesvirtual.com/servlet/SirveObras/12271652042369384109435/p0000001.htm#I_6_/. Las reformas de 2002 y 2005 no han afectado este artículo.

supresión, rectificación, confidencialidad o actualización de aquellos. No puede afectarse el secreto de la fuente de información periodística."

7.2.14. Formosa

La Constitución de 2003[26] establece en su artículo 14: "Los papeles particulares, la correspondencia epistolar y las comunicaciones telegráficas, telefónicas, cablegráficas o de cualquier otra especie, son inviolables, y nunca podrá hacerse sus registros, exámenes o interceptaciones, sino conforme a las leyes que se establecieren para casos limitados y concretos. Los que sean sustraídos o recogidos contra las disposiciones de aquéllas no podrán ser utilizados en procedimientos judiciales ni administrativos. Quedan asimismo protegidos los datos públicos o privados de los habitantes."

7.2.15. Tucumán

La Constitución reformada en 2006[27] establece en el artículo 39: "Toda persona podrá interponer acción expedita de Hábeas Data para tomar conocimiento de los datos referidos a ella o a sus bienes y su finalidad, que consten en registros o bancos de datos públicos o privados. En caso de datos falsos, erróneos, obsoletos, incompletos o de carácter discriminatorio podrá exigir su supresión, rectificación, confidencialidad, adición o actualización. En ningún caso podrá afectarse el secreto de las fuentes de información periodística. Ningún dato podrá registrarse con fines discriminatorios, ni será proporcionado a terceros salvo que tengan un interés legítimo. El uso de los registros informáticos y de otras tecnologías no podrá vulnerar el honor, la intimidad personal y familiar, y el pleno ejercicio de los derechos."

7.2.16. Neuquén

El art. 27 de la Constitución de 2006[28] dispone: "Inviolabilidad personal. Se

---

[26] aprobada el 07/07/2003, http://www.legislaturaformosa.gov.ar/documentos/constitucion%202003.htm/
[27] aprobada el 06/06/2006, http://www.tucuman.gov.ar/legislacion/docs/constituciondetucuman.pdf/
[28] aprobada el 17/02/2006 y publicada el 123/03/2006,

declara inviolable la seguridad individual. Con ese carácter serán respetados: la conciencia, la integridad física, la defensa en juicio, la correspondencia de toda índole, los papeles privados, las comunicaciones telefónicas, telegráficas, cablegráficas u originadas por cualquier otro medio, así como el normal ejercicio del trabajo, profesión o medios de vida." El artículo 21 (derechos enumerados) aclara que **"**Los habitantes de la Provincia gozan en su territorio de todos los derechos y garantías enumerados en la Constitución Nacional y en esta Constitución, con arreglo a las leyes que reglamenten su ejercicio y de los Derechos del Hombre sancionados por la Organización de las Naciones Unidas en París en 1948, los que se dan por incorporados al presente texto constitucional."

7.2.17. Reenvíos a la Constitución Nacional

En otras cartas magnas provinciales no se encuentran disposiciones referidas en forma explícita a la protección de los datos personales ni al hábeas data, pero ciertas normas permiten reenviar al artículo 43 de la Constitución Nacional.

Así, la Constitución de La Pampa de 1960, reformada en 1994[29], establece en su artículo 17: "Los jueces prestarán amparo a todo derecho reconocido por las Constituciones de la Nación o de la Provincia, y si no hubiere reglamentación o procedimiento legal arbitrarán a ese efecto trámites breves."

La Constitución de Santa Cruz de 1998[30], en su artículo 15 establece: "Los Jueces prestarán amparo a todo derecho reconocido por la Constitución Nacional y ésta, y si no hubiera reglamentación o procedimiento legal, arbitrará a ese efecto trámites breves."

La Constitución de Misiones de 1988[31], en el artículo 7º dice: "Los habitantes de la Provincia gozan de todos los derechos y garantías reconocidos en la Constitución Nacional, con arreglo a las leyes que reglamenten su ejercicio" y el artículo 29: "Los derechos y garantías enumerados en la Constitución Nacional y los

---

http://www.neuquen.gov.ar/constitucion/art_21_36.html/
[29] http://www.lapampa.gov.ar/CConstit.htm/
[30] aprobada el 27/11/1998, http://www.hcdsc.gov.ar/portal/content.asp?contentid=522/
[31] aprobada el 22/12/1988, http://www.misiones.gov.ar/legal/constitucion.htm/

que ésta misma establece, no serán entendidos como negación e otros no enumerados que hacen a la esencia de la democracia, al sistema republicano de gobierno, a la libertad, a la seguridad ya la dignidad humana."

En la Constitución de 1962 de la Provincia de Santa Fe[32], el artículo 17 dispone que "Un recurso jurisdiccional de amparo, de trámite sumario, puede deducirse contra cualquier decisión, acto u omisión de una autoridad administrativa provincial, municipal o comunal, o de entidades o personas privadas en ejercicio de funciones públicas, que amenazare, restringiere o impidiere, de manera manifiestamente ilegítima, el ejercicio de un derecho de libertad directamente reconocido a las personas en la Constitución de la Nación o de la Provincia, siempre que no pudieren utilizarse los remedios ordinarios sin daño grave e irreparable y no existieren recursos específicos de análoga naturaleza acordados por leyes o reglamentos."

7.2.18. Constituciones que no contemplan ni reenvían

En otros casos, la redacción es más ambigua, como la Constitución de Catamarca de 1988[33], cuyo artículo 15 establece: "Cualquier persona que se considere afectada por una publicación podrá recurrir a la justicia ordinaria para que ella por medio de un procedimiento sumario ordene al autor responsable o a la empresa publicitaria la inserción en sus columnas en el mismo lugar y con la misma extensión, la réplica o rectificación pertinente, sin perjuicio de las responsabilidades de otro orden (civil, penal, etc.) que correspondieran."

7.3. Jurisprudencia anterior a la Ley 25.326 (LPDPA)

Doctrina y jurisprudencia han coincidido en que los objetivos del hábeas datos son cinco: a) acceder a la información; b) actualizarla; c) rectificarla; d) asegurar su confidencialidad y e) suprimir la información sensible (intimidad, ideas políticas, religiosas, etc.)[34].

---

[32] aprobada el 14/04/1962, http://www.santa-fe.gov.ar/gbrn/noticias/constitucion.htm/
[33] aprobada el 03/09/1988, http://www.diputados-catamarca.gov.ar/datos/conti-prov.pdf/
[34] CNACAF, sala IV, 05/09/1995, "Farrel, Desmond A. v. Banco Central de la República

En los inicios, no bien se aprobó la reforma constitucional, se entendió que “el hábeas data (que) se explica en virtud del desarrollo del llamado *poder informático*, es una acción que tiende a proteger los derechos de los *registrados* en los archivos o bancos de datos, que pueden contener información equivocada, antigua, falsa o con potenciales fines discriminatorios, o lesiva del derecho a la intimidad de las personas, por lo que el promotor del hábeas data tendrá que alegar, para tener buen resultado, que los registros del caso incluyen información que es inexacta, o que puede provocarle discriminación”.[35]

La asimilación al amparo era notoria, sobre la base de considerar que dada la diversidad de legislaciones que han establecido el hábeas data, se origina la inexistencia de homogeneidad en cuanto al modo en que fue acogido el instituto, a su naturaleza, a los bienes jurídicos protegidos, etc.; (aunque) circunscribiendo el análisis en el ámbito de la Constitución Nacional, el art. 43 lo considera como una modalidad del amparo o como un amparo específico. Dado que el amparo es un medio judicial que se inicia contra actos u omisiones de autoridades públicas o particulares que en forma actual o inminente, lesionen, restrinjan, alteren o amenacen con arbitrariedad o ilegalidad manifiesta derechos y garantías reconocidas por la

---

Argentina y otros”, JA 1995-IV-350: “El hábeas data tiene cinco objetivos principales: a) que una persona pueda acceder a la información que sobre ella consta en un registro o banco de datos, b) que se actualicen datos atrasados, c) que se rectifiquen los datos inexactos, d) que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros, y e) supresión del registro de la llamada “información sensible” -vida íntima, ideas políticas, religiosas o gremiales”; SCJMdza, sala I, 17/11/1997, “Costa Esquivel, Oscar A. c. CO. DE. ME.”, DJ, 1998-3-864: “El “hábeas data” admite variantes, así; el informativo procura recabar la información obrante en registros y bancos; el aditivo tiene por finalidad agregar más datos a los que constan en los registros; el rectificador apunta a corregir o sanear datos falsos; el reservador tiende a asegurar la confidencialidad de los datos, y el cancelatorio pretende la supresión de información sensible.”

[35] CNCiv., sala F, 06/07/1995, “B. de S., D. A. c/ Sanatorio Greyton S. A.”, LA LEY, 1996-C, 473, con nota de Baigorria, Claudia Elizabeth, “Algunas precisiones sobre la procedencia del hábeas data”. En este caso, el acto reclamó por esta vía la entrega de una historia clínica, a lo que el tribunal entendió que si bien el hábeas data deducido por la actora para lograr que el sanatorio demandado le entregue su historia clínica es improcedente para tal fin, el principio “iura novit curia” autoriza a los jueces a efectuar la calificación jurídica de las pretensiones de las partes. En consecuencia, puede encuadrarse la cuestión en las disposiciones contenidas en el art. 323 del Cód. Procesal.

Constitución Nacional, un tratado o una ley; extremos que surgen del primer párrafo del art. 43 de la Constitución, y establecen cuáles son los bienes jurídicos protegibles por el amparo considerado genéricamente y que, por ende, deben presidir la consideración de las distintas especies del mismo, salvo que específicamente las últimas estén circunscriptas a determinados aspectos que lo pueden acotar[36].

El art. 43, párr. 3º de la Constitución Nacional establece una subespecie de amparo o amparo específico, conocido en el derecho comparado como hábeas data, que algunos califican como “amparo informativo” o “amparo informático”.[37]

En esa misma época se reiteraba que dentro de las garantías constitucionales incluidas en la reforma de 1994 se halla el hábeas data como una variable de derecho a la intimidad, consagrado tradicionalmente en el art. 19 CN., que otorga a toda persona el derecho de interponer acción de amparo 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 informe, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos (art. 43 párr. 3 CN).[38]

En el ámbito provincial se producían definiciones similares, al afirmar que la acción de hábeas data es una modalidad de amparo que permite a toda persona interesada acceder al conocimiento de los datos que consten en registros o bancos de datos públicos o privados destinados a proveer informes, y a exigir su supresión, rectificación, confidencialidad o actualización de aquéllos, en caso de falsedad o discriminación. Esta información debe referirse a cuestiones relacionadas con la intimidad, no pudiendo utilizarse por terceros sin derecho a hacerlo[39].

Sin embargo, las diferencias conceptuales comenzaban a ser vislumbradas,

---

[36] Del dictamen del fiscal de Cámara en autos citados en nota anterior.
[37] CNCiv, sala A, 08/09/1997, “Pochini, Oscar y otro c/ Organización Veraz S. A.”, LA LEY, 1998-B, 3.
[38] CNCiv, sala H, 25/09/1995, “Rossetti Serra, Salvador v. Dun & Brandstreet S.R.L.”, JA 1995-IV-355.
[39] Cám. Cont.Adm.1a Nominación Cba, 29/03/1995, “Flores, Marcela A. c/ Provincia de Córdoba”, LLC, 1996-316, con nota de Cafferata, Juan Carlos “La acción de hábeas data”.

por ejemplo, al señalar que el hábeas data es una figura de derecho procesal constitucional cuyos contornos y profundidad se encuentran en un candente proceso de demarcación. Hay quien afirma que si bien el "nomen juris" guarda natural vinculación con el hábeas corpus, el hábeas data sería por naturaleza una especie de amparo. En el específico caso del hábeas data se advierte analógicamente una versión particularizada -y con el sello del amparo constitucional- de la urgente acción preventiva de daños.[40]

Por otro lado, en los primeros pronunciamientos se aclaró que no es imprescindible el reclamo administrativo previo si el objeto de la acción de habeas data es tener acceso a la información relativa al actor.[41] O que el agotamiento de la vía administrativa para generar el acto que cause estado susceptible de revisión contencioso administrativa no resulta de necesaria producción como paso previo al habeas data, ya que tal proceder no se concilia con lo normado por la Constitución, al considerarlo como un supuesto de amparo.[42] El mismo tribunal señaló que el agotamiento de la vía administrativa a fin de generar el acto que cause estado susceptible de revisión contencioso administrativa, no es necesario que se lleve a cabo como paso previo al hábeas data, (ya que) tal proceder no concilia con lo normado por la Constitución al considerarlo como un tipo de “amparo” y como tal, garantizable mediante un remedio sencillo y rápido (pero) sería aconsejable, en virtud de los principios de buena fe, que previo a la interposición de la acción se solicite a la administración tanto el suministro de la información necesaria, de su finalidad, como de su rectificación, y/o demás aspectos abarcativos de este nuevo instituto (ya que) no hacerlo, no comporta un obstáculo susceptible de inadmisibilidad formal del hábeas data, correspondiendo al tribunal analizar el fondo de la cuestión. Pero tal comportamiento administrativo bien puede ser tenido en cuenta al momento de la

---

[40] Jdo. Civ., Com. y Minas Nº 12, Mza, 03/11/1997, “Huertas, Juan C. c/ CO.DE.ME.”, VJ, 1998-6-99 y LL Gran Cuyo 1998, 975.
[41] CFed. Bahía Blanca, sala I, 30/12/1994, “Gutiérrez, Héctor R. c/ Casino Militar del Personal Superior de la Base Naval Puerto Belgrano”, LA LEY, 1996-A, 314.
[42] Cám. Cont.Adm.1a Nominación Cba, 29/03/1995, “García de Llanos, Isabel c/ Caja de Jubilaciones Pensiones y Retiros de Córdoba”, LLC, 1995-948, con nota de Bayo, Oscar A., “Habeas data. Un derecho constitucional en su adecuado cauce como resultado de una decisión elogiable.”

imposición de las costas.[43]

Pero prontamente se señaló que quien promueve la acción de hábeas data debe acreditar haber realizado las gestiones o tramitaciones para acceder a los registros u obtener la información o rectificación requerida o bien la inutilidad de los trámites administrativos.[44]

Las disposiciones constitucionales regulatorias del hábeas data exigen para su admisibilidad la configuración de una hipótesis de falsedad o desactualización, pues su finalidad es la actualización de aquélla con el propósito de hacer cesar el agravio proveniente de una información que, aunque cierta en su origen, pudo quedar desvirtuada con el tiempo.[45]

En este sentido, es destacable el análisis del Ministro Petracchi, en el caso "Matimport"[46], que llegó a la Corte Suprema para resolver si procedía el habeas data para suprimir en el Registro de Juicios Universales (Dec.3003/56) la anotación de un pedido de quiebra, que había sido desestimado. El actor invocó el artículo 43 de la Constitución Nacional y sostuvo que la persistencia de ese dato lo perjudicaba, por su mera permanencia, y tenía efectos discrimintarios para su parte. Vale la pena aclarar que la actora era una persona jurídica (una sociedad anónima). El Tribunal desestimó tanto la tacha de arbitrariedad de la sentencia de la Cámara Comercial, como los efectos que se atribuían al registro. Sin embargo, en el voto premencionado del Dr. Petracchi, se efectúan algunas acotaciones precursoras de posteriores pronunciamientos.

En tal ocasión, el ministro sostuvo que "el registro del dato cuestionado en el

---

[43] Cám. Cont.Adm.1a Nominación Cba, 29-03/1995, "Flores, Marcela A. c/ Provincia de Córdoba", LLC, 1996-316.
[44] CNCom, sala D, 13/05/1996, "Figueroa Hnos. S. A. c/ Banco de la Provincia de Santiago del Estero", LA LEY, 1997-E, 1003, 39.763-S.
[45] CNCom, sala A, 10/09/1997, "Munditol S.A. y otros c/ Allianz Ras Argentina Sociedad de Seguros", LA LEY 1999-D, 744 y DJ 1999-3, 938.
[46] CSJN, 09/03/1999, "Matimport S.A. s/ medida precautoria", LA LEY 2000-B, 31, con nota de Slaibe, María Eugenia y Gabot, Claudio, "Hábeas data: su alcance en la legislación comparada y en nuestra jurisprudencia"; DJ 2000-1, 25; RU 2000-3, 13; ED 182, 1303 y RCyS 1999, 879.

sub lite no produce *per se* una intromisión desproporcionadamente invasiva y, en cambio, facilita al público información acerca de los avatares de juicios que, de uno u otro modo, pudieran afectarlo en algún momento. A esto ha de agregarse que, en el caso, quien padece la lesión es una persona jurídica, que por su calidad de tal, cuenta con una protección constitucional de la "privacidad" (en tanto exclusión de injerencias arbitrarias) mucho más débil, y que ocurre en un marco significativamente más estrecho que respecto de los individuos."

Aunque discrepemos con este enfoque del sistema de protección de datos personales fundado exclusivamente en el respeto a la "privacidad", como hemos sostenido, es destacable la distinción que realiza entre la privacidad de las personas físicas y las personas jurídicas. En este aspecto, nos parece más adecuado el voto del Ministro Boggiano, quien sostuvo que "nuestra Constitución ha incorporado un nuevo derecho a la protección de los datos personales frente a cualquier intromisión arbitraria o abusiva que pudiera implicar una violación a la intimidad y a los demás derechos constitucionales". "Pues, dicho derecho encuentra una íntima relación con el derecho a la integridad, a la dignidad humana, a la identidad, al honor, a la propia imagen, a la seguridad, de peticionar, a la igualdad, a la libertad de conciencia, a la libertad de expresión, de reunión, de asociación, de comerciar y con cualquier otro que, de uno u otro modo, pudiera resultar afectado (conf. causa ya citada "Suárez Mason", disidencia del juez Boggiano, considerando 10)."

Más allá de ello, y teniendo en cuenta que aún no se había sancionado la Ley Nacional de Protección de Datos Personales (de ahora en adelante, LPDPA), también señalamos como relevante que se haga referencia al principio de "calidad", al sostener "que con relación a la conservación de la información, y en tanto se ha mantenido intacta su "calidad", las mismas razones impiden acceder a su eliminación a través de la vía intentada"

También se introduce el tema del dato caduco, aunque los argumentos empleados tengan escasa relevancia en el debate que aún sigue abierto al respecto. En tal sentido, se dijo: "en contra de lo señalado por la demandante, ninguna similitud puede establecerse entre su petición y los plazos de caducidad de las condenas penales (art. 51, Código Penal). Tal argumento desconoce la diferencia sustancial que hay entre el registro de la preexistencia de una *condena*, que, como es obvio, sí formula un juicio negativo acerca de aquél respecto de quien se predica, y un *pedido*

de quiebra rechazado, afirmación relativamente neutra, y que, en última instancia, sólo señala el fracaso de quien solicitara la falencia. Por otra parte, los objetivos completamente diferentes de ambos registros y su orientación por principios jurídicos no trasladables del campo del derecho penal al del derecho comercial, impiden formular razonablemente una identidad básica entre ambas categorías que apoye la analogía propuesta y autorice su idéntico tratamiento."

7.4. Ley Nacional de Protección de Datos Personales

El 4 de octubre de 2000 se sancionó la Ley 25.326, denominada "Ley de Protección de datos personales y Hábeas Data"[47] (LPDPA) cuyo artículo 1º declara que está destinada a regular la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, y permitir el acceso a la información que sobre las mismas se registre (artículo 43, párr. 3° C.N.). Se establece que la norma será aplicable, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal y se excluyen las bases de datos y las fuentes de información periodísticas.

La norma tiene 48 artículos, distribuidos en 7 capítulos: I. Disposiciones generales; II. Principios generales relativos a la protección de datos; III. Derechos de los titulares de datos; IV: Usuarios y responsables de archivos, registros y bancos de datos; V: Control; VI. VII. Sanciones y Acción de protección de datos personales. Se establece un plazo de 180 días para que el Poder Ejecutivo la reglamente, y tiene dos disposiciones transitorias.

La reglamentación parcial corresponde al decreto 1558/2001[48] y la Dirección Nacional de Protección de Datos Personales, que crea el art. 29 de la LPDPA, ha emitido varias Disposiciones que complementan esta reglamentación.

---

[47] BO Nº 29517 del 02/11/2000.
[48] BO Nº 29787 del 03/12/2001.

7.4.1. Glosario

El artículo 2° tiene una suerte de glosario con varias definiciones. En primer término entiende por “datos personales”, la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables. También define a los llamados “datos sensibles” como los datos personales que revelan 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 sexua.

Son considerados “archivos, registros, bases o banco de datos”, indistintamente, todo 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. Define al tratamiento de datos como las “operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias”

Se llama “responsable de archivo, registro, base o banco de datos” a la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos, y titular de datos, a toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere esta ley.

“Usuario de datos” se denomina a toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros, o bancos de datos propios o a través de conexión con los mismos.

Finalmente, se llama “disociación de datos” a todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

7.4.2. Legitimación activa

El segundo párrafo del artículo 43 CN, al establecer quienes están legitimados para el amparo, menciona al "afectado", el defensor del pueblo y las asociaciones que

propendan a esos fines. De tal modo, se ha sostenido que han quedado comprendidos en esta tutela quienes invoquen no sólo un derecho subjetivo, sino también los llamados "intereses difusos" y aún un "interés simple".

Nosotros habíamos afirmado que el texto constitucional otorga legitimación activa a "toda persona", por lo que dada la definición del Código Civil de que "persona es todo sujeto susceptible de adquirir derechos y contraer obligaciones", debía entenderse que comprendía tanto a las personas físicas como las personas jurídicas, con el alcance del artículo 33 del Código Civil.

La Corte Suprema de Justicia, en el caso "Urteaga", antes de la ley, amplió notablemente el significado del texto constitucional al declarar que "Debe admitirse la legitimación invocada por quien reviste la calidad de hermano de quien se supone fallecido, toda vez que la habilitación para accionar de un familiar directo con sustento en el derecho a que se proporcione información, configura una de las alternativas de reglamentación posibles de la acción de hábeas data"[49].

El artículo 34 de la ley reconoce como legitimado para ejercer la “acción de protección de datos personales o de habeas data” al afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. También puede intervenir en forma coadyuvante el Defensor del Pueblo.

7.4.3. Legitimación pasiva

El texto constitucional se refiere a dos clases de registros o bancos de datos: los "públicos", y los "privados destinados a proveer informes".

La jurisprudencia y alguna doctrina han efectuado una interpretación amplia.

---

[49] CSJN, 15/10/1998, “Urteaga, Facundo R. c/ Estado Mayor Conjunto de las Fuerzas Armadas”, LA LEY 1998-F,237.

7.4.3.1. Bancos de datos públicos

En tal sentido, por registros o bancos de datos públicos debemos entender tanto a los existentes en los organismos del Estado, de cualquier naturaleza, ya que la ley no establece excepciones. Se incluye a las reparticiones de la Administración Pública nacional centralizada, los entes descentralizados, autárquicos, empresas públicas y sociedades estatales, así como dependencias provinciales y municipales.

La expresión "registros o bancos de datos públicos" no debe ser interpretada como lo opuesto a registros reservados o secretos, ya que la norma se refiere a los titulares u operadores de los registros o bancos de datos. La redacción del texto abona esta interpretación ya que armoniza con la referencia a "los privados destinados a proveer informes".

El debate sobre este tema fue resuelto por la Corte Suprema de Justicia, en el caso “Ganora”, en el que dos abogados interpusieron una acción para acceder a los datos que sobre ellos tenían los organismos de seguridad. Rechazada la acción en primera y segunda instancia, el máximo tribunal declaró que “afirmar que, mediante la acción de habeas data, sólo es posible acceder a la información "pública" o "al alcance de los particulares", importa desnaturalizar la vigorosa garantía incorporada en la Constitución Nacional”[50], ya que “no cabe asignar a una cláusula constitucional un alcance tal que signifique privarla de valor y efecto”[51]. Y más específicamente, “en la medida en que en el texto constitucional se instituye con el habeas data un instrumento que permite ejercer un control activo sobre los datos registrados sobre una persona, no puede existir ninguna duda en cuanto a que también han de estar alcanzados por dicho control aquellos datos que no están destinados a ser publicitados”[52], ya que “excluir de la protección reconocida por el art. 43, párrafo tercero, de la Constitución Nacional, a aquellos datos que organismos estatales mantienen fuera del acceso de los particulares, comporta la absurda consecuencia de ofrecer una acción judicial sólo en los casos en los que no es necesaria y vedarla

[50] CSJN, 16/09/1999, “Ganora, Mario E y otra” (voto del ministro Carlos S. Fayt), LA LEY, 2000-A,.355; 2000-B, 29; DJ, 2000-1-1328; SAIJ, Sum. A0054160.
[51] CSJN, in re Ganora cit., SAIJ, sum. A0054163: votos ministros Enrique Petracchi y Gustavo Bossert.
[52] CSJN, in re Ganora cit., SAIJ, sum. A0054167, voto ministro Enrique Petracchi.

en aquellos en los que el particular no puede sino recurrir, ineludiblemente, a la tutela judicial para ejercer su derecho"[53], entre otras categóricas afirmaciones en el sentido que sostenemos de legitimación pasiva de los bancos de datos de organismos públicos en general y de seguridad en particular[54]. Desde un primer momento sostuvimos que si sólo los (bancos de datos) privados "destinados a proveer informes" están comprendidos en la previsión constitucional, y en el caso de los públicos no hay aclaraciones, deben considerarse incluidos a todos los registros o bancos de datos pertenecientes u operados por organismos públicos[55].

7.4.3.2. Bancos de datos privados destinados a proveer informes

La otra categoría de bancos de datos que menciona el artículo 43 de la Constitución Nacional es la de "bancos de datos privados destinados a proveer informes".

En un primer momento se interpretó que la expresión se refería a las empresas de informes comerciales o de riesgo crediticio[56].

---

[53] CSJN, in re Ganora cit., voto ministros Petracchi y Bossert.
[54] CSJN, in re Ganora cit. (voto del ministro Carlos S. Fayt), SAIJ, sum A0054159: "El habeas data garantiza a toda persona que su afiliación política, sus creencias religiosas, su militancia gremial, sus antecedentes laborales o académicos, no pueden ser divulgados ni utilizados en su perjuicio por órganos públicos o entes privados"; idem, SAIJ, sum. A0054161: "El art. 43 de la Constitución Nacional protege aquellos datos que no se encuentran regularmente al alcance de los particulares, de tal manera, los datos obrantes en las fuerzas y organismos de seguridad, incluso los reservados y con carácter secreto, están especialmente contenidos en la norma"; ídem, SAIJ, sum. A0054164: "Excluir de la protección reconocida por el art. 43, párrafo tercero, de la Constitución Nacional, a aquellos datos que organismos estatales mantienen fuera del acceso de los particulares, comporta la absurda consecuencia de ofrecer una acción judicial sólo en los casos en los que no es necesaria y vedarla en aquellos en los que el particular no puede sino recurrir, ineludiblemente, a la tutela judicial para ejercer su derecho." (votos de los ministros Enrique Santiago Petracchi y Gustavo A. Bossert), etc.
[55] Altmark, Daniel R. y Molina Quiroga, Eduardo, "Habeas Data y reforma constitucional", I Congreso Internacional de Informática y Derecho, Mérida, España, 1995, en "Informática y Derecho", UNED, Dir. Valentín Carrascosa López, vol. 11 y 12, Idem: "Habeas Data", en La Ley 1996-A, 1554.
[56] Ver por ejemplo, Dubié, Pedro, "Análisis del debate parlamentario del hábeas data con relación a la información crediticia", JA 1999-II-882.

El derecho español se ocupó en su primera norma reglamentaria[57] de la prestación de servicios de información sobre solvencia patrimonial y crédito, entendiendo que la ley 5/1992 los regulaba desde una doble perspectiva, ya que por un lado, determina que quienes se dediquen a la prestación de servicios de información sobre solvencia patrimonial y crédito sólo podrán tratar automatizadamente datos personales obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento, pero por otro, regula el tratamiento de datos personales relativos al cumplimiento o incumplimiento de obligaciones dinerarias señalando que podrán tratarse dichos datos siempre que sean "facilitados por el acreedor o por quien actúe por su cuenta e interés"[58].

En este sentido, se consideró que mientras los primeros no se apartan de la regulación común que establece la LORTAD; los segundos presentan, por el contrario, un conjunto de especialidades (excepción del principio del consentimiento, tanto en la recogida del dato como en su tratamiento), que hacen necesario efectuar una serie de precisiones y que además, dentro de estos últimos, la realidad demuestra que coexisten perfectamente engarzados dos tipos de ficheros: uno, el propio del acreedor, que se nutre de los datos personales que son consecuencia de las relaciones económicas mantenidas con el afectado, cuya única finalidad es obtener la satisfacción de la obligación dineraria, y otro, un fichero que se podría denominar común que, consolidando todos los datos personales contenidos en aquellos otros ficheros, tiene por finalidad proporcionar información sobre la solvencia de una persona determinada y cuyo responsable, al no ser el acreedor, no tiene competencia para modificar o cancelar los datos inexactos que se encuentran en aquellos[59].

La LPDPA no aclaró el tema, y el Decreto reglamentario 1558/2001, luego de algunos vaivenes, terminó delimitando que "bancos privados destinados a proveer informes" son aquellos que excedan el uso meramente personal, y que estén

---

[57] Instrucción 1/1995, 01/03/1995, de la Agencia de Protección de Datos, relativa a "Prestación de servicios de información sobre solvencia patrimonial y crédito", BOE, 04/03/1995.
[58] Fundamentos de la Instrucción supra citada.
[59] Ídem.

destinados a ser distribuidos, sea a título oneroso o gratuito[60].

En primer término, las empresas o personas individuales dedicadas a recolectar información personal para suministrarla a sus clientes quedan comprendidas en esta categoría, como las empresas de informes comerciales o financieros, que proveen a bancos, financieras, comercios y a quienes conceden crédito en general, información sobre situación patrimonial, reclamos pecuniarios judiciales o extrajudiciales, etc. Esto ha sido reconocido por estas mismas empresas desde el inicio.

También consideramos que se incluyen en la especie otras entidades, tales como los colegios profesionales, establecimientos educativos, clubes deportivos, en la medida que los datos que recolecten puedan ser cedidos o difundidos a terceros.

Más conflictivo resulta deslindar si las entidades financieras, bancos, emisoras de tarjetas de crédito integran esta categoría, ya que no estarían “prima facie”, destinadas a proveer informes, aunque en nuestro caso particular creemos que están legitimadas pasivamente.

En el mismo dilema nos encontramos con el caso del Banco Central de la República Argentina (BCRA), que por supuesto no es “privado”, pero brinda informes sobre personas por intermedio de la Central de Deudores del sistema financiero, base de datos de la que se nutren las empresas proveedoras de informes crediticios[61]. Si

---

[60] Artículo 1º Decreto 1558/2001: “A los efectos de esta reglamentación, quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito”.

[61] Livellara, Silvina, “Hábeas data e información crediticia. La eventual responsabilidad civil de las entidades financieras y del banco central de la república argentina por cesión y publicidad de datos inexactos”, elDial DC2A7, trabajo en el que se concluye “En cuanto al B.C.R.A. si bien no se halla ligado contractualmente con el titular de los datos, cabe tener especialmente en cuenta lo dispuesto por el art.11 de la Ley 25.326 apartado cuarto, puesto que a nuestro entender reviste el carácter de cesionario. Dicha norma expresa que el cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la inobservancia de las mismas ante el organismo de control y el titular de los datos de

bien con escasos antecedentes, se ha admitido la procedencia de una acción de hábeas data no sólo contra la entidad que había efectuado la calificación errónea sino también contra el B.C.R.A., imponiéndole las costas, por considerar que su doble calidad de órgano de control y administrador de esa base de datos le imponía la fiscalización de la actividad desarrollada por el banco informante en punto a la calificación de sus clientes.[62]

Por nuestra parte, adherimos a la interpretación que ha efectuado un tribunal al incluir a los bancos entre los legitimados pasivos, entendiendo que ”en cuanto al argumento del banco demandado en el sentido que no constituye una entidad destinada a proveer informes a terceros, lo que excluiría la aplicabilidad del art. 43, tercer párrafo, de la Constitución Nacional, es del caso hacer notar que la garantía del habas data alcanza aún aquellos supuestos en los que no interviene una entidad destinada estrictamente a proveer informes (arg. arts. 2 y 33, inc. 1-b, LPDPA). Y en todo caso, resta siempre la protección genérica del amparo, basada en el 1er. párrafo del art. 43, toda vez que se halla en juego la garantía contemplada en el art. 42 de la misma Constitución inherente al derecho de los consumidores a una "información adecuada y veraz". De manera que, sea por la vía del habeas data, específicamente dirigida a la protección de los datos de las personas, o bien por la vía genérica del amparo, esta argumentación del banco resulta estéril.”[63].

La Suprema Corte de la Provincia de Mendoza en un caso muy preculiar en el que se demandó al banco que para que suprimiera un informe de mora por haberse cumplido el plazo de caducidad previsto en la LPDPA, frente a la defensa de falta de legitimación opuesta, resolvió que “Es procedente la acción de hábeas data incoada contra una entidad financiera a fin de que realice la actividad necesaria para suprimir la inclusión del actor en un registro privado de deudores por haber transcurrido el plazo legal de caducidad, pues si bien la entidad demandada no fue la que informó el

---

que se trate.”

[62] CNFed., Cba, sala A, Semanario Jurídico, 1999-II-179, con nota de Picasso, Sebastián y Wajntraub, Javier H., “La protección de los datos personales en un acertado decisorio” y Picasso, Sebastián “El BCRA y la imposición de costas en el hábeas data”, LA LEY 2002-D, 261.

[63] CNCom, sala C, 26/03/2002, “Halabi c/Citibank”, elDial AAE44 y Diario Judicial.com, 04-04-2002.

estado de mora del reclamante sino el fideicomiso a quien cedió dicho crédito, la notificación de la cesión fue posterior a la traba de la litis, por lo que el reclamante pudo creerse autorizado a demandar al cedente, que era con quien estableció originalmente el vínculo"[64]

Otra situación para analizar detenidamente es la de los tribunales que proveen informes sobre iniciación de juicios, que en la práctica funcionan como bancos de datos destinados a proveer informes[65].

7.4.3.3. Secreto de las fuentes de información periodística

La Constitución argentina veda el ejercicio de estos derechos con relación al "secreto de las fuentes periodísticas", disposición que a nuestro juicio no inhibe el ejercicio del derecho de acceso con relación a información de carácter personal contenida en bases de datos o registros "destinados a proveer informes".

Lo que se protege es el secreto de la "fuente", es decir del origen o proveedor de la información[66], pero no puede impedirse que "toda persona" conozca qué datos personales suyos están registrados en un banco o archivo, si estos datos luego están destinados a hacerse públicos. Este derecho de acceso tiene por finalidad, precisamente, la rectificación, actualización, supresión o confidencialidad, cuando exista inexactitud o discriminación.

---

[64] SCJ Mendoza, sala I, 16/02/2009, "Albares Raúl c/ Banco de Galicia", LLGran Cuyo 2009, marzo, 157; LA LEY 2009-B, 247, con nota de Molina Quiroga, Eduardo, y LLGran Cuyo 2009 (abril), 223.

[65] En nuestra opinión, es el caso de la Cámara Nacional de Apelaciones en lo Comercial, en virtud de lo dispuesto en el art. 52 inc. j) de su Reglamento: "Diariamente se editarán por orden alfabético listas de demandas iniciadas con indicación de partes, objeto, Juzgado y Secretaría, que se archivarán cronológicamente y servirán como libro general se asignaciones del fuero comercial. Similar edición se efectuará trimestralmente. Tales constancias (y las existentes en el sistema informático) serán publicas, con excepción de las medidas cautelares y diligencias preliminares que se editarán por separado manteniéndose reservadas. Se emitirán en similares tiempo y condiciones planillas donde consten los juicios asignados por recusación o excusación, partes, día, juzgado de origen y adjudicado."

[66] JNCAF Nº 3, 02/11/1995, "Nalib Yabrán, Alfredo E. v. Estado Nacional", Reseña "Hábeas data" por Marco Rufino, en JA 1996-III-1102: "La acción de hábeas data no debe afectar el secreto de las fuentes de información periodística."

La jurisprudencia ha declarado que “el hábeas data constituye un remedio excepcional que resulta de aplicación cuando la información resulte falsa. Pero en la medida en que para verificar si las evaluaciones periodísticas resultan o no veraces debe recurrirse a la fuente de información de cada medio, la Constitución Nacional pone un vallado a la aplicación del propio instituto, la prohibición de afectación del secreto de la fuente de información periodística, conforme lo ordena el último párrafo del art. 43 de la Carta Magna.”[67]

A pesar de ser esta nuestra interpretación del texto constitucional, la LPDPA establece otra cosa, ya que el último párrafo del artículo 1º reza: “En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas”, en un claro exceso legislativo frente al texto constitucional.

7.5. Incorporación de los principios internacionales de protección de datos

La LPDPA ha receptado en gran medida los principios que hemos analizado en capítulos anteriores.

7.5.1. Principio de Licitud.

Como se ha destacado anteriormente, los datos personales deben ser "tratados de manera leal y lícita"; de tal modo que sean "recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines". Este principio ha sido receptado en la LPDPA con la siguiente redacción: “La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley” (art. 4º inciso 2).

7.5.2. Calidad

El principio de referencia establece que los datos que sean objeto de

[67] CNPenal Económ., sala B, 25/09/1997. “Dirección General Impositiva”, LA LEY 1999-A, 204, con nota de Bazán, Víctor, “El hábeas data ante una visión jurisdiccional restrictiva”.

tratamiento deben ser "exactos y, cuando sea necesario, actualizados, debiendo tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados".

Este requisito de exactitud y actualización debe completarse con la necesidad que los datos en tratamiento sean "adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente"

La LPDPA ha reproducido este concepto del siguiente modo: “Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido” (art. 4º inciso 1) y “Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario” (art. 4º inciso 4).

Es importante destacar que los responsables del tratamiento, es decir la persona física o jurídica que gestiona u opera el procesamiento de la información, son quienes están encargados de garantizar el cumplimiento de estos principios de calidad[68]. La LPDPA establece: “Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley” (art. 4º inciso 5)

Esta regla, de fundamental importancia en la estructura del sistema de protección de datos personales, ha sido expresamente reconocida por la jurisprudencia de la Corte Suprema de Justicia de la Nación, sobretodo desde el año 2005, al resolver en un recurso de hecho sobre la información difundida por una empresa de informes crediticios[69].

---

[68] Artículo 6 inciso e) Directiva europea supra citada.

[69] CSJN, 05/04/2005, "Martínez, Matilde Susana c/ Organización Veraz S.A.", LA LEY 2005-B, 743; RCyS 2005, 806; DJ 2005-1, 1020 y Fallos 328:797. El voto de la mayoría estuvo a cargo de los ministros Petracchi, Fayt, Maqueda, Zaffaroni, Lorenzetti y Argibay (según su voto). En disidencia votaron Boggiano, Belluscio y Highton. (En el caso la actora había celebrado un

En dicha ocasión el máximo tribunal sostuvo que “De conformidad con los arts. 4, incs. 4º y 5º, 26 y 33 de la LPDPA, los datos registrados por las empresas que prestan servicios de información crediticia deben ser exactos y completos; vale decir, no es suficiente con que la información haya sido registrada y transmitida sin "arbitrariedad manifiesta", sino que tiene que ser precisa. En tal sentido, lo expresado en el art. 43 de la Constitución Nacional con relación al derecho del afectado en obtener la supresión o rectificación de toda información personal que incurra en "falsedad" debe ser interpretado conforme a los términos de la respectiva ley reglamentaria. Según ésta, no basta con que lo registrado como verdadero sea tal si, al tomar razón de los datos relevantes al objeto y finalidad del registro de manera incompleta, la información registrada comporta una representación falsa.”

Y agregó que "No basta con decir una parte de la verdad y con proceder a registrarla para quedar exento de responsabilidad, si la información registrada (por ser falsa o incompleta) afecta la intimidad, privacía, o la reputación de terceros (confr. Dun & Bradstreet v. Greenmoss Builders 472 U.S. 7439)."

Para ello tuvo en cuenta que "La empresa demandada goza de la libertad de informar, y satisfacer así el objeto comercial para el que fue creada y el interés de su clientela, o puede abstenerse de hacerlo. Pero si en provecho propio procede a registrar y comerciar con la información registrada sobre la actividad de los terceros, debe hacerlo en las condiciones legalmente exigidas, esto es, de manera exacta y completa y, de no ser así, rectificar o completar los datos personales de un modo que representen del modo más fielmente posible la imagen de aquellos respecto de

---

contrato de mutuo hipotecario, y como el banco acreedor (posteriormente quebrado) había seguido actualizando el monto del préstamo pese a la prohibición de indexar impuesta por la ley 23.928, promovió una acción judicial consignando el monto de lo que estimó adeudar. La Corte consideró que “en tales condiciones, el informe que se limita a describirla como una deudora "irregular", es decir, morosa, aunque aclare que mantiene "dos juicios contra el banco" prestamista por revisión de precio y consignación, no representa más que una imagen parcializada del comportamiento de la actora en el cumplimiento de sus obligaciones comerciales.”). La sala B de la Cámara Nacional de Apelaciones en lo Comercial, había denegado el recurso extraordinario sosteniendo que había una mera discrepancia con la valoración de las constancias de la causa, pero no un apartamiento notorio de la solución normativa prevista para el caso ni una decisiva ausencia de fundamentos. El dictamen del Procurador General, en el año 2002, había aconsejado desestimar la queja.

quienes suministra información, máxime cuando no cuenta con el consentimiento de éstos."

La Corte insistió con este criterio pocos meses después[70], en un caso en el que el cuestionamiento del actor estaba dirigido a aclarar que existía un estado litigioso sobre la deuda reportada por la empresa de informes crediticios[71]. Entonces dijo que "no puede calificarse de "exacta" o "actualizada" una información que se limita a indicar, *sin ninguna aclaración o salvedad,* que la actora mantiene una deuda con una entidad bancaria, correspondiendo que esa información se actualice y complete a fin de que quede reflejado, del modo más preciso posible, el estado de litigiosidad suscitado respecto de los créditos a los que se ha hecho referencia. Agregó que no se advierte que la inclusión en la base de datos de la existencia de la querella penal aludida por la actora merezca objeciones, ya que los hechos allí investigados se relacionan de manera directa e inmediata "con datos personales de carácter patrimonial relativos a la solvencia económica y al crédito" (art. 26, ap. 1, de la LPDPA) de la actora, dado que ésta alega que ha sido víctima de una estafa en la operatoria del otorgamiento de los préstamos, y niega el carácter de deudora que le atribuye la entidad bancaria. Es decir, se trata de datos relevantes para los fines previstos por la ley que reglamenta la acción de habeas data, la cual, cabe recordarlo, tiene por objeto la protección de las personas a las que se refieren los datos, y no a las instituciones -públicas o privadas- que los registren o almacenen (Fallos: 321:1660)."

Aunque el fallo no haga referencia explícita al principio de calidad, consideramos que la solución responde al mismo.

---

[70] CSJN, 21/11/2006, "Di Nunzio, Daniel F. c/ The First National Bank of Boston y otros s/ hábeas data", LA LEY 2007-C, 131.

[71] La demanda perseguía la intimación al Banco de Boston y a la Organización Veraz S.A. para que se agregara, en los datos referidos a la actora, con relación a los créditos otorgados por el primero cuyo incumplimiento se le atribuye, la información derivada del dictamen de un funcionario del Banco Central -en el que se formulan objeciones al otorgamiento de tales créditos en tanto su importe era acreditado por el banco en la cuenta del concesionario de venta de automotores sin controlar que los clientes, como sucedió con la actora, recibieran las unidades objeto de aquéllos- y de una causa penal promovida a raíz de una denuncia formulada por la accionante -atinente a los mismos hechos- en la que alega que fue damnificada por una estafa.

7.5.3. Consentimiento

El art. 5º de la LPDPA dispone en su inc.1, en consonancia con este principio: “El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias”.

Se afirma que el consentimiento se exige en tres momentos[72]:

a) Al tiempo de la obtención

b) Mientras se mantenga en el archivo

c) Cuando los datos se cedan o transfieran.

El consentimiento del titular de los datos constituye la condición justificante de las operaciones de tratamiento de los datos de carácter personal (con las correspondientes excepciones previstas en la ley).

El consentimiento del titular de los datos debe ser libre, expreso e informado, quedando descartado la posibilidad de ser otorgado en forma tácita o presunta.

La ley privilegia la prestación de ese consentimiento en forma escrita, pero admite otros medios equiparables de acuerdo a las circunstancias.

La ausencia del soporte físico en el medio informático -propio de la manifestación por escrito, llamado soporte “papel”- hace que dicha manifestación no pueda equipararse estrictamente a esta última, no obstante resultar posible su reproducción de esa forma.[73]

Esa diferencia hace necesaria la adopción de los recaudos técnicos que permitan garantizar la autoría de la declaración de voluntad a fin de tener por

---

[72] Gozaíni, Osvaldo Alfredo, “El consentimiento para el uso de los datos personales”, LA LEY, 2001-C, 781.

[73] Gozaíni, ob.cit. supra, entiende que es imprescindible la firma, seguramente por la expresión “por escrito” de la norma. No compartimos esta opinión.

válidamente prestado el consentimiento, como asimismo que se haya cumplido con los requisitos de “libertad” e “información” a su respecto, requeridos por la ley.

El recaudo de la “información” en el consentimiento, consiste en una puesta en conocimiento al titular de los datos, en una suerte de esclarecimiento de circunstancias relativas a esas informaciones, como igualmente de las relacionadas con las operaciones a que podrán ser sometidos, y de ciertos derechos que le reconoce la ley en relación a los mismos.

El consentimiento libre, expreso e “informado” es requerido para el “tratamiento” de los datos de carácter personal, comprendiendo por ende todas las operaciones involucradas en ese término. Las operaciones intermedias de almacenamiento, categorización, clasificación, etc., requerirán también del mismo, al igual que las referidas a la comunicación de estas informaciones (transferencia, cesión ,etc.).[74]

El sentido de esta exigencia finca en descartar la posibilidad de la obtención de conformidades, conseguidas sin la cabal conciencia de los titulares respecto de su contenido y alcances.-

El consentimiento prestado para el tratamiento de datos de carácter personal debe tener carácter revocable.

La reglamentación aprobada por el decreto Nº 1.558/2.001 dispone: “El consentimiento dado para el tratamiento de datos personales puede ser revocado en cualquier tiempo”, y agrega que esa revocación “no tiene efectos retroactivos”. Así se remedia la omisión de la LPDPA, que implicaba una injustificada limitación del poder de disponibilidad que sobre los datos se reconoce a sus titulares.[75]

Los derechos de los titulares de los datos de carácter personal, deben ser

---

[74] En similar sentido, Gozaíni, ob.cit. supra.
[75] Peyrano, Guillermo F., “El principio del consentimiento en el “sistema de protección de los datos personales”. las condiciones de su validez y la posibilidad de revocación del consentimiento prestado”, ponencia presentada en la XIV Conferencia Nacional de Abogados (F.A.C.A.) Santa Fe-Paraná 2004.

interpretados de modo amplio, incluso en lo relativo a la posibilidad de oponerse al tratamiento de datos en determinadas circunstancias y mediando causa justificada, no obstante el consentimiento prestado en forma previa al efecto.-

El art. 5 de la LPDPA sobre protección de datos personales exige el consentimiento del interesado para la validez del dato asentado en el Archivo. Su importancia "radica en que constituye el medio o la modalidad a través de la cual el interesado tiene oportunidad de elegir el nivel de protección que le dará a la información sobre su persona por eso debe tratarse de una expresión de voluntad consciente e informada..."[76]. La LPDPA dice, además, "que el consentimiento debe ser libre, expreso e informado y constar por escrito o por otro medio que permita se le equipare de acuerdo a las circunstancias. Y agrega luego que debe ser expreso". Incluso ha ganado terreno la tesis de requerir un "consentimiento inequívoco del titular de los datos para que sea lícito su tratamiento. Ésta es la regla adoptada por la Directiva 95/96 UE, la cual establece que los Estados miembros autorizarán el tratamiento de datos personales sólo si el interesado ha dado su consentimiento en forma inequívoca.

Sin embargo, el mismo artículo 5º LPDPA admite numerosas excepciones a esta regla regla ya que el mismo no será necesario cuando: “a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526”.

A ello cabe agregar que la propia LPDPA en su Art. 26, legitima la prestación de servicios de información crediticia en la medida que se refieran a datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de

[76] Gils Carbó, Alejandra M., "Régimen legal de las bases de datos y Habeas Data", supra citado, p. 78 y sigtes.

fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento, o datos relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés (incs. 1° y 2°)."[77]

7.5.4. Conocimiento o información

El artículo 6º de la LPDPA establece que la persona requerida "deberá ser anoticiada sobre la finalidad y el destino que se les dará a los datos solicitados; identidad y domicilio del responsable del Archivo; de las consecuencias de proporcionar sus datos y la posibilidad de ejercer, en su caso, el derecho de acceso, rectificación y supresión de los datos".

La solución es perfectamente lógica porque la Constitución Nacional, al establecer el recurso de "habeas data" en su art. 43, y el Cód. Civil argentino en sus arts. 19 y 1071 bis, al reglamentar el derecho a la intimidad de que goza todo ciudadano, son particularmente celosos en la protección de este derecho personalísimo que hace al honor, a la reputación y al prestigio de aquellos que pueden quedar gravemente "comprometidos, por no decir totalmente desfigurados, por el almacenamiento electrónico e indiscriminado de datos sensibles y/o personales, con mucha mayor razón cuando aquellos son falsos, discriminatorios o producto, de un error del Banco, como ocurre en el caso *(del voto de Moreno Hueyo, fundamentando la responsabilidad de Veraz)*[78]

7.5.5. Derecho de acceso

Nuestra ley ha incorporado este principio en los artículos 13, 14 y 15.

La LPDPA admite su ejercicio extrajudicial en el artículo 14, que establece que el titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y

---

[77] CNCom, sala D, 11/10/2002 "Fusto, Liliana Antonia c/ Organización Veraz Sociedad Anónima s/amparo", Diariojudicial.com, 13/12/2002.
[78] CNCiv, sala K, 08/10/2003, “Botta, Rodolfo E. c/ Citibank N.A. y otros”, LA LEY 08/01/2004, 3; Idem: CNCiv, sala K, 22/10/2002, “Gutiérrez, Vicente Juan Carlos Demetrio c/ Banco de la Provincia de Buenos Aires y otro”, LA LEY 2002-F, 781.

obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes, y luego dispone que el responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.

Sin embargo, en una disposición que nos parece cuestionable, el inciso 3) del mencionado artículo 14, limita el derecho de acceso en cuanto a su gratuidad, a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto[79].

---

[79] En general estas restricciones pueden verse en otras legislaciones, aunque ellas no tienen un texto constitucional como nuestro artículo 43 párrafo 3º- Ver por ejemplo el art. 12 de la Ley 19.628 de Chile: “Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen. Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos. Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal. En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente. Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos.” El artículo 15 de la Ley española 15/1999 es en cambio más restrictivo “1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las

Esta restricción no funciona cuando se trata de bases de datos con fines de publicidad.

En cuanto al ejercicio del derecho de acceso en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. Asimismo, el artículo 15 impone que la información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.

En cuanto a la forma de proporcionar la información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

7.5.6. Derechos de actualización, rectificación y supresión

El artículo 16 de la LPDPA reglamenta estos derechos, estableciendo que toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. A tales efectos, el responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad. El incumplimiento de esta obligación dentro del término

---

comunicaciones realizadas o que se prevén hacer de los mismos. 2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.”

acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley[80].

En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.

La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.

Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.

Sin embargo, la ley admite que los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros (artículo 17 LPDPA).

Al respecto vale recordar que la Corte Suprema en el caso “Ganora” ya había establecido que “en principio, la obtención de información sobre datos personales obrantes en los organismos y fuerzas de seguridad halla adecuación legal en la acción

[80] CNCiv, sala K, 22/10/2002, “Gutiérrez, Vicente Juan Carlos Demetrio c/ Banco de la Provincia de Buenos Aires y otro s/daños y perjuicios”, LA LEY 2002-F, 781: “Existe negligencia o descuido imputable a una empresa que lucra con información sobre riesgo crediticio, si frente al reclamo efectuado por un particular para rectificar un dato falso o inexistente, le exige al interesado la prueba de un hecho negativo -en el caso de que no era ni nunca fue deudor del banco- cuando su obligación era recabar a la entidad bancaria responsable la ratificación o rectificación del dato en cuestión para confirmarlo o suprimirlo, según el caso. Cuando una empresa que lucra con información sobre riesgo crediticio, debe asentar en su archivo de datos la calificación de "deudor irrecuperable" respecto de un particular, previamente -para no incurrir en culpa o negligencia- debe notificar de inmediato al interesado a fin de permitirle formular las observaciones que estimara pertinentes (conf. Art. 5º de la ley 25326 sobre protección de datos personales)”. (Del voto de la mayoría)

de habeas data, sin perjuicio de que el suministro de esa información pueda, eventualmente, afectar la seguridad, la defensa nacional, las relaciones exteriores o una investigación criminal, cuestión que en cada caso deberá ser invocada por el titular de la respectiva institución."[81]

Más recientemente, se ha resuelto que "La mera negativa del organismo de seguridad acerca de la existencia de los informes requeridos-en el caso, respecto de un partido político y su titular- no es por sí sola suficiente para el rechazo de la acción de hábeas data deducida, pues ello implicaría otorgar al demandado la posibilidad de evadir su obligación sin brindar explicaciones suficientes."[82]

Otra excepción al derecho de acceso por parte de los responsables o usuarios de bancos de datos públicos se habilita cuando ello pudiera obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado (art. 17 inciso 2) LPDPA).

Pero aún en estos dos casos, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa (art. 17 inc. 3 LPDPA).

7.5.7. Conservación. Derecho al olvido

La ley argentina ha previsto que "Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados" (art. 4º inciso 7).

La interpretación del llamado derecho al olvido, o eliminación del dato caduco no ha sido pacífica, en especial, con referencia a los informes crediticios, como

---

[81] CSJN, 16/09/1999, "Ganora, Mario E y otra", LA LEY, 2000-A,.355; 2000-B, 29; DJ, 2000-1-1328; SAIJ, sum. A0054150. Comp: Sagües, Néstor P, "El hábeas data contra organismos estatales de seguridad", LA LEY, 2000-A, 352.
[82] CNACAF, sala IV; 17/05/2001, "B., G. O. y otro c/ M.I", LA LEY, 2001-b, 812.

ampliaremos en el capítulo siguiente.

7.5.8. Elaboración de perfiles

Como hemos señalado en la legislación europea, uno de los objetivos de la protección de datos personales es evitar la elaboración de perfiles. En la LPDPA, esta limitación se encuentra restringida al ámbito estatal, ya que el artículo 20 establece: "1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del Interesado; 2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos".

Consideramos que este estándar debe extendese al ámbito de las relaciones entre particulares, sobre todo en materia de informes de solvencia crediticia, y así lo han entendido algunas conferencias nacionales de abogados[83] en las que hemos planteado la cuestión.

7.6. Leyes provinciales

Varias provincias han sancionado leyes regulatorias del procedimiento de Habeas Data, sin perjuicio de alguna norma que avanza en la creación de registros vinculados con la protección de datos personales.

7.6.1. Santiago del Estero

En 1996 se sanciona la ley Nº 6.296[84], regulatoria del Amparo. El artículo 2 de

---

[83] La XIV Conferencia Nacional de Abogados (Santa Fé, Paraná, octubre 2003), en base a nuestra ponencia, recomendó: "En la autodeterminación informativa se considera como un uso arbitrario de la información, generador de derecho al resarcimiento del daño moral y material, toda decisión con efectos jurídicos sobre una persona o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, no solo en el ámbito público (art. 20 LPDP) sino también en el ámbito de las relaciones entre particulares ..."

[84] Ley 6296, sancionada el 11/06/1996, Boletín Oficial, 12/07/1996, modifica el Código

esta ley dice: “Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra cualquier decisión, acto, hecho u omisión de una autoridad pública o privada, que amenazare, restringiere, impidiera o pusieren peligro inminente de manera manifiesta e ilegítima el ejercicio de un derecho reconocido a las personas en la Constitución de la Nación o de la Provincia, a fin de que el Juez arbitre los medios para el inmediato restablecimiento del derecho afectado. Los derechos amparados son aquellos expresa o implícitamente recogidos por la Constitución de la Nación o de la Provincia, a fin de que la parte que soporta los efectos de la medida manifiestamente ilegítima, obtenga su cese o el cumplimiento según el caso. Para que la acción proceda debe tratarse de derechos ciertos e incontestables asegurados por las Constituciones, las leyes o los contratos públicos.” El artículo siguiente específicamente dispone: “Artículo 3. - La acción deberá instaurarse dentro del plazo de treinta (30) días de producido el agravio y desde el cual tomare conocimiento el amparista. Podrá interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como los derechos de incidencia colectiva general; tendrá acción el afectado y demás instituciones legalmente habilitadas. Toda persona afectada podrá interponer esta acción para tomar conocimiento de los datos a ellos referidos y de su finalidad que conste en registros o bancos de datos públicos, o los privados destinados a proveer informaciones y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos.”

7.6.2. Chaco

En 1996 se sanciona la ley Nº 4.360[85], regulatoria del procedimiento de Hábeas Data

---

Procesal Civil y Comercial provincial.

[85] Ley 4360, sancionada el 21/11/1996, promulgada el 09/12/1996, publicada el 20/12/1996.

7.6.3. Chubut

En 1996[86] se aprueba la ley Nº 4.244, que tiene por objeto la reglamentación del procedimiento de protección de los datos carácter personal que obren en registros o bancos de datos públicos pertenecientes al Estado provincial y los municipios, y en sus similares privados, estos últimos siempre y cuando estén destinados a generar y proveer de información a terceros y no se afecte el secreto de la información periodística (art. 1º) y reglamenta la acción de habeas data.

7.6.4. Río Negro

En 1998 aprueba la Ley Nº 3.246[87], regulatoria de la acción de Hábeas data.

7.6.5. Neuquén

En 1999 sanciona la Ley Nº 2.307[88] y luego adhiere a la Ley Nacional 25.326[89]. En el año 2003 se crea el Registro Provincial de Datos Personales de Neuquén[90].

7.6.6. Tucumán

En el artículo 67 del Código Procesal Constitucional[91] dispone: “Amparo informativo (hábeas data) “Cualquier persona física puede reclamar por vía del amparo, una orden judicial para conocer las informaciones relativas a su persona, que consten en registros o bancos de datos de entidades públicas o privadas, destinadas a proveer informes; el destino, uso o finalidad dado a esa información, para actualizar dichas informaciones o rectificar sus errores; para imposibilitar su uso con fines discriminatorios, para asegurar su confidencialidad, para exigir su supresión o para impedir el registro de datos relativos sus convicciones ideológicas, religiosas o

---

[86] Ley 4244, sancionada el 05/12/1996, promulgada el 19/12/1996, publicada el 31/12/1996.
[87] Sancionada el 16/11/1998. Boletín Oficial, 07/12/1998.
[88] sancionada el 07/12/1999.
[89] Ley 2399, la Provincia de Neuquén adhirió a la Ley Nacional 25.326.
[90] Decreto Nº 313/03, del 28/02/2003, publicado el 14/03/2003, crea el Registro Provincial de Datos Personales (REPRODAP).
[91] BO 12/07/1996.

políticas, a su afiliación partidaria o sindical, o a su honor, vida privada, condición social o racial o intimidad familiar y personal. Será competente para conocer en esta acción el juez en lo civil y comercial común."

7.6.7. Misiones

En el año 2001 sanciona la Ley Nº 3.794[92] que regula el procedimiento del hábeas data y crea una autoridad de aplicación en el marco de la LPDPA.

7.6.8. Mendoza

La Ley Nº 7.116[93]dispone la entrada en vigencia parcial de disposiciones de Código Procesal Penal[94], entre las que se incluye el Capítulo 4, (Habeas Corpus y Habeas Data), que corresponde a los artículos 440 al 448. El artículo 440 in fine dispone que "En lo pertinente el habeas data se regira por las disposiciones contenidas en el presente titulo. (concs. Art. 474 CPP Mza.)", que regula el Hábeas Corpus". Además, la Ley Nº 7.261 de Mendoza, crea el Registro de Empresas Privadas de Información de Deudores (R.E.P.I.D.)[95], norma sobre la que ampliaremos más adelante.

7.6.9. San Juan

En 2003 se aprueba la Ley Nº 7.447[96] cuyo artículo 1º dispone: "Las personas físicas o jurídicas, que como actividad principal o accesoria se dediquen a almacenar datos o elaborar informes para sí o para terceros sobre la situación comercial o financiera de los ciudadanos, deberán, previamente, estar debidamente inscriptas en el Registro Público de Comercio, reconocer estatutariamente esa finalidad y

---

[92] Sancionada el 25/10/01, http://www.diputadosmisiones.gov.ar/expedientes/docs/2004/sanciones/SA7321.pdf/
[93] Sancionada el 28/05/2003, promulgada por decreto 889 del 10/06/2003 y publicada: B.O. 13/06/2003.
[94] Ley 6.730 (T.O. Ley 7.007), http://www.tribunet.com.ar/tribunet/ley/6730.htm/
[95] sancionada el 31/08/2004 y publicada el 15/10/2004. El proyecto fue presentado por los Diputados Aníbal Rodríguez y Daniel Nieto en agosto de 2002 y fue sometido a un largo proceso de reglamentación, http://www.tribunet.com.ar/tribunet/ley/7261.htm/
[96] Sancionada el 20/11/2003, promulgada el 01/12/2003 y publicada el 30/01/2004, http://www.legsanjuan.gov.ar/indexley/LEYES/2003/LEY7447.DOC/

registrarse en tal carácter en la Dirección de Defensa al Consumidor.” Volveremos más adelante a un examen más amplio de la norma.

7.6.10. Ciudad Autónoma de Buenos Aires

En 2005 se aprueba la Ley Nº 1.845[97] que “tiene por objeto regular, dentro del ámbito de la Ciudad de Buenos Aires, el tratamiento de datos personales referidos a personas físicas o de existencia ideal, asentados o destinados a ser asentados en archivos, registros, bases o bancos de datos del sector público de la Ciudad de Buenos Aires, a los fines de garantizar el derecho al honor, a la intimidad y a la autodeterminación informativa, de conformidad a lo establecido por el artículo 16 de la Constitución de la Ciudad de Buenos Aires. Cuando los datos se refieran a información pública y no a datos personales será de aplicación la Ley N° 104 de la Ciudad de Buenos Aires.” (art. 1º)

El ámbito de aplicación está definido por el artículo 2º en estos términos: “A los fines de la presente ley se consideran incluidos dentro del sector público de la Ciudad de Buenos Aires a todos los archivos, registros, bases o bancos de datos de titularidad de los órganos pertenecientes a la administración central, descentralizada, de entes autárquicos, empresas y sociedades del estado, sociedades anónimas con participación estatal mayoritaria, sociedades de economía mixta y todas aquellas otras organizaciones empresariales donde el Estado de la Ciudad de Buenos Aires tenga participación en el capital o en la formación de las decisiones societarias, del Poder Legislativo y del Judicial, en cuanto a su actividad administrativa, y de los demás órganos establecidos en el Libro II de la Constitución de la Ciudad de Buenos Aires.”

La autoridad de aplicación es la Defensoría del Pueblo de la Ciudad Autónoma.

7.6.11. Entre Ríos

Se aplica la Ley 8369 de Procedimientos constitucionales[98], según lo ha

[97] aprobada el 24/11/2005; parcialmente vetada decreto Nº 1.914/005 del 04/01/2006; aceptado por Resolución N° 233 LCABA Publicación: BOCBA N° 2494 del 03/08/2006.
[98] B.O. 4/10/90, http://www.profesorgentile.com.ar/erios.html/. Ver ST Entre Ríos, 22/12/2000 “O, M.N. c/ Compañía Financiera Argentina SA”, LL Litoral 2001/424.

entendido la jurisprudencia local[99].

7.6.12. Córdoba

En 1999, se sanciona la Ley Nº 8.803[100] que regula el Derecho a la Información Pública y la Publicidad de los Actos de Gobierno, mediante una suerte de habeas data impropio, similar a la Ley 104 de la CABA. El artículo 3º señala que "No se suministra información: a) Que afecte la intimidad de las personas, ni bases de datos de domicilios o teléfonos."

Judicialmente se ha resuelto que cuando la acción de habeas data se interpone contra la Administración Pública, resulta de aplicación el trámite que rige el amparo por mora del art. 52 de la Constitución de Córdoba y la pacífica jurisprudencia de los tribunales en la materia, en la medida que tales pautas no desnaturalicen la peculiaridad de la acción.[101]

7.7. Síntesis

Argentina es considerado en el contexto de naciones de América Latina como uno de los países que cuenta con una legislación más avanzada en materia de protección de datos personales, situación que le ha permitido ser calificada por el Grupo creado por el art. 30 de la Directiva europea 95/46 como país que cumple con las exigencias de dicha normativa. En el año 2003 la Unión Europea ha otorgado a la normativa argentina la adecuación en los términos de la Directiva N° 95/46/CE, según Decisión de la Comisión Europea C(2003) 1731 del 30 de Junio de 2003.[102]

Ello no es óbice para señalar que se trata de una legislación poco conocida en

---

[99] STJ. Entre Ríos, sala 1ª, 08/11/1994, "R. R., J. E. v. Banco Francés del río de la Plata", Reseña "Hábeas data" por Marco Rufino, en JA 1996-III-1102.
[100] sancionada el 06/10/1999, publicada en el BO el 15/11/1999, http://www.adc.org.ar/recursos/594/Leycba8803%20acceso/
[101] Cám. Cont.Adm.1a Nominación Cba, 29/03/1995, "García de Llanos, Isabel c/ Caja de Jubilaciones Pensiones y Retiros de Córdoba", LLC, 1995-948, con nota de Bayo, Oscar A., ""Habeas data. Un derecho constitucional en su adecuado cauce como resultado de una decisión elogiable."
[102] El texto completo se encuentra en un vinculo en el sitio web de la DNPDP: http://www.jus.gov.ar/datospersonales/index.html/

el ámbito judicial, y de escasa aplicación integral, sobre todo en cuanto a los principios que la informan.

Para el supuesto de analizarse una reforma, sería recomendable tener en cuenta la reciente ley colombiana, que es mucho más detallada en diversas cuestiones que la norma nacional no tuvo en cuenta, además de la evolución que el tema ha tenido desde los casi diez años de su sanción.

Capítulo 8. Los informes de solvencia patrimonial y de incumplimiento de obligaciones

Sumario: Generalidades. Regulación de los servicios de información crediticia. Clases de informes crediticios. Informes sobre cumplimiento de obligaciones. Informes de solvencia. Crítica a la ley argentina. Informes crediticios en el derecho comparado. Requisitos para que se informe sobre un incumplimiento. Límite para la conservación de los informes. Agencias que brindan informes crediticios. Fuentes de los informes crediticios. Información financiera. Información sobre juicios. Información proporcionada por el acreedor. Consentimiento e información. Síntesis.

8.1. Generalidades.

Los informes crediticios, de solvencia o evaluación de riesgo pueden describirse como una especie del género datos personales, consistente en la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, así como la referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen, así como la información relativa a las demás actividades propias del sector financiero o sobre el manejo financiero o los estados financieros del titular[1]. También puede describirse como los datos de los consumidores o clientes, debidamente incorporados en una base o banco de datos, que reflejen las transacciones económicas, mercantiles, financieras o bancarias pagaderas a plazo, o "historial de crédito"

En síntesis es información de carácter personal que refleja la conducta de un sujeto en el ámbito patrimonial y que, básicamente, contiene los bienes de propiedad del concernido, sus cumplimientos e incumplimientos de obligaciones dinerarias o de contenido patrimonial, y puede incluir un análisis del riesgo que implica otorgarle crédito a esa persona. Analizaremos como ha sido regulado en el derecho nacional y comparado.

[1] Hemos adoptado el texto de la ley estatutaria 1266/08 de Colombia, por considerarla la más moderna y abarcativa de los diversos aspectos que comprende este tipo de informes.

Obviamente, también nos referiremos a las personas físicas o jurídicas que desarrollan la actividad de agencias de información crediticia, o prestan este servicio, cualquiera sea la denominación que adopten.

La expansión de la actividad de suministro de informes sobre la conducta comercial o la solvencia crediticia de las personas, tanto físicas como jurídicas, se ha convertido en fuente de numerosos conflictos, muchos de los cuales se han tratado de resolver judicialmente, por medio del hábeas data u otras vías, y esos casos constituyen el grupo más voluminoso de doctrina judicial publicada en los repertorios nacionales.

No cuestionamos la actividad, que ha merecido una regulación específica en la ley argentina, tal como ocurre, aunque con técnicas diversas, en casi todo el mundo.[2] Lo que sostenemos es que un uso inadecuado de estos informes provoca daños, cuyo detalle realizaremos más adelante.

8.2. Regulación de los servicios de información crediticia

El artículo 26 de la ley 25.326 (LPDPA) establece:

"1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio

[2] Cf. Palazzi, Pablo A, "Informes comerciales", Ed. Astrea, Buenos Aires, 2007, p. 127 (donde puede verse una excelente reseña).

del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho.

5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios".

8.2.1. Clases de informes crediticios

La LPDPA se refiere a la prestación de servicios de información sobre solvencia patrimonial y crédito desde una doble perspectiva.

En primer término menciona a los "datos personales de carácter patrimonial relativos a la solvencia económica y al crédito" y luego se refiere a "datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial"

Estas dos especies dentro del género informes comerciales o crediticios, son distintas, y aún cuando puedan coexistir en una información sobre riesgo crediticio, cada una de ellas tiene una estructura diferente y una existencia autónoma.

8.2.2. Informes sobre cumplimiento de obligaciones

Cuando estamos frente a un registro o banco de datos referido al cumplimiento o incumplimiento de obligaciones de dinero, o lo que se conoce como "historial de crédito", la información es de titularidad no sólo del deudor, sino también del acreedor. Más aún, si enfocamos la cuestión desde la perspectiva del acreedor, este es titular de un banco de datos que se nutre de los datos personales que son consecuencia de las relaciones económicas mantenidas con el deudor ("afectado" en la terminología española), cuya única finalidad es obtener la satisfacción de la obligación dineraria.

Esta es una base de datos con registros lógicos, es decir que solo admiten como atributo los signos positivo (pagó) o negativo (no pagó), carácterística más

propia de un balance.

Como situación intermedia, podríamos decir que existe un tipo de banco de datos, común a diversas personas, que unifica los datos personales contenidos en los registros de cada acreedor y tiene por finalidad proporcionar información sobre la solvencia de una persona determinada, analizada desde la perspectiva del cumplimiento o incumplimiento de las obligaciones que dicha persona registra.

8.2.3. Informes de solvencia

En cambio el llamado informe de solvencia (o de riesgo crediticio), necesariamente contiene datos referidos a la composición del activo y del pasivo, el flujo de fondos, la liquidez, y por supuesto, el registro de cumplimientos e incumplimientos crediticios, entre otros elementos a considerar.

Se trata de una operación compleja, que debe tener en cuenta varios aspectos y necesariamente debe concluir en un juicio de valor, que oriente al prestador de crédito o eventual contratante, sobre los riesgos que asumiría. Incluye el registro de incumplimientos, pero no puede agotarse en este rubro. Y como veremos, debe cumplir con el principio de calidad que hemos explicado en anteriores capítulos.

8.2.4. Crítica a la ley argentina

El texto legal argentino, contiene varias ambigüedades, por lo menos en comparación con su fuente española, ya que mezcla especies de distinta naturaleza y no es claro –en una primera lectura- sobre las consecuencias.

La ley española, en esta materia ***(art. 29, ley 15/1999)*** dice:

“1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar automatizadamente datos de carácter personal obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento.

2. Podrán tratarse, igualmente, datos de carácter personal relativos al cumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. **En estos casos se notificará a los afectados respecto de**

los que hayan registrado datos de carácter personal en ficheros automatizados, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley." (el resaltado es nuestro)

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos."

En esta norma, fuente de la LPDPA es clara la distinción entre la información sobre solvencia patrimonial y crédito con los datos personales relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Hay un registro o banco de datos que es del acreedor, que se nutre de los datos personales que son consecuencia de las relaciones económicas mantenidas con el afectado, cuya única finalidad es obtener la satisfacción de la obligación dineraria (cumplimiento o incumplimiento de obligaciones dinerarias).

Pero existe otro tipo de banco de datos, común a diversas personas, que unifica los datos personales contenidos en los registros de cada acreedor y tiene por finalidad proporcionar información sobre la solvencia de una persona determinada. Estos son los registros que elaboran las empresas prestadoras de servicios de solvencia patrimonial o cumplimiento crediticio, aunque como veremos se valgan para ello casi exclusivamente de los informes sobre cumplimiento o incumplimiento de obligaciones dinerarias.

La Agencia española de Protección de Datos, dictó la Instrucción 1/1995 (1/3/95) sobre "Prestación de servicios de información sobre solvencia patrimonial y

crédito", reglamentando este aspecto de la anterior norma, conocida como LORTAD (Ley Orgánica Regulatoria del Tratamiento Automatizado de Datos Personales, 5/92) .

Uno de los aspectos que buscó resolver la mencionada Instrucción fue la limitación de los responsables de estos bancos de datos, que al no ser el acreedor, no tendrían competencia para modificar o cancelar los datos inexactos que se encuentraran en aquellos. En función de ello, la Instrucción estableció que "la inclusión de los datos personales en los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias debe efectuarse solamente cuando concurra la existencia previa de una deuda cierta, vencida y exigible, que haya resultado impaga y medie requerimiento previo de pago a quien corresponda, en su caso, el cumplimiento de la obligación".

A pesar de ser conocida esta norma, la LPDPA omitió un agregado esencial introducido en la modificación española de 1999 que dice: "Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados **... siempre que respondan con veracidad a la situación actual de aquéllos"**[3] (el resaltado es nuestro)

Esta omisión afecta gravemente el principio de calidad establecido por el artículo 4 de la LPDP, ya que la condición de "determinante para enjuiciar la solvencia" y la exigencia de responder con veracidad a la "situación actual" del interesado es obviada por las entidades financieras y empresas prestadoras de informes de riesgo crediticio.

En general los informes que se suministran se limitan a consignar los incumplimientos denunciados por las entidades financieras al Banco Central, o las demandas que figuran presentadas ante la Cámara Nacional de Apelaciones en lo

[3] A pesar la manifestación del miembro informante en el Senado (senador Yoma) quien sostuvo: "En la prestación de servicios de información crediticia —que es un tema que ha sido motivo de opinión de organizaciones intermedias y comunitarias en el tratamiento en comisión— sólo pueden brindarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito. Es decir, en virtud de esta norma, en la prestación de servicios de información crediticia sólo pueden ser incorporados datos de carácter patrimonial que tengan que ver con la solvencia económica de las personas, y obtenidos de fuentes de acceso público o procedentes de información facilitada .por el propio interesado" (VT Senado 04/10/2000).

Comercial, y en su caso, los incumplimientos informados por las personas que mantienen contratos con las empresas de informes crediticios.

Claros ejemplos de la inobservancia del principio de calidad son los casos resueltos por la Corte Suprema de Justicia en “Martínez” y “Di Nunzio”, reseñados en el capítulo anterior, al que nos remitimos en mérito a la brevedad.

8.3. Informes crediticios en el derecho comparado

En Paraguay, la ley 1969/2002[4], modificatoria de la ley 1682/2001[5] reguló con especial detalle el tema, estableciendo: (Artículo 5º) “*Los datos de personas físicas o jurídicas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales y financieras, podrán ser publicados o difundidos solamente: a) cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente; b) cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimiento de disposiciones legales específicas; y, c) cuando consten en las fuentes públicas de información".*

*Específicamente, el artículo 6° determinó que podrán ser publicados y difundidos: “*a) Los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional; b) Cuando se trate de datos solicitados por el propio afectado; y, c) Cuando la información sea recabada en el ejercicio de sus funciones, por magistrados judiciales, fiscales, comisiones

[4] http://www.proparaguay.gov.py/?mod=ley_1969/02/

[5] El texto anterior decía: Artículo 5º: “Los datos de personas físicas o jurídicas individualizadas que revelen, describan o estimen su situación patrimonial, su solvencia económica o el cumplimiento de sus obligaciones comerciales y financieras, podrán ser publicados o difundidos solamente: Cuando esas personas hubiesen otorgado autorización expresa y por escrito para que se obtengan datos sobre el cumplimiento de sus obligaciones no reclamadas judicialmente; y, cuando se trate de informaciones o calificaciones que entidades estatales o privadas deban publicar o dar a conocer en cumplimiento de disposiciones legales específicas. Cuando consten en las fuentes públicas de información.”

parlamentarias o por otras autoridades legalmente facultadas para ese efecto.”

El principio de calidad se reflejó en el artículo 7º: “Serán actualizados permanentemente los datos personales sobre la situación patrimonial, la solvencia económica y el cumplimiento de obligaciones comerciales y financieras que de acuerdo con esta Ley pueden difundirse.

El mismo texto aclaró: “La obligación de actualizar los datos mencionados en el párrafo anterior pesan sobre las empresas, personas o entidades que almacenan, procesan y difunden esa información. Esta actualización deberá realizarse dentro de los cuatro días siguientes del momento en que llegaren a su conocimiento. Las empresas, personas o entidades que utilizan sus servicios tienen la obligación de suministrar la información pertinente a fin de que los datos que aquéllas almacenen, procesen y divulguen, se hallen permanentemente actualizados, para cuyo efecto deberán comunicar dentro de los dos días, la actualización del crédito atrasado que ha generado la inclusión del deudor. Los plazos citados precedentemente empezarán a correr a partir del reclamo realizado por parte del afectado. En caso de que los datos personales fuesen erróneos, inexactos, equívocos o incompletos, y así se acredite, el afectado tendrá derecho a que se modifiquen. La actualización, modificación o eliminación de los datos será absolutamente gratuíta, debiendo proporcionarse además, a solicitud del afectado y sin costo alguno, copia auténtica del registro alterado en la parte pertinente".

En Chile, la ley 19.628, modificada por la ley 19.812, dedicó al tema en tratamiento, el Título III, caratulado “De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial “(Artículos 17 a 19).

En primer término, delimitó los casos en los que se puede comunicar información crediticia (artículo 17): “Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios,

cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales". Y agregó: "También podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento."

En cuanto a la actualización de estos informes, el artículo 19 in fine, dispuso: "Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor." Dejó a salvo que "El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito."

Agregó que "Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información. La infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo previsto en el artículo 16."

La ley 14/2006 de Panamá, que modificó la ley 24/2002, dedicada a la regulación del historial de crédito de consumidores[6] dispuso: *"Calidad de los datos. Los datos sobre historial de crédito, brindados por los consumidores o clientes o por los agentes económicos, los manejados por las agencias de información de datos y los generados por transacciones de carácter económico, financiero, bancario, comercial o*

[6] http://www.asamblea.gob.pa/NORMAS/2000/2002/2002_522_0698.PDF/

industrial, deberán ser exactos y actualizados, de forma que respondan con veracidad a la situación real del consumidor o cliente. Con este propósito, los datos que manejen y comuniquen los agentes económicos y las agencias de información de datos reflejarán el movimiento de los pagos, los abonos y las cancelaciones de las obligaciones del consumidor o cliente, así como cualquier otra información producto del tratamiento de los datos de este, que faciliten la comprensión y el análisis de su historial de crédito." (art. 4).

En Colombia, que recién a fines de 2008 puso en vigencia su ley sobre protección de datos, la *Circular Básica Contable y Financiera de la Superintendencia Bancaria estableció la* reglas de gestión del "riesgo crediticio"[7]. En el caso de la información financiera y crediticia proveniente de las centrales de riesgo se dispuso que las entidades vigiladas deben cuidar que la misma sea veraz, completa y actualizada[8], a cuyo fin deben diseñar y establecer los mecanismos idóneos que aseguren el adecuado flujo de la información de manera tal que, en todo momento, se garantice la efectiva protección de los derechos constitucionales consagrados en favor de los titulares de tal información"[9].

También dispuso que "a solicitud de cada cliente, dentro de los diez (10) días siguientes a la respectiva solicitud, la entidad financiera acreedora deberá comunicarle la última calificación y clasificación de riesgo que le ha asignado, junto con los fundamentos que la justifican según la evaluación correspondiente realizada por la entidad. (...) los clientes deberán ser notificados de que tienen acceso a esta

---

[7] Circular Externa 052/2004 de la SBC, diciembre 2004.
[8] Al regular el sistema de actualización de datos (SARC) el artículo 2.4.5.1. dice: "Un mecanismo que permita reflejar de manera ágil e inmediata cualquier cambio en la situación de pago del deudor, de manera que la información sobre él sea veraz, completa y actualizada, en forma acorde con el derecho fundamental al habeas data."
[9] 2.4.6. Mecanismos de divulgación en relación con las centrales de riesgo: El SARC debe contar con mecanismos de información periódica (carteleras, folletos, información adjunta a los extractos, Internet, etc.) a los clientes y deudores de la entidad acerca del alcance de sus convenios con centrales de riesgos, de los efectos generales que conlleva el reporte a las mismas y de las reglas internas sobre permanencia del dato que hayan adoptado tales centrales de riesgos teniendo en cuenta la jurisprudencia constitucional y los mandatos que se establezcan en las normas legales aplicables.

información, en el momento en que se solicita u otorga el crédito o contrato"[10]. "Las entidades deben considerar la información proveniente de las centrales de riesgo al momento de hacer la evaluación de riesgo crediticio de sus deudores presentes y futuros". "Tales reportes no son, y en ningún caso pueden llegar a serlo, los únicos elementos de juicio que las entidades vigiladas deben considerar para tomar decisiones sobre otorgamiento de crédito". "Los reportes originados en tales centrales de riesgo son un instrumento adicional que, junto con la información financiera reportada por los solicitantes, por las calificadoras de riesgo cuando existan calificaciones o por cualquier otra fuente que resulte pertinente, le permitan a las entidades hacer una adecuada evaluación de la capacidad de pago esperada del deudor y por lo tanto, a partir del respectivo análisis, asumir o no riesgos con el otorgamiento de crédito". (…) "dado que todas las personas tienen el derecho constitucional a conocer, actualizar y rectificar la información que se hayan recogido sobre ellas en las bases de datos y en archivos de entidades públicas y privadas, derecho de cuyo alcance y contenido se ha ocupado en diferentes oportunidades la Honorable Corte Constitucional en pronunciamientos que tienen efectos generales, la Superintendencia Bancaria considera que las instituciones vigiladas tienen el deber de diseñar e implementar los mecanismos operativos que resulten necesarios para que se garanticen de manera eficaz los mencionados derechos constitucionales en favor de los usuarios del sistema financiero".

La Corte Constitucional de Colombia había señalado que, dentro de la autodeterminación informática, entendida como la facultad de la persona a la cual se refieren los datos, para autorizar su conservación, uso y circulación, de conformidad con las regulaciones legales, la libertad económica, en especial, podría ser vulnerada al restringirse indebidamente en virtud de la circulación de datos que no sean veraces, o que no haya sido autorizada por la persona concernida o por la ley; y que la actualización y rectificación de los datos contrarios a la verdad, son, en principio,

[10] 2.4.4."Información a suministrar al deudor: Dentro de los diez (10) días siguientes a la respectiva solicitud del cliente, la entidad financiera acreedora deberá comunicarle la última calificación y clasificación de riesgo que le ha asignado, junto con los fundamentos que la justifican según la evaluación correspondiente realizada por la entidad. Como se indicó en el literal a del numeral 1.3.2.3.1 de este capítulo, en el momento en que se solicita u otorga el crédito, el cliente deberá ser ilustrado acerca de su derecho a obtener esta información".

obligaciones de quien maneja el banco de datos. Ergo, si él no las cumple, la persona concernida puede exigir su cumplimiento, dado que el conflicto entre el derecho al buen nombre y el derecho a la información, se presenta cuando aquél se vulnera por la divulgación de ésta, dado que la información debe corresponder a la verdad, ser veraz, pues no existe derecho a divulgar información que no sea cierta.

En el año 2007 el Congreso de Colombia sancionó la ley 221-07, que contiene las disposiciones generales del Hábeas Data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países, y otras disposiciones[11]. La Corte Constitucional el 16 de octubre de 2008 declaró "exequible"[12] en su aspecto formal a esta norma, por lo que la misma ha comenzado a regir, bajo el título de Ley Estatutaria 1266/2008[13].

Una de las precisiones que trae la nueva ley colombiana es la definición de usuario, en estos términos: "d) Usuario. El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el

[11] Puede consultarse el texto completo en http://www.habeasdata.org/colombia-texto-fnal/

[12] Esta expresión, cuyo significado literal sería "accesible", se refiere a un procedimiento previsto por el art. 167 de la Constitución de Colombia, que habilita a la Corte Constitucional a examinar la constitucionalidad de una norma cuando ésta ha sido objetada total o parcialmente por el Ejecutivo, pero ha sido insistida por ambas Cámaras. El texto mencionado dice: "*Artículo 167. El proyecto de ley objetado total o parcialmente por el Gobierno volverá a las Cámaras a segundo debate. El Presidente sancionará sin poder presentar objeciones el proyecto que, reconsiderado, fuere aprobado por la mitad más uno de los miembros de una y otra Cámara. Exceptúase el caso en que el proyecto fuere objetado por inconstitucional. En tal evento, si las Cámaras insistieren, el proyecto pasará a la Corte Constitucional para que ella, dentro de los seis días siguientes decida sobre su exequibilidad. El fallo de la Corte obliga al Presidente a sancionar la ley. Si lo declara inexequible, se archivará el proyecto. Si la Corte considera que el proyecto es parcialmente inexequible, así lo indicará a la Cámara en que tuvo su origen para que, oído el Ministro del ramo, rehaga e integre las disposiciones afectadas en términos concordantes con el dictamen de la Corte. Una vez cumplido este trámite, remitirá a la Corte el proyecto para fallo definitivo. Artículo 168. Si el Presidente no cumpliere el deber de sancionar las leyes en los términos y según las condiciones que la Constitución establece, las sancionará y promulgará el Presidente del Congreso."*

[13] Ver http://www.corteconstitucional.gov.co/ - Expte P-029 Sentencia C-1011/08

operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos". La Suprema Corte de Justicia de Mendoza tuvo de dilucidar un caso en el que –sin mencionar esta ley- aplicó correctamente el mismo criterio[14].

El título IV de la ley colombiana está referido a los "bancos de datos de información crediticia" con varios principios interesantes.

El "principio de favorecimiento a una actividad de interés público" implica que "la actividad de administración de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países está directamente relacionada y favorece una actividad de interés público, como lo es la actividad financiera propiamente, por cuanto ayuda a la democratización del crédito, promueve el desarrollo de la actividad de crédito, la protección de la confianza pública en el sistema financiero y la estabilidad del mismo, y genera otros beneficios para la economía nacional y en especial para la actividad financiera, crediticia, comercial y de servicios del país".

Adviértase que incluye entre los fines de la actividad la "democratización del crédito", expresión que se reitera en el parágrafo 1° del artículo 10º, al señalar que *la administración de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, por parte de fuentes, usuarios y operadores deberá realizarse de forma que permita favorecer los fines de expansión y democratización del crédito.*

En cuanto al modo de analizar y evaluar este tipo de información, se indica que debe hacerse "en forma concurrente con otros factores o elementos de juicio que técnicamente inciden en el estudio de riesgo y el análisis crediticio, y no podrán

[14] SCJ Mza, 16/~~02/2009~~02/2009, "Albares, Raúl O. en j. 216.691/31.210 Albares Raúl c/Bco. Galicia p/habeas data s/inc.cas", LLGran Cuyo 2009 (marzo), 157; LA LEY 2009-B, 247, LLGran Cuyo 2009 (abril), 223.

basarse exclusivamente en la información relativa al incumplimiento de obligaciones suministrada por los operadores para adoptar decisiones frente a solicitudes de crédito". Y en este aspecto es donde se advierte la diferencia esencial con la práctica que se lleva a cabo en nuestro país, o al menos, la que genera la mayor cantidad de litigios.

En sentido coincidente, la ya mencionada "Fair Credit Reporting Act"[15], había señalado que "el sistema de actividades bancarias depende de la divulgación justa y exacta del crédito. Los informes de crédito inexactos deterioran directamente la eficacia del sistema de actividades bancarias, y los métodos injustos de la divulgación de crédito minan la confianza pública que es esencial para el funcionamiento continuado del sistema de actividades bancarias." Y por ello es necesario "*que las agencias de información sobre consumidores adoptan los procedimientos razonables para resolver las necesidades del comercio del crédito al consumidor, del personal, del seguro, y de otra información de una manera que sea justa y equitativa al consumidor, con respecto al secreto, a la exactitud, a la importancia, y a la utilización apropiada de tal información de acuerdo con los requisitos de este título*."

8.4. Requisitos para que se informe sobre un incumplimiento

La reglamentación española a la que nos hemos referido también establece que no pueden incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba documental que aparentemente contradiga alguno de los requisitos anteriores y que tal circunstancia determina igualmente la desaparición cautelar del dato personal desfavorable en los supuestos en los que ya se hubiera efectuado su inclusión en el fichero.

Lo destacable es la exigencia para el acreedor, o quien actúe por su cuenta e interés, de asegurarse que concurran todos los requisitos exigidos en esta norma en el momento de notificar los datos adversos al responsable del fichero común. Se especifica que la carga de comunicar el dato inexistente o inexacto, con el fin de obtener su cancelación o modificación, debe efectuarla el acreedor o quien actúe por

[15] Sección (§) 1681, del Título 15, capítulo 41, subcapítulo III del Código de Estados Unidos (U.S. Code), subsecciones o parágrafos 601 a 625.

su cuenta, al responsable del fichero común en el mínimo tiempo posible, y en todo caso en una semana.

En cuanto a la metodología para registrar una obligación incumplida, indica que debe hacerse en un sólo asiento si fuese de vencimiento único, o en tantos asientos como vencimientos periódicos incumplidos existan señalando, en este caso, la fecha de cada uno de ellos. Es necesario efectuar una notificación por cada deuda concreta y determinada con independencia de que esta se tenga con el mismo o con distintos acreedores, estando a cargo del responsable del fichero adoptar las medidas organizativas y técnicas necesarias que permitan acreditar la realización material del envío de notificación y fecha de entrega o intento de entrega de la misma. La notificación se hace a la ultima dirección conocida del afectado a través de un medio fiable e independiente del responsable del fichero.

En Paraguay, (art. 9°) de la ley no autoriza la divulgación de informes en los siguientes casos: a) pasados tres años de la inscripción de deudas vencidas no reclamadas judicialmente; b) pasados tres años del momento en que las obligaciones reclamadas judicialmente hayan sido canceladas por el deudor o extinguidas de modo legal; c) sobre juicios de convocatoria de acreedores después de cinco años de la resolución judicial que la admita.” Y además obliga a las empresas o entidades que suministran información sobre la situación patrimonial, la solvencia económica y el cumplimiento de compromisos comerciales y financieros, a implementar mecanismos informáticos que de manera automática eliminen de su sistema de información los datos no publicables, conforme se cumplan los plazos establecidos en la ley.

La ley colombiana impone a las fuentes una serie de deberes (art. 12)**;** tales como actualizar mensualmente la información suministrada al operador pero, además, el reporte de información negativa sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los operadores de Bancos de Datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, sólo procederá previa comunicación al titular de la información, con el fin de que este pueda demostrar o efectuar el pago de la obligación, así como controvertir aspectos tales como el monto de la obligación o cuota y la fecha de exigibilidad. Dicha comunicación podrá incluirse en los extractos periódicos que las fuentes de información envíen a sus clientes.

En todo caso, las fuentes de información podrán efectuar el reporte de la información transcurridos veinte (20) días calendario siguientes a la fecha de envío de la comunicación en la última dirección de domicilio del afectado que se encuentre registrada en los archivos de la fuente de la información y sin perjuicio, si es del caso, de dar cumplimiento a la obligación de informar al operador, que la información se encuentra en discusión por parte de su titular, cuando se haya presentado solicitud de rectificación o actualización y esta aún no haya sido resuelta.

Estas cargas desaparecieron del texto de la LPDPA, con la excusa de los altos costos de notificar a los presuntos deudores, antes de incluirlos en informes negativos, con la inevitable consecuencia de numerosos errores o inexactitudes que provocan daños, como se verá en el capítulo siguiente.

8.5. Límite para la conservación de los informes.

Un aspecto que aún genera debate es el referido al tiempo de conservación de los informes de crédito negativos, que a pesar de haber sido limitado a cinco años por la Ley 25.326 (art. 26), sigue mereciendo interpretaciones distintas.

Poco antes de sancionarse la LPDPA hubo un pronunciamiento judicial que había iniciado la revisión del criterio decenal que venía reflejando la jurisprudencia[16].

En España, el limite es de seis años, cuando "sean determinantes para enjuiciar la solvencia económica de los interesados y siempre que respondan con veracidad a la situación actual de aquéllos" (art. 29 inciso 4 Ley 15-1999).

La Fair Credit Reporting Act establece en siete años el límite de conservación de los informes.

En Paraguay, ya hemos citado los plazos de la la ley 1682 (modificada por ley

[16] CNCom, sala C, 18/08/2000, “Scarpia, Juan C. c/ Organización Veraz S.A.”, LA LEY 2001-B, 298. Debe citarse también el fallo de Graciela Medina, por entonces jueza de primera instancia, in re “Falcionelli, Esteban P. v. Organización Veraz S.A. s/ amparo”, JNPICiv 91, 05/03/1996, no confirmada por la sala G de la Cámara, con nota de Palazzi, Pablo, “El hábeas data y el "derecho al olvido", JA, 1997-I, 33; http://www.gracielamedina.com/

1969).

En Chile, la Ley 19628 en su artículo 18, establecía en siete años el plazo máximo de conservación de estos datos y lo reducía a tres años, cuando la obligación se había cancelado, pero la reforma de la ley 19.812 redujo y unificó el plazo en cinco años.[17]

Sin embargo, se aclara que "El pago o la extinción de estas obligaciones por cualquier otro modo no produce la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente."

La Ley sobre Bureau de información Crediticia de Ecuador 2005-13[18] establece en seis años el plazo de conservación de los datos crediticios.

La ley 27.489 de Perú, que regula las centrales privadas de información de riesgos y de protección al titular de la información (CEPIR)[19], indica (art. 10º) que las CEPIRS no podrán contener en sus bancos de datos ni difundir en sus reportes de crédito entre otros supuestos la siguiente información: Información referida al incumplimiento de obligaciones de naturaleza civil, comercial o tributaria, cuando (i) hayan transcurrido 5 (cinco) años desde que la obligación fue pagada o extinguida en forma total o (ii) haya prescrito el plazo legal para exigir su cumplimiento, lo que suceda primero; Información referida a sanciones exigibles de naturaleza tributaria, administrativa u otras análogas, de contenido económico, cuando (i) hayan transcurrido 5 (cinco) años desde que se ejecutó la sanción impuesta al infractor o se extinguió por cualquier otro medio legal, o (ii) haya prescrito el plazo legal para exigir su ejecución, lo que suceda primero; Información referida a la insolvencia o quiebra del

[17] Artículo 18 Ley 19.628 de Chile, modificada por la Ley 19.812: “En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible. Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal”.

[18] http://www.habeasdata.org/Ecuador-Ley-de-Buros-de-informacion-Informes-crediticios/

[19] Publicada 28/06/2001, http://www.habeasdata.org/Peru-Ley-informes-comerciales/

titular de la información, cuando hayan transcurrido 5 (cinco) años desde que se levantó el estado de insolvencia o desde que se declaró la quiebra.

La ley 17.838 de Uruguay[20] dispone (artículo 9º): “Los datos personales relativos a obligaciones de carácter comercial sólo podrán estar registrados por un plazo de cinco años contados desde su incorporación. En caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al titular de la base de datos, por única vez, su nuevo registro por otros cinco años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original. Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción.”

En Colombia, la Corte Constitucional habia expresado que “Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de "personas virtuales" que afecten negativamente a sus titulares, vale decir, a las personas reales. De otra parte, es bien sabido que las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia después de algún tiempo tales personas son titulares de un verdadero derecho al olvido".[21]

La ley colombiana estableció que la información de carácter positivo permanecerá de manera indefinida en los Bancos de Datos de los operadores de información. Los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera, y en general, aquellos datos referentes a una situación de incumplimiento de obligaciones, se regirán por un término máximo de permanencia, vencido el cual deberá ser retirada de los Bancos de Datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información. El término de permanencia de esta información será de cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea pagada la obligación vencida.

---

[20] Publicada D.O., 01/10/2004, Nº 26599, http://www.parlamento.gub.uy/Leyes/Ley17838.htm/

[21] Corte Constitucional de Colombia, sala Primera de Revisión, sentencia T-414/1992.

La Corte Constitucional de Colombia, al analizar este artículo resolvió: declarar ***exequible*** el artículo 13 del Proyecto de Ley objeto de revisión, *"en el entendido que la caducidad del dato financiero en caso de mora inferior a dos años, no podrá exceder el doble de la mora, y que el término de permanencia de cuatro años también se contará a partir del momento en que se extinga la obligación por cualquier modo".*

La sala C de la Cámara Nacional en lo Comercial se ha expedido en torno a esta cuestión y el llamado "derecho al olvido". En dos oportunidades ha señalado que "*El inc. 4º del art. 26 de la ley 25.326 establece que sólo se podrán archivar, ceder o registrar los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Así, dicho plazo deberá contarse desde el momento en que el banco verificó la mora de la deudora ya que esta fue la última información significativa que reveló la existencia de una deuda exigible, ya que de allí en más, la entidad bancaria sólo repitió esa misma información por seis años más. De tal suerte, deberá ser revocado el fallo apelado, en el cual fue propiciado computar el plazo del art. 26 citado, desde la fecha de la última información adversa pues, admitir esa interpretación permitiría al banco informante postergar sine die el transcurso del plazo de caducidad a través del simple recurso de repetir mensualmente la información registrada, lo que desnaturalizaría el derecho al olvido tutelado por el ley 25.326".*[22]

Distinta posición ha asumido la sala C de la Cámara Nacional en lo Civil, quien ha sostenido que "El hecho que la ley de protección de datos personales fije un plazo durante el cual deben ser archivados, registrados o cedidos datos que resulten significativos para evaluar la solvencia económica-financiera de un particular, no implica que obligue a suprimir asientos que son fidedignos, es decir que responden a hechos ciertos -en el caso, el actor reconoció la vigencia de la deuda publicada-, aun cuando éstos se remonten a una época que exceda ese término."[23] Esta ha sido la línea que siguió la Dirección Nacional de Protección de Datos Personales en su

[22] CNCom, sala C, 2007/06/28, "Torri Marta Laura c/ Bankboston N.A. s/ amparo", Microjuris: MJJ14105; CNCom, sala C, 06/07/2007, "Carballo Alberto Rubén c/ Hexagon Bank Argentina S.A s/ amparo", Microjuris: MJJ14558 y diariojudicial.com 07/08/2007.

[23] CNCiv, sala C, 03/06/2004, "D., C, A. c/ Lloyds Bank TSB Bank", LA LEY 19/10/2004, 5.

Dictamen 61/05.[24]

Más recientemente, la sala D de la Cámara Nacional en lo Comercial resolvió que “La repetición de la información no es susceptible de suspender o interrumpir el plazo de caducidad, ”[25] entendiendo que el cómputo del plazo establecido por la ley 25326 (art. 26 inc.4) y el decreto reglamentario, no admite la discusión respecto a si debe iniciarse al hacerse exigible la obligación o al publicarse los datos, cuando ello se refiere a la misma deuda, con idéntica causa y por igual monto; pues el hecho que la entidad acreedora continúe enviando esos datos con o sin solución de continuidad, no importa el desplazamiento del dies a quo a la última comunicación; ya que, de ser interpretada la norma de ese modo, se caería en la incongruencia de otorgar a los acreedores la facultad de evitar sine die el denominado "derecho al olvido"; de tal manera, la repetición de la información anterior no es susceptible de suspender o interrumpir el plazo de caducidad.[26]

Creemos que la interpretación correcta es la de la Cámara Nacional en lo Comercial, sin perjuicio del nuevo criterio de la Dirección Nacional, conforme a su Dictamen 150/07[27], en el que adecuó su interpretación a lo indicado por la Procuración

---

[24] Expte. 144810/04 MJyDH, Dictamen 61/05. La DNPDP sostuvo que “1) El plazo de caducidad se aplica al servicio de información crediticia y no a la fuente del dato, en este caso Citibank N.A., quien como tal tiene la obligación de brindar la información de conformidad a los principios de la ley. 2) El plazo de 5 años de información archivada por la empresa de riesgo crediticio se computará a partir de la última información difundida por fuente legítima (el titular del dato, el acreedor, fuentes de acceso publico, cfr. artículo 26 Ley Nº 25.326). 3) Para la reducción del plazo a 2 años, el deudor debe acreditar ante la empresa de riesgo crediticio que ha cancelado o de cualquier modo se ha extinguido la deuda; ello sin perjuicio que la empresa de riesgos crediticios deba suprimir el dato cuando por otros medios tome conocimiento, o tenga la obligación de conocer, sobre la extinción o cancelación de la deuda (cfr. artículo 4º de la Ley Nº 25.326)” 3) Para la reducción del plazo a 2 años, el deudor debe acreditar ante la empresa de riesgo crediticio que ha cancelado o de cualquier modo se ha extinguido la deuda; ello sin perjuicio que la empresa de riesgos crediticios deba suprimir el dato cuando por otros medios tome conocimiento, o tenga la obligación de conocer, sobre la extinción o cancelación de la deuda (cfr. artículo 4º de la Ley Nº 25.326).”, http://www.jus.gov.ar/dnpdpnew/

[25] CNCom, sala D, 19/03/2009, "Sciarreta Claudio Alberto c/Equity Trust Company Argentina SA FID Fidec Renova s/ amparo", elDial AA52C7.

[26] En el mismo sentido, CNCom., sala E, 07/11/2007, "Segretin, Carlos c/ ABN Amro Bank NV Sucursal Argentina s/sumarísimo", elDial AA4597.

[27] Actuación 366/1381 B.C.R.A. del 27/09/2007, http://www.jus.gov.ar/dnpdpnew/

del Tesoro de la Nación, diciendo que “debe computarse el plazo de los cinco años que establece el artículo 26, inciso 4º, de la Ley Nº 25.326, desde que la obligación se tornó exigible, por considerarse que esta es la última información adversa que revela que dicha deuda era exigible, en los términos del artículo 26 de reglamentación aprobada por el Decreto 1558/01.”

En dicho dictamen se distingue entre las obligaciones con vencimiento único y las de vencimientos múltiples[28], aclarando que si se trata de obligaciones con vencimiento único o en cuotas, el plazo del denominado derecho al olvido comienza a correr a partir de la fecha en la que la deuda se tornó exigible, es decir, con prescindencia de la prescripción. En los casos de obligaciones con vencimiento único la mora se configura en el momento estipulado para el cumplimiento del total de la obligación y la información susceptible de ser incluida en la central de deudores sería la relacionada con el total de lo adeudado. En los casos de obligaciones en cuotas, la mora y, consecuentemente, el inicio del plazo del derecho al olvido se produce con el vencimiento de la primera cuota impaga y se interrumpe y reinicia con cada nuevo vencimiento en tanto el banco acreedor no haga uso de la facultad de dar por decaídos todos los plazos y exigir el pago de la totalidad de la deuda. Dentro de ese plazo y en virtud del principio de integridad del pago, se puede informar la totalidad de la deuda existente desde el inicio de la obligación.

Otro aspecto digno de tener en cuenta en esta materia es el referido al tiempo de conservación de los informes, limitado a cinco años, aunque ya existía un pronunciamiento judicial que había iniciado la revisión del criterio decenal que venía reflejando la jurisprudencia[29].

8.6. Agencias que brindan informes crediticios.

En España, las empresas que se dedican a proveer este tipo de informes deben someterse a auditorías que dictaminan sobre la adecuación de las medidas y

[28] Siguiendo el criterio del servicio jurídico permanente del B.C.R.A., en el Dictamen S.E.F.y C. Nº 178/07.
[29] CNCom., sala C, 18/08/2000, “Scarpia, Juan C. c/ Organización Veraz S.A”, LA LEY , 2001-B, 298.

controles destinados a garantizar la integridad y la confidencialidad de los datos personales almacenados o tratados, identificar sus deficiencias e insuficiencias y proponer las medidas correctoras o complementarias necesarias[30]. En nuestro país se dictó la Disposición 11/2006 de la Dirección Nacional de Protección de Datos Personales, y en el año 2008 se publicó el inicio de inspecciones a diversas entidades que tienen bases de datos personales. Esta actividad es fundamental para controlar adecuadamente esta actividad, que está afectando seriamente a muchas personas, aun cuando sean cuestiones que no lesionan necesariamente el derecho a la intimidad o privacidad, pero que sí pueden ocasionar daño si se emplean arbitrariamente[31].

En México, la ya mencionada Ley de Sociedades de Información crediticia[32], establece que para constituirse y operar como "Sociedad de Información Crediticia" se requerirá autorización del Gobierno Federal, por intermedio de la Secretaría Hacienda y Crédito Público, oyendo la opinión del Banco de México y de la Comisión Nacional Bancaria y de Valores y serán intransmisibles (art. 6°)[33]. Estas sociedades deben

---

[30] Ver Real Decreto 1720/2007, 21/12/2007, que aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, BOE Nº 17, 19/01/2008, http://www.boe.es/aeboe/consultas/bases_datos/doc.php?coleccion=iberlex&id=2008/00979/

[31] La Disposición de la DNPDP 11/2006 fue publicada en el BO 30996 del 22/09/2006 y fue modificada por la Disposicion 9/2008, publicada en BO 31481 del 03/09/2008.

[32] Sancionada el 27/12/2001, promulgada el 14/01/2002. Un análisis más extenso de la normativa mejicana puede consultarse en del Villar, Rafael. "Consideraciones económicas de la regulación de Sociedades de Información Crediticia: El Caso de México", ponencia presentada en "Seminario-Taller sobre Datos Personales, Internet y Sistemas Judiciales", Heredia, Costa Rica, 8 y 9/07/2003: http://www.iijusticia.edu.ar/Seminario_Taller/textos.htm/

[33] A su vez, según el artículo 7º, "La solicitud para constituirse y operar como Sociedad deberá contener lo siguiente: I. Relación de accionistas indicando el capital que cada uno de ellos suscribirá y pagará así como, en su caso, sus currícula vitarum; II. Relación de los consejeros y principales funcionarios de la Sociedad, incluyendo a aquellos que ocupen cargos con la jerarquía inmediata inferior a la del director general, así como su currícula vitarum; III. Proyecto de estatutos sociales; IV. Acreditar que se cuenta con los recursos para aportar el capital a que se refiere el artículo 8º de la presente ley. V. Programa general de funcionamiento, que comprenda por lo menos: 1. La descripción de los sistemas de cómputo y procesos de recopilación y manejo de información; 2. Las características de los productos y servicios que prestarán a los Usuarios y a los Clientes; 3. Las políticas de prestación de servicios con que pretenden operar; 4. Las medidas de seguridad y control a fin de evitar el manejo indebido de la información; 5. Las bases de organización; 6. El programa detallado de inversión a tres años, y 7. El calendario de apertura de oficinas y plazas en que se

contar con un capital mínimo, íntegramente suscrito y pagado, el cual será determinado por la Comisión mediante disposiciones de carácter general. Las acciones representativas del capital social de las Sociedades serán de libre suscripción; sin embargo, no podrán participar en forma alguna en el capital social de las Sociedades, personas morales extranjeras que ejerzan funciones de autoridad.

El nombramiento de los consejeros y del director general de las Sociedades deberá recaer en personas de reconocida calidad técnica, honorabilidad e historial crediticio satisfactorio, así como de amplios conocimientos y experiencia en materia financiera o administrativa.[34]

Incluso cualquier modificación a los estatutos sociales de las Sociedades deberá ser sometida a la aprobación previa de la Secretaría, para su posterior inscripción en el Registro Público de Comercio.

La ley de Panamá también contiene requisitos especiales para las Agencias de

---

ubicarán. VI. La demás información y documentación conexa que la Secretaría le solicite por escrito a efecto de evaluar la solicitud respectiva."

[34] El art. 9º dispone que "en ningún caso podrán ocupar los cargos a que alude el párrafo anterior: I. Las personas condenadas por sentencia definitiva por delitos intencionales, las inhabilitadas para ejercer el comercio o para desempeñar un empleo, cargo o comisión en el servicio público, o en el sistema financiero mexicano, durante el tiempo que dure su inhabilitación; II. Los quebrados y concursados que no hayan sido rehabilitados, y III. Quienes realicen funciones de regulación, inspección o vigilancia respecto de las Sociedades. No podrán ser funcionarios de las Sociedades quienes presten sus servicios en cualquier Usuario, Entidad Financiera o Empresa Comercial, cuando tal circunstancia genere un conflicto de intereses, a juicio de la Comisión. La Sociedad deberá verificar que las personas que sean designadas como consejeros y director general cumplan, con anterioridad al inicio de sus gestiones, con los requisitos señalados en este artículo. La Comisión podrá establecer, mediante disposiciones de carácter general, los criterios mediante los cuales se deberán integrar los expedientes que acrediten el cumplimiento de lo señalado en el presente artículo. Las Sociedades deberán informar a la Comisión los nombramientos de consejeros y del director general dentro de los cinco días hábiles posteriores a su designación, manifestando expresamente que los mismos cumplen con los requisitos aplicables. La Comisión, oyendo previamente al interesado y a la Sociedad afectada, podrá determinar que se proceda a la suspensión de uno o más de los miembros del consejo de administración y del director general de la Sociedad, cuando no cuenten con la suficiente calidad técnica, honorabilidad e historial crediticio satisfactorio para el desempeño de sus funciones, o incurran de manera grave o reiterada en infracciones a la presente ley o a las disposiciones de carácter general que de ella deriven."

Información de datos (arts. 11 y ss ley 24/2002).

La ley peruana 27.489 entiende por “Centrales privadas de información de riesgos” (CEPIRS), a las empresas que en locales abiertos al público y en forma habitual recolecten y traten 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. No se consideran CEPIRS, para efectos de la presente Ley, a las entidades de la administración pública que tengan a su cargo registros o bancos de datos que almacenen información con el propósito de darle publicidad con carácter general, sin importar la forma como se haga pública dicha información.”

La ley ecuatoriana regula los “Burós de información crediticia (burós)”, a los que caracteriza como las sociedades anónimas cuyo objeto social exclusivo es la prestación de servicios de referencias crediticias del titular de la información crediticia.

8.7. Fuentes de los informes crediticios

La información básica que por lo general difunden las empresas de informes de riesgo crediticio abarca los siguientes rubros:

a) Información financiera, que tiene como fuente al Banco Central de la República Argentina (BCRA)[35´].

b) Información sobre juicios iniciados

c) Cheques rechazados y cuentacorrentistas inhabilitados, que tiene como fuente al BCRA[36].

d) Información societaria, que incluye sociedades inscriptas, socios, directores, gerentes, entre otros datos y se obtiene del Boletín Oficial y/o el Registro Público de Comercio.

---

[35] Fuente: http://www.bcra.gov.ar/

[36] La información que contiene la Central de Cheques Rechazados del BCRA es difundida de acuerdo con los criterios establecidos en las Comunicaciones "B" 7074 y 8103 del 21/12/2001 y 09/01/2004, respectivamente.

e) Deudas informadas por el acreedor.

El concepto de fuente no figura en el glosario del artículo 2 de la LPDPA, pero está implícito, por un lado en la noción de cedente de datos, y por otra lado, la norma solo excluye de su ámbito a las “fuentes de información periodística”.

La ley colombiana, en este aspecto, cubre este aparente vacío, al regular expresamente que “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 o de cualquier otra índole 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 al usuario final”. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos (art. 31 inc. b).

También impone deberes a las fuentes de la información, que consisten en garantizar que la información que se suministre a los operadores de los Bancos de Datos o a los usuarios sea veraz, completa, exacta, actualizada y comprobable (principio de calidad); reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada; rectificar la información cuando sea incorrecta e informar lo pertinente a los operadores; diseñar e implementar mecanismos eficaces para reportar oportunamente la información al operador; solicitar, cuando sea del caso, y conservar copia o evidencia de la respectiva autorización otorgada por los titulares de la información, y asegurarse de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado, cuando dicha autorización sea necesaria, de conformidad con lo previsto en la ley; certificar, semestralmente al operador, que la información suministrada cuenta con la autorización de conformidad con lo previsto en la presente ley; resolver los reclamos y peticiones del titular en la forma en que se regula en la ley; informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de

rectificación o actualización de la misma, con el fin de que el operador incluya en el Banco de Datos una mención en ese sentido hasta que se haya finalizado dicho trámite; cumplir con las instrucciones que imparta la autoridad de control en relación con el cumplimiento de la presente ley y los demás que se deriven de la Constitución o de la ley.

Como puede advertirse, se trata de una legislación moderna, que ubica adecuadamente la función que cumplen quienes proveen información y contribuye a la efectiva vigencia de los principios para el tratamiento de datos personales que hemos comentado en el capítulo anterior.

Repasaremos ahora las principales fuentes de información que suministran datos patrimoniales a las empresas que luego procesan y divulgan los informes crediticios o comerciales.

8.7.1. Información financiera

La Central de Deudores del Sistema Financiero clasifica a los deudores en dos grandes grupos: Cartera de consumo y vivienda y Cartera comercial (incluye datos de cumplimiento e incumplimiento, o sea, positivos y negativos), aunque algunas empresas de informes operan con entidades financieras como fuente directa.

El funcionamiento de esta Central está regulado por el B.C.R.A.[37] el que ha establecido pautas para la calificación de cumplimiento de los clientes del sistema financiero. Esta tarea de clasificación o calificación de deudores es realizada por cada entidad de crédito en forma obligatoria y periódica.

Uno de los aspectos más importantes, y paradójicamente, desconocidos por su

---

[37] Ver http://www.bcra.gov.ar. La reglamentación de la CDSF ha sufrido diversas modificaciones, cuyo análisis excede largamente el objeto de este trabajo, pero recomendamos el trabajo de Dubié, Pedro, “El habeas data financiero”, LA LEY 2002-B, 1009 y del mismo autor, “Análisis del debate parlamentario del hábeas data con relación a la información crediticia”, JA 1999 Tomo II, 894, así como Livellara, Silvina, “Habeas Data e información crediticia. La eventual responsabilidad civil de las entidades financieras y del Banco Central de la República Argentina por cesión y publicidad de datos inexactos.”, elDial DC2A7.

falta de aplicación, es la obligación que esta norma impone a las entidades financieras, de informar a cada persona la calificación que le ha asignado. "A solicitud de cada cliente, dentro de los 10 días corridos del pedido, la entidad financiera deberá comunicarle la última clasificación que le ha asignado, junto con los fundamentos que la justifican según la evaluación realizada por la entidad, el importe total de deudas con el sistema financiero y las clasificaciones asignadas que surjan de la última información disponible en la "Central de deudores del sistema financiero".Los clientes deberán ser notificados de que tienen la posibilidad de requerir esos datos, en el momento de presentarse las solicitudes de crédito, mediante una formula independiente de ellas." (art. 8.1. Com.2729/1998).

8.7.2. Información sobre juicios

La Cámara Nacional de Apelaciones en lo Comercial difunde diariamente el listado de presentaciones efectuado ante su Mesa General receptora[38], sin perjuicio de otros tribunales provinciales que también observan prácticas similares.

Hemos señalado reiteradamente la gravedad de ciertas prácticas tribunalicias, entre las que se destaca la de la Cámara Nacional de Apelaciones en lo Comercial.

El artículo 52 del Reglamento para la Justicia Nacional en lo Comercial dispone que los juicios iniciados, con la simple asignación de juzgado, pero sin siquiera haber sido radicados efectivamente, sean dados a publicidad. Ello permite que esta información se integre a las bases de datos en función de las cuales comercios, bancos y simples particulares adoptan decisiones de incidencia económica[39].

---

[38] Cf. Art. 52 inc. j) Reglamento para la Justicia Nacional en lo Comercial. Para ampliar ver Molina Quiroga, Eduardo, "El tratamiento de los datos judiciales y los informes crediticios", http://www.cpacf.org.ar/verde/vAA_Doct/archDoctri/MQuiroga4.htm/

[39] Cámara Nacional de Apelaciones en lo Comercial, art. 52 inc. j) de su Reglamento: "Diariamente se editarán por orden alfabético listas de demandas iniciadas con indicación de partes, objeto, Juzgado y Secretaría, que se archivarán cronológicamente y servirán como libro general se asignaciones del fuero comercial. Similar edición se efectuará trimestralmente. Tales constancias (y las existentes en el sistema informático) serán públicas, con excepción de las medidas cautelares y diligencias preliminares que se editarán por separado manteniéndose reservadas. Se emitirán en similares tiempo y condiciones planillas donde consten los juicios

Hemos criticado esta modalidad, e incluso la Asociación de Abogados de Buenos Aires (AABA) pidió a las autoridades de Superintendencia de la Cámara Nacional de Apelaciones en lo Comercial[40] la modificación de su Reglamento Interno, de modo que en los listados o informes que emita diariamente solo se informen los juicios que efectivamente han sido presentados en los juzgados asignados, o en su defecto, de continuar con la actual práctica, se consigne que "la información obrante en sus registros consiste exclusivamente en el nombre de las partes, objeto del juicio y monto del litigio, cuya solicitud de asignación de juez interviniente ha sido resuelta en la fecha, quedando a cargo de las empresas de bancos de datos y/o interesados la realización de la compulsa de las actuaciones para constatar el estado de las mismas", aclaración que debe ser obligatoriamente incluida en toda distribución o cesión de estos informes; y sugerir también a la Cámara Nacional de Apelaciones en lo Comercial que emita listados diarios sobre la base de informes que requiera a los Juzgados Nacionales de Primera Instancia del fuero sobre la conclusión de las causas en trámite". En dicha declaración se expresó públicamente la preocupación de la AABA por “las consecuencias negativas que la utilización arbitraria de estos informes provoca en los derechos de consumidores y usuarios que ven restringido o vedado su acceso al crédito sobre la base de informes sobre acciones judiciales supuestamente iniciadas, que en numerosos casos, no revelan siquiera un incumplimiento cierto de obligaciones, lo que se contradice con los principios de calidad de los datos personales introducidos por la Ley 25.326".

Por otro lado, implicaría también un beneficio para los proveedores de información, ya que se contaría con una fecha cierta del reclamo judicial.

La preocupación por el impacto de la información de origen judicial que se difunde por Internet, en un contenido por supuesto mucho más amplio que el de los informes de juicios patrimoniales, ha venido creciendo y motivó la realización de un seminario en Costa Rica, en julio de 2003. Como fruto de los trabajos y deliberaciones, se acuñaron las llamadas "Reglas de Heredia", o "Reglas mínimas para la difusión de

---

asignados por recusación o excusación, partes, día, juzgado de origen y adjudicado.”

[40] Declaración de la Asociación de Abogados de Buenos Aires del 06/06/2001, en cuya redacción hemos participado: http://www.aaba.org.ar/

información judicial en Internet"[41].

En esas recomendaciones destacamos, por la relación con nuestro propósito, la "regla 5", que sostiene que "Prevalecen los derechos de privacidad e intimidad, cuando se traten datos personales que se refieran a niños, niñas, adolescentes (menores) o incapaces; o asuntos familiares; o que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos; así como el tratamiento de los datos relativos a la salud o a la sexualidad; o victimas de violencia sexual o domestica; o cuando se trate de datos sensibles o de publicación restringida según cada legislación nacional aplicable o hayan sido así considerados en la jurisprudencia emanada de los órganos encargados de la tutela jurisdiccional de los derechos fundamentales. En este caso se considera conveniente que los datos personales de las partes, coadyuvantes, adherentes, terceros y testigos intervinientes, sean suprimidos, anonimizados o inicializados salvo que el interesado expresamente lo solicite y ello sea pertinente de acuerdo a la legislación."

Cuando estas "reglas mínimas" definen los "datos personales" incluyen el "patrimonio"[42] como uno de los elementos incluidos en esta regla y por lo tanto debería merecer un cuidado especial.

El daño que puede provocar la difusión de datos judiciales negativos, aunque luego sean rectificados, suele ser de difícil reversión.

---

[41] Aprobadas durante el "Seminario Internet y Sistema Judicial", realizado en la ciudad de Heredia Costa Rica, los días 8 y 9/07/2003, con la participación de poderes judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay: http://www.iijusticia.edu.ar/Reglas_de_Heredia.htm/

[42] Regla 10ª: Definiciones. Datos personales: "Los datos concernientes a una persona física o moral, identificada o identificable, capaz de revelar información acerca de su personalidad, de sus relaciones afectivas, su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio físico y electrónico, número nacional de identificación de personas, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad o su autodeterminación informativa. Esta definición se interpretara en el contexto de la legislación local en la materia."

En materia de difusión o publicidad de juicios comerciales, deberían modificarse las circunstancias y modalidades que se conocen en nuestro país, ya que no existen razones para apartarse del principio de calidad del dato que la legislación específica establece sin excepciones y que la Corte Suprema de Justicia, así como recientes fallos han aplicado expresamente[43].

Existe también preocupación por los efectos discriminatorios que pueden tener, por ejemplo mediante la confección de "listas negras", tanto los listados de demandados en juicios comerciales, como quienes accionan en defensa de sus derechos laborales[44].

El desafío es encontrar un equilibrio entre los avances en materia de información que permiten las nuevas tecnologías de la Informática y las Comunicaciones, preservando al mismo tiempo los derechos y garantías de las personas.[45]

8.7.3. Información proporcionada por el acreedor

Como el acreedor es también titular del dato de incumplimiento de una obligación, puede convertirse en fuente de información crediticia, mediante convenios con empresas comerciales, estudios profesionales, entre otros.

Las empresas de tarjetas de crédito tienen prohibido informar de manera

[43] CNCom, sala B, 14/02/2005, “Palavecino, Mariela c/ Banco de Galicia y Buenos Aires”, LA LEY 2005-C, 456; CNCom, sala D, 01/09/2005, “Cardinale, Miguel A. y otro c/ Banco de Galicia y Buenos Aires”, LA LEY 2006-A,287.

[44] En tal sentido, el jurista brasileño Lobato de Paiva, Mario Antônio, ha elaborado una ponencia sobre la “Responsabilidad civil del Estado por daños provenientes de la circulación de datos en los sitios de Internet de los tribunales(A difusão de informações judiciais na Internet e seus efeitos na esfera trabalhista)”, http://jus2.uol.com.br/doutrina/texto.asp?id=4672/

[45] La regla 7ª de las Reglas de Heredia expresa que “En todos los demás casos se buscará un equilibro que garantice ambos derechos. Este equilibrio podrá instrumentarse: a) en las bases de datos de sentencias, utilizando motores de búsqueda capaces de ignorar nombres y datos personales; b) en las bases de datos de información procesal, utilizando como criterio de búsqueda e identificación el número único del caso. Se evitará presentar esta información en forma de listas ordenadas por otro criterio que no sea el número de identificación del proceso o la resolución, o bien por un descriptor temático”

directa a las empresas de riesgo crediticio conforme a lo dispuesto por el art. 53 de la ley 25.065, criterio que ha sido ratificado por la Corte Suprema de Justicia[46], aunque ha merecido la crítica de la doctrina especializada.[47]

Más allá del acierto o no de esta prohibición, lo que se advierte en el derecho comparado, especialmente en la reglamentación española a la que nos hemos referido precedentemente es la prohibición, o limitación consistente en no incluir en los informes crediticios datos personales sobre los que exista un principio de prueba documental que aparentemente contradiga la exigibilidad de la obligación presunta incumplida, así como la posibilidad de bloqueo cautelar del dato personal desfavorable en los supuestos en los que ya se hubiera efectuado su inclusión en el archivo o base de datos.

Lo destacable es la exigencia para el acreedor, o quien actúe por su cuenta e interés, de asegurarse que concurran todos los requisitos exigidos en esta norma en el momento de notificar los datos adversos al responsable del archivo o base de datos común. Es el acreedor, o quien actúe por su cuenta, quien tiene la carga de comunicar el dato inexistente o inexacto, con el fin de obtener su cancelación o modificación, al responsable de la base de datos común, en el mínimo tiempo posible, y en todo caso en una semana.

En cuanto a la metodología para registrar una obligación incumplida indica que debe hacerse en un sólo asiento si fuese de vencimiento único, o en tantos asientos como vencimientos periódicos incumplidos existan señalando, en este caso, la fecha de cada uno de ellos. Es necesario efectuar una notificación por cada deuda concreta y determinada con independencia de que esta se tenga con el mismo o con distintos acreedores, estando a cargo del responsable del archivo o base de datos adoptar las medidas organizativas y técnicas necesarias que permitan acreditar la realización material del envío de notificación y fecha de entrega o intento de entrega de la misma. La notificación se hace a la ultima dirección conocida del afectado, a través de un medio fiable e independiente del responsable del archivo o base de datos.

---

[46] CSJN, 06/03/2007, “Organización Veraz S.A. v. Estado Nacional”, JA 2007-II-732, LA LEY 2007-B, 303; DJ 21/03/2007, 692; RCyS 2007-IV, 37; Fallos 330:304.
[47] Palazzi, ob.cit. supra.

En Panamá la reciente modificación a la ley que regula la actividad (ley 14/2006) establece que "Los datos sobre historial de crédito brindados por los consumidores o clientes a los agentes económicos, solo podrán ser recopilados y/o transmitidos a las agencias de información de datos y suministrados por estas a los agentes económicos, con el consentimiento o la autorización expresos de los consumidores o clientes, con excepción de las obligaciones de carácter económico, financiero, bancario, comercial o industrial, siempre que estas consten en cheques protestados por falta de fondos o por haber girado contra cuenta corriente cerrada o por orden de suspensión de pago." (art.23).

La Corte Suprema argentina se ha expedido en un sentido similar al resolver que "*no puede calificarse de "exacta" o "actualizada" una información que se limita a indicar -sin ninguna aclaración o salvedad- que la actora mantiene una deuda con la mencionada entidad bancaria. Y, por ende, asiste a aquélla, el derecho a que tal información se actualice y complete a fin de que quede reflejado, del modo más preciso posible, el estado de litigiosidad suscitado respecto de los créditos a los que se ha hecho referencia.*"[48]

La Suprema Corte de Justicia de Mendoza, recientemente[49], sostuvo que la fuente de la información siempre es demandable, tal como surge de una interpretación a contrario sensu del art. 43 in fine de la CN, ya que esa norma significa que se puede accionar contra cualquier fuente, excepto cuando la información provenga de bancos de datos de los periodistas. Citando a Puccinelli concluyó que en definitiva, el elenco de sujetos demandables debe considerarse amplio, tanto por efecto de las disposiciones legales y reglamentarias, como por los más elementales principios de la protección de datos y, en consecuencia, siempre que haya tratamiento que exceda el uso estrictamente personal, habrá demandabilidad"[50].

Hemos sostenido en otra publicación, también citada en el fallo precedente,

---

[48] CSJN, 21/11/2006, "Di Nunzio, Daniel F. c/ The First National Bank of Boston y otros s/ hábeas data", LA LEY 2007-C, 131, con nota de Palazzi, Pablo A., "El derecho del titular de información personal a aclarar un dato controvertido por la vía del hábeas data".

[49] SCJMdza, sala I, 16/02/2009, "Albares Raúl c/ Banco de Galicia", LLGran Cuyo 2009 (marzo), 157; LA LEY 2009-B, 247, LLGran Cuyo 2009 (abril), 223.

[50] Puccinelli, Oscar, "Protección de datos de carácter personal", Bs. As., Ed. Astrea, Buenos Aires, 2004, pág. 584.

que mientras los usuarios son quienes realizan a su arbitrio operaciones de tratamiento de datos personales, sea en registros o archivos propios o en los de terceros, es importante añadir en la enumeración a quienes operan como fuente de los datos, es decir, quienes proporcionan -o de quienes son tomados- los datos personales al circuito para su tratamiento, que pueden revestir el carácter de bancos de datos, que tendrán responsables, o tratarse de usuarios de los datos. Si quien proporciona los datos al circuito no cubre ninguno de los roles precedentemente expresados, será una fuente simple del dato.[51]

8.8. Consentimiento e información

Diversas normas del derecho comparado exigen el consentimiento previo del titular en el tratamiento de datos personales referidos al cumplimiento de obligaciones dinerarias, e incluso a los informes de riesgo crediticio[52]. Sin embargo, en la mayoría, como ocurre en nuestra legislación, este recaudo no es exigible.

Al respecto se ha dicho que “en efecto, resultaría irrazonable que la divulgación de los datos vinculados al cumplimiento o incumplimiento de las deudas dependa del arbitrio del propio deudor, motivo por el cual el art. 26, inc. 5° de la ley citada establece que "la prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios". Obviamente, el interesado puede solicitar la rectificación del asiento, siempre que demuestre que es inexacto, falso o que está desactualizado, supuesto en el cual la carga de la prueba se rige por el régimen general y pesa -en consecuencia- sobre quien la alega (arg. art. 377, C.Proc.). (eran deudas de 1992 y 1993)[53].

Esta solución es razonable, y a pesar de ello, pensamos que aún cuando esté

---

[51] Molina Quiroga, Eduardo, “Daños derivados de las bases de datos”, en “Tratado de Daños reparables, Ghersi, Carlos (Dir.), Weingarten Celia (Coord), Ed. La Ley, Buenos Aires, 2008.
[52] Ley de Paraguay 1682, art. 5 inc.a).
[53] CNCiv, sala C, 03/06/2004, “D., C, A. c/ Lloyds Bank TSB Bank”, LA LEY, 19/10/2004, 5.

excusado el consentimiento previo, por disposición legal, es fundamental cumplir con el deber de información o conocimiento, presupuesto del ejercicio de los derechos de acceso, rectificación y cancelación de rango constitucional[54]. Esta circunstancia también es viable exigirla desde el punto de vista de la defensa del consumidor.[55]

8.9. Síntesis

Los informes crediticios constituyen una especie del género datos personales, que pueden revestir al menos dos modalidades. Una es la que se limita a registrar el cumplimiento o incumplimiento de obligaciones, que hemos asimilado a un dato de balance, en el sentido de su configuración lógica (es verdadero o falso).

La otra variedad, que es la más útil para medir el riesgo de crédito, son los informes sobre solvencia, que constituyen una operación compleja, que articula diversos datos e incluye un juicio de valor, tal como indica, por ejemplo, la reglamentación del Banco Central para calificar a un deudor.

Aunque la primera esté necesariamente imbricada en la segunda, es inaceptable que se establezca el grado de riesgo de una persona en base, exclusivamente, a su incumplimiento de una obligación, la existencia de una deuda o de una demanda en su contra.

Actuar de este modo implica malversar una norma destinada a proteger los datos personales y convertirla en un mecanismo de cobro extrajudicial de deudas cuya persecución judicial resulta poco rentable.

En la mayoría de las legislaciones se establecen plazos para conservar información patrimonial negativa, en base al llamado “derecho al olvido”. El debate

[54] CNCiv, sala K, 22/10/2002, "Gutiérrez, Vicente Juan Carlos Demetrio c/Banco de la Provincia de Buenos Aires y otro s/daños y perjuicios", LA LEY 2002-F, 781; DJ 2002-3, 883: "Cuando una empresa que lucra con información sobre riesgo crediticio, debe asentar en su archivo de datos la calificación de "deudor irrecuperable" respecto de un particular, previamente -para no incurrir en culpa o negligencia- debe notificar de inmediato al interesado a fin de permitirle formular las observaciones que estimara pertinentes (conf. Art. 5º de la ley 25326 sobre protección de datos personales)."

[55] CCyC La Matanza, sala I, 05/07/2001, "Bressan, Walter Darío c/Banco Galicia y Bs.As. s/daños y perjuicios (ordinario)", elDial AAC6E.

sobre cuando estos datos deben considerarse caducos, si bien no ha concluído, parece inclinarse en el sentido más favorable para el deudor, en una interpretación que acoge la verdadera finalidad de la norma. Ello no implica condonación alguna, sino una limitación para difundir o ceder esa información.

Es conveniente regular la actividades de los agentes que brindan información crediticia, sean fuentes o bancos de datos, e incluso usuarios, y un modelo razonable puede ser el de la ley de Colombia.

Finalmente, es indudable que los principios rectores del tratamiento de datos personales son plenamente aplicables a los informes crediticios, en particular, el principio de calidad, como lo ha consagrado la jurisprudencia de la Corte Suprema de Justicia de la Nación y de otros tribunales.

Sería aconsejable que se profundizara más aún en este aspecto, incluyendo entre los sujetos obligados a respetarlo tanto al Banco Central como a las Mesas Generales de tribunales y por supuesto, a todas las otras entidades financieras que son actores en el tratamiento de datos personales.

Capítulo 9. Responsabilidad por informes crediticios erróneos

Sumario: Bien jurídico protegido. Conductas antijurídicas. Naturaleza de la responsabilidad. Responsabilidad agravada por profesionalidad. Responsabilidad empresas informes crediticios. Costas.Daño resarcible. Daño moral. Daño material.Daño al crédito e imagen comercial. Usuarios y fuente de los datos.La nueva ley de defensa del consumidor y los bancos de informes crediticios. Extensión del concepto de relación de consumidor. Nuevo paradigma de respeto a los consumidores. Legitimados pasivos.Daño directo.Daño punitivo. Cadena de responsables. Síntesis.

9.1. Bien jurídico protegido

Luego de haber afirmado que el tema de la protección de datos personales excede la tutela de la vida privada, y que reconoce exigencias específicas para su tratamiento, que tienen acogida tanto en documentos internacionales como en la legislaciones nacionales, incluida la LPDPA, nos proponemos analizar los supuestos en los que existe responsabilidad por un inadecuado manejo de los datos personales que integran los informes crediticios.

En un contexto en el que no se trataba de informes comerciales, sino de analizar los alcances de la garantía consagrada en el artículo 43 de la Constitución Nacional, la Corte Suprema señaló que “la acción de hábeas data ha sido reconocida no sólo en las legislaciones de diversos países, sino también por los organismos internacionales que, en sus diferentes ámbitos, han elaborado pautas que contribuyen a integrar la perspectiva con que ha de ser evaluada la modalidad de su ejercicio por este Tribunal. Así, en términos generales coinciden las directrices formuladas por la Organización de Naciones Unidas, la Organización de los Estados Americanos, el Consejo de Europa, e inclusive la jurisprudencia de la Corte Europea de Derechos Humanos. La amplitud de sus alcances, tanto en lo relativo a la exigencia de licitud, lealtad y exactitud en la información, como en lo que hace al acceso de las personas

legitimadas -conforme con la coincidente opinión de estas instituciones y organismos - encuentra limitaciones, fundamentalmente, en razones de seguridad y defensa nacional."[1]

Reiteramos entonces que la autodeterminación informativa excede ampliamente el ámbito de los llamados datos sensibles, y su adecuada tutela impacta fuertemente en la actividad económica.

En una primera etapa se consideraba que "el bien jurídico protegido (en las acciones de hábeas data) era la privacidad o intimidad de las personas sobre las que recae el informe", pero esto se confrontaba con la actividad que pueden desarrollar algunas empresas privadas produciendo informes sobre aspectos que hacen a la situación patrimonial de las personas, cuya utilidad comunitaria se vincula a la seguridad en las obligaciones contractuales y cambiarias.[2]

Efectivamente, la información suministrada por las bases de datos personales de carácter patrimonial, comercial, crediticios y de cumplimiento de obligaciones no incursiona en el terreno del honor e intimidad de la persona.

En tanto decimos que el patrimonio es el conjunto de derechos y obligaciones de una persona, damos por sentado que todo dato patrimonial tiene una estructura bipolar, dado que implica información sobre uno o más deudores, pero simultáneamente contiene datos del o de los acreedores. Por ello se ha resuelto que su difusión o divulgación no es discriminatoria para su vida de relación en tanto se orienta a actividades de índole económica.[3]

Antes incluso de la sanción de la LPDPA se había resuelto que la recolección de datos en un registro de morosos es lícita, aún sin mediar consentimiento del

---

[1] CSJN, 15/10/1998 "Urteaga, Facundo R. c/ Estado Mayor Conjunto de las FFAA s/amparo", LA LEY 1998-F,237 (entre otras publicaciones).
[2] JNPICivil N º 93, 27/05/1997, "Pochini, Oscar de Jesús y otro c/Organización Veraz SA s/habeas data", fallo confirmado por Cámara: CNCiv, sala A, 08-09-1997 "Pochini, Oscar de Jesús y otro c/Organización Veraz SA s/habeas data" LA LEY 1988-B, 3.
[3] CNACAF, Sala III, 22/12/1999, "M., M. c. Fidelitas S. A. y otros", LA LEY 2001-B, 791, con nota de María Eugenia Slaibe y Claudio Gabot: "La discriminación en los informes comerciales frente a la nueva regulación del Hábeas data".

interesado, cuando los datos coinciden con los que aparecen en el padrón electoral, son los propios de cualquier operación de crédito, señalando que la jurisprudencia había admitido por principio la legitimidad de la divulgación de informes que se reciben a simple denuncia según la operativa de esos grupos , sin que se releve la imposición de una obligación ab initio a estos antes de que verifiquen la veracidad de esta denuncia, pero esto no excluía la responsabilidad que les pudiera caber por la mendacidad[4].

Los informes de riesgo crediticio son generados, distribuidos y divulgados por un conjunto de actores integrado por bancos, empresas emisoras de tarjetas de crédito, el Banco Central, y las empresas que especiíficamente prestan el servicio que impacta en varios aspectos de la vida social y particularmente en el otorgamiento de crédito, cualquiera sea su finalidad.

Se trata de información personal que la ley colombiana califica como “semi privada”, y que por el carácter relativo de los vínculos obligacionales concierne tanto al deudor como al acreedor.

Esto no significa que en esta materia no rijan las exigencias que se desprenden de los principios rectores que hemos comentado en capítulos precedentes.

En tal sentido los actores involucrados en la generación, difusión y utilización de informes crediticios están obligados a observar, en el tratamiento de estos datos, las reglas de calidad que establece la ley y cuando no lo hagan, serán responsables de los daños que se ocasionen derivados de dicho tratamiento.

El prestigio, la imagen de un empresario o comerciante, e incluso la posibilidad de acceso al crédito de los consumidores[5], pueden sufrir graves perjuicios, en virtud de informes patrimoniales negativos, cuando estos no se ajustan a los requisitos de calidad en el tratamiento de los datos personales.

---

[4] SCJMdza, 15/04/1999, “Huertas, Juan C. c. Co.De.Me”, LA LEY 1999-F, 296; LLGran Cuyo 1999, 600 y SCJ Mdza, sala I, 24/11/1999, “Costa Esquivel, Luis c. Banco Crédito de Cuyo S. A. y CO. DE. ME.”, LLGran Cuyo, 2000-54.

[5] Ver Pérez Bustamente, Laura, “El derecho de acceso al consumo como derecho subjetivo”, http://www.astrea.com.ar/

La imagen del empresario no solo se construye en base a sus aciertos industriales, mercantiles o de servicios, sino también sobre la percepción que sus clientes y proveedores, así como las entidades crediticias, tienen acerca de su comportamiento en relación a las obligaciones dinerarias[6].

Un dato apresurado, como sería la solicitud de radicación de un juicio (que quizás nunca se haga efectivo, o difundido apresuradamente, por que se han iniciado incorrectamente y luego no se presentan, o que han perdido vigencia (por haber prescripto la acción, o perimido la instancia) e incluso que han sido rechazados por inexistencia de deuda, etc., pueden afectar la imagen empresaria, comercial o de un consumidor.

Como veremos más adelante, se ha reconocido en algunos casos un daño a la imagen comercial. En otros supuestos, se ha merituado la vulneración del "buen nombre" de una persona.

Es decir que en nuestra visión, los bienes jurídicos protegidos en el campo de los informes comerciales, en el contexto de la protección de datos personales, son intangibles que no podemos circunscribir a derechos personalísimos, como el honor, o la identidad, sino también aspectos dignos de tutela, como la referida imagen comercial, o el buen nombre comercial, que abarca no solo a empresarios, sino también a consumidores.

En ambos casos, el acceso al crédito es otro aspecto digno de tutela, que se ve afectado cuando no hay una información cierta, adecuada, actualizada y pertinente.

9.2. Conductas antijurídicas.

Como hemos señalado, los informes crediticios están alcanzados por la exigencia de calidad en el tratamiento del dato, es decir que deben ser ciertos, adecuados, pertinentes y actualizados.

---

[6] para un mayor desarrollo del tema ver MOLINA QUIROGA, Eduardo, "Prestigio e imagen del comerciante. Protección de datos personales", en Código de Comercio y normas complementarias. Análisis doctrinario y jurisprudencial, Director Raúl A. Etcheverry, Coordinación: Héctor O. Chomer, Editorial Hammurabi de José Luis de Palma, 2005.

El artículo 31 de la LPDPA establece, siguiendo su fuente española[7], que "Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos."

Es decir que la propia LPDPA establece la existencia de responsabilidad por daños y perjuicios derivados de su inobservancia.

En una línea similar, la legislación de Panamá establece que los consumidores o clientes "que sufran algún daño o perjuicio por razón de la inclusión de uno o más datos erróneos, inexactos, equívocos, incompletos, atrasados o falsos, en la base o banco de datos de una agencia de información de datos, tendrán derecho a ser indemnizados por quien resulte responsable por la inclusión de dichos datos, ya sea por culpa o por negligencia, sea este el agente económico o la agencia de información de datos. Este derecho se ejercerá ante la jurisdicción ordinaria correspondiente y según los términos y condiciones establecidos en los artículos 9 y 10 de la presente Ley."[8]

La legislación de Paraguay, en su redacción originaria también preveía la posibilidad de reclamar daños y perjuicios, además de las sanciones administrativas, en el caso de informes crediticios o patrimoniales no ajustados a la ley.[9]

La ley ecuatoriana que regula los burós de información crediticia[10]

---

[7] Artículo 19 ley 15/1999. Derecho a indemnización. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

[8] Art. 23, inc. 6º, ley 24-2002, modificada por art. 6 ley 14-2006.

[9] Art. 10 in fine, ley 1682, que al ser modificado por la ley 1969, eliminó el párrafo.

[10] Art. 10, ley 13-2005.

establece:“Los burós y las fuentes de información crediticia serán legalmente responsables por los daños ocasionados al titular como consecuencia de la transmisión de información ilegal, inexacta o errónea y, por tanto, no estarán exonerados alegando ausencia de dolo o de culpa. La responsabilidad de las fuentes es entregar información a los burós de manera exacta y legal; la responsabilidad de los burós es reportarla sin alteración o modificación alguna. Sin perjuicio de lo anterior, en los procesos promovidos contra los burós, éstos podrán pedir que se cite también con la demanda a la o las fuentes de las que hubieren obtenido la información crediticia materia del proceso, siguiendo el procedimiento establecido en el artículo 94 del Código de Procedimiento Civil. También responderán por los daños causados al titular de la información crediticia, quienes utilicen dolosa o culposamente informaciones o reportes provenientes de los burós. El afectado podrá demandar indemnización, cuando la información errónea no ha sido rectificada por los burós.”

La ley peruana 27489, sobre Centrales de Información de riesgo y protección del titular de la información estipula: “18.1 La responsabilidad civil de las CEPIRS por los daños ocasionados al titular por efecto del tratamiento o difusión de información será objetiva. Las CEPIRS podrán repetir contra las fuentes proveedoras de información cuando el daño sea ocasionado como consecuencia del tratamiento de información realizada por éstas.

18.2 Igualmente existe responsabilidad por parte de los usuarios o receptores de información de riesgos proporcionada por las CEPIRS, en caso de utilización indebida, fraudulenta o de modo que cause daños al titular de la información, la misma que se determinará conforme a las normas de responsabilidad civil y penal a que hubiese lugar. Sin perjuicio de lo anterior, las CEPIRS podrán repetir contra los usuarios o receptores de información en caso de haber asumido responsabilidad frente al titular de la información o terceros, en los supuestos antes indicados en que esté involucrada la responsabilidad de los usuarios o receptores de información.”

La ley 19628, de Chile establece: “Artículo 11.- El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños”

Aún en los países que no tienen norma expresa, como Costa Rica, se encuentran sentencias judiciales condenatorias que ordenan excluir determinados

datos crediticios negativos, por haber caducado su vigencia (derecho al olvido) y condenan a la empresa que había difundido la información a pagar los daños y perjuicios correspondientes.[11]

Como se advierte, aunque con distintas formulaciones, el panorama latinoamericano en la materia es suficientemente rico.

En la Argentina, a pesar de la existencia de normas expresas, inicialmente, la jurisprudencia fue reacia a reconocer la antijuridicidad de la conducta cuando bancos, entidades crediticias o empresas de informes crediticios producían informes erróneos[12].

Esta orientación ha sufrido cambios y paulatinamente se va afinando el tratamiento de la responsabilidad en esta materia.

Constituyen supuestos de conducta antijurídica, por no observar el principio de calidad en el tratamiento de informes crediticios:

a) los informes erróneos en materia de cumplimiento de obligaciones dinerarias, que implican la inclusión en un listado de deudores morosos, de quien no lo es.

b) la incorrecta calificación del deudor, en los términos de la ya comentada

[11] Corte suprema de justicia, Sala Constitucional, Costa Rica, 22/08/2006, Exp: 06-006218-0007-CO, Res. Nº 2006-12245, http://200.91.68.20/scij/busqueda/jurisprudencia/jur_repartidor.asp?param1=XYZ&param2=1&nValor1=1&nValor2=355787&strTipM=T&lResultado=3&strLib=LIB y jurisprudencia allí citada.

[12] Jdo. Civ., Com. y Minas Nº 12, Mendoza, 03-11-1997, “Huertas, Juan C. c/ CO.DE.ME”, VJ, 1998-6-99 y LL Gran Cuyo 1998, 975. “La jurisprudencia ha admitido por principio la legitimidad de la divulgación de informes que se reciben a simple denuncia -según la operativa de eso grupos-, sin que se releve la imposición de una obligación ab initio a estos antes de que verifiquen la veracidad de esta denuncia. Sin perjuicio de la responsabilidad que les quepa por la mendacidad.”; CNCom, sala D, 10/08/2001, "Bachrach, Pedro c/ Banco Central de la República Argentina s/ ordinario", ElDial AAA3D: “Es notorio que el BCRA no se maneja con información propia sino con la que le transmiten los bancos; de tal modo, no parece dudoso que tanto la inclusión del accionante en la base de datos de cuentacorrentistas inhabilitados, cuanto la notoria demora en registrar en la misma el pago del cheque y otras novedades, no son atribuibles al aquí demandado B.C.R.A." (entre otros fallos similares)

Central de Deudores del Sistema financiero[13].

c) la inserción de una persona en un listado de deudores morosos, cuando ello es el resulado de información errónea, desactualizada, o impertinente.

d) la difusión de iniciación de causas judiciales sin confirmar que las mismas han sido efectivamente radicadas ante los tribunales

e) La no actualización de informes sobre deudas

f) La no actualización de información sobre juicios pendientes

g) la cancelación o negación de instrumentos de acceso al crédito, como cuentas corrientes, tarjetas de crédito, cuando la información que sustentó la medida era errónea, desactualizada o impertinente.

9.3. Naturaleza de la responsabilidad

Los daños producidos por la difusión de información de carácter personal errónea, desactualizada o falsa puede originarse en una situación contractual[14] o extracontractual.

Cuando interviene una empresa emisora de tarjetas de crédito se ha sostenido que el servicio en el cual se enmarca ese sistema ubica la responsabilidad de sus integrantes en el ámbito contractual, imponiendo una obligación solidaria entre todos los intervinientes (art. 40, ley 24240) y en todo caso, le queda a la emisora una acción de repetición contra el banco, si así lo considera.[15]

Pero también se considera que el error en que incurrió el banco demandado,

---

[13] CNCom, sala B, 17/10/2003, "Garnica José Redolfo y otro c/Banco Itau Buen Ayre SA s/ordinario", elDial AA732.
[14] CNCom, sala E, 03/06/2003, "Perlman Manuel c/ Bank Boston SA y otro s/ ordinario", elDial AA19C6, sentencia en la que se hizo lugar al reclamo contra el banco (responsabilidad contractual), pero se rechazó contra la empresa de informes crediticios (extracontractual)
[15] CNCom, Sala B, 24/02/2006, “Hager, Enrique Carlos c/Lloyds Bank y otro s/ordinario”, elDial AA33D9 y ED 01-08-2006.

sin perjuicio de la relación que lo vincula al afectado, configura un obrar antijurídico que encuadra dentro del ámbito de la responsabilidad aquiliana, en cuanto a las publicaciones en diversos sitios de Internet del informe erróneo que proporcionó. Ello justificó la condena tanto por las consecuencias inmediatas, como por las consecuencias mediatas, ocasionadas por su imprudente comportamiento (arts. 904 y 1109 del cód. civil)[16].

9.3. Responsabilidad agravada por profesionalidad

El carácter profesional juega un papel importante para establecer la responsabilidad de las entidades financieras, ya que la superioridad técnica que detentan les impone el deber de obrar con mayor prudencia y pleno conocimiento del negocio[17] y les exige una diligencia acorde con su objeto haciendal, con organización adecuada para desarrollar su giro[18], o sea su carácter profesional.[19]

Es que parece evidente que la conducta de una entidad bancaria o de una emisora de tarjetas de crédito no puede apreciarse con los parámetros exigibles a un neófito, sino conforme al standard de responsabilidad agravada que el profesional titular de una empresa con alto nivel de especialización tiene frente al usuario, dado que en los contratos en los que una de las partes detenta superioridad técnica, la otra soporta una situación de inferioridad jurídica[20].

Similares argumentos son aplicables con relación al gestor de una base de datos sobre riesgo crediticio, quien por su indudable condición profesional, asume una

---

[16] CNCom, sala E, 17/10/2003, “Martínez, Nelly Aida c/Lloyds Bank s/ordinario”, Diario Judicial.com 21/01/2004 y La Ley Online; CNCom, sala E, 115/12/1999,“Álvarez, Jorge Oscar c/Banco Roberts SA”, JA-2000-III-503.
[17] CNCom, sala E, 16/08/2006, “Guryn, Néstor c. Lloyds Bank S.A.”, LA LEY 2006-F, 830 y DJ 2007-02-14, 345.
[18] CNCom, sala B, 24/11/1999, "Molinari, Antonio F. C/ Tarraubella Compañía Financiera SA", Doctrina Societaria, ed. Errepar, tomo XI, pag. 905, JA, revista n° 6235 del 28-2-2001; CNCom, sala A, 11/04/2003, " Solares Adrián Daniel c/Bansud SA s/sumario", elDial AA17EB; CNCom, sala B, 20/09/1999, "Banesto Banco Shaw SA c/ Dominutti, Cristina",JA 2000-IV-811.
[19] CNCom, sala B, 30/12/2008, “González, Alberto Israel y otro c. Banco de Galicia y Buenos Aires S.A.”, LA LEY2009-B, 548.(y fallos allí citados).
[20] CNCiv, Sala H, 04/09/2002, “Sosa Marcelo c/Citibank S.A. s/Daños y perjuicios", elDial AA135C.

obligación de diligencia especial (arg. art. 902, Cód.Civil), que está claramente establecida en nuestra LPDPA y puede advertirse en las normas de Derecho comparado que hemos reseñado.

En tal sentido, se ha destacado que la complejidad del tráfico hace exigible una protección responsable del consumidor (art. 42 C.N.y ley 24.240) desde que la confianza como principio de contenido ético impone a los operadores un inexcusable deber de honrar esas expectativas, y cuando ello se quiebra se contravienen los fundamentos de toda organización, tornando inseguro el tráfico[21].

Esta exigencia de mayor diligencia, en el tema que nos toca abordar, se traduce también en una adecuada respuesta para rectificar datos erróneos, medida en términos de tiempo[22].

En esta línea, por ejemplo, se ha aplicado el principio de las cargas probatorias dinámicas, al sostener que la circunstancia que la entidad financiera no acompañe la documentación (que respalde sus defensas), en rigor, es invocar su propia torpeza en una técnica operativa concerniente a su esfera de actuación, lo que resulta enteramente inadmisible, yq que se trata de un empresario titular de hacienda especializada en razón del objeto; y ello no sólo implica estándares agravados de responsabilidad (Cód. Civil, 902); sino plena oponibilidad a su respecto de un modo operacional convencionalmente pactado y dotado de fuerte tipicidad.**[23]**

Relacionado con tarjetas de crédito se ha responsabilizado tanto al banco como a la emisora de la tarjeta, cuando no han obrado con diligencia frente a maniobras dolosas de terceros que llevaron a la inclusión del actor como deudor

---

[21] CNCom, sala B, 30/06/2003, "Treviño Oscar c/Banco de Galicia y Buenos Aires SA s/ ordinario", elDial AA1971; CNCom, sala C, 26/03/2002, “Halabi, Ernesto c/ Citibank NA”, elDial AAE44.
[22] CNCom, sala C, 02/05/2001, "Martín, José Luis c/Banco Roberts Sociedad Anónima s/Ordinario", elDial AA890; CNCom, sala C,14/07/2006, “Sak, Liliana S. c. Citibank NA”, LA LEY 2007-A, 456, con nota de Verónica Knavs y Maite Herrán, “La responsabilidad bancaria por error de información. Alcances de la reparación”.
[23] CNCom, sala B, 08/10/2003, "Caruso, Pablo Daniel c/Banco Frances SA s/ordinario”, elDial AA1CF9; CNCom, sala D, 10/11/2005, “Valenti, Edmundo c/ Banco Francés S.A. s/ ordinario”, derechoybanca.com 104-3.

moroso[24], o a errores del banco al emitir tarjetas no solicitadas[25]. También se ha resuelto que existe daño moral cuando se ha debido sufrir la destrucción en público de tarjetas de crédito, con motivo de informes erróneos suministrados por un banco[26].

En los casos de “robo de identidad” se ha responsabilizado a las entidades bancarias, sosteniendo que no las exime de responsabilidad el hecho de un tercero (que había sustraído el DNI de la actora), si al momento de dar curso a la apertura de cuenta corriente a nombre de la accionante, no cumplió con las exigencias que su especialización y diligencia requerían a fin de dar cumplimiento con las disposiciones bancarias respecto a la comprobación de la identidad y la solvencia moral y económica del solicitante[27].

9.4. Responsabilidad empresas informes crediticios

La situación de las empresas proveedoras de informes crediticios presenta un panorama menos claro, distinguiéndose los tribunales que rechazan su legitimación pasiva sosteniendo que se limitan a reproducir información obtenidas de fuentes de acceso público o proporcionada por los acreedores[28], de aquellos otros que –aun sin mencionarlo- tienen en cuenta la aplicación a su respecto de claras disposiciones de la LPDPA en cuanto a los principios rectores del tratamiento de datos de carácter personal.

---

[24] CNCom, sala B, 11/04/2003, "Litvak, Adolfo y otro c/ Bansud S.A. y otro s/ sumario", elDial AA17DD.
[25] CNCom, sala D, 19/10/2005, "Sejas Mariana Paula c/ Bankboston N.A. s/ sumario", elDial AA2FAD; CNCom, sala D, 07/11/2000, "Vasen, Hugo Fernando c/ Citibank N.A., s/ordinario", elDial AA732.
[26] CNCom, sala C, 08/08/2003, "Polito, Francisco Antonio c/Banco Bansud Sociedad Anónima s/sumario", elDial AA1A5B; CNCom, sala B, 14/02/2003, "Buschiazzo, Juan A. y otro c/Banco Bansud SA y otro s/ordinario”, elDial AA166D; CNCom, sala D, 2005/06/27, "Svampa Ana María c/ Banco Francés del Río de la Plata S.A. s/ ordinario", elDial AA2CA6, entre otros.
[27] CNCiv, sala: L, 01/11/2007, “Galarza Valeria Romina c/ Banco Credicoop Cooperativo Limitado s/ daños y perjuicios”, Microjuris MJJ16858; CNCiv, sala L,31/03/2006, "Rodríguez, Pedro Ruben c/Ford Credit Compañía Financiera S.A., s/daños y perjuicios", elDial AA334B; CNCiv, sala F, 08/07/2005, “S., J. C. c/ Banco Itaú Buen Ayre SA s/ daños y perjuicios”, elDial AA2CBC.
[28] CNCiv, sala F,2003/11/06, "Fallone, Eugenio Donato c/ HSBC Banco Roberts SA s/ daños y perjuicios", elDial AA1DD0.

En el primer grupo encontramos fallos en los que se ha dicho que la actividad de las empresas de informes crediticios se ajusta a lo dispuesto en los art 26 y 5 inc.2-a) de la LPDPA y que éstas cumplen una función de interés público, lo que impide que tengan responsabilidad por los errores que cometan los bancos informantes, que operaría como factor eximente al ser la culpa de un tercero (art. 1113 del Código Civil). En algunos de estos pronunciamiento se ha esgrimido que si las empresas de informes crediticios debieran verificar la veracidad de cada uno de los datos informados por el Banco Central antes de comunicarlos a terceros (lo que se da por descontado que sería imposible, porque les exigiría tener acceso a la totalidad de las carpetas de las entidades financieras), sería tal la magnitud de la *ímproba* tarea, que concluirían por cerrar sus puertas, con lo que literalmente una actividad lícita vendría a resultar prohibida por efecto de una teoría pretoriana.[29].

En similar sentido se ha argumentado que las empresas dedicadas a brindar información comercial, registran datos obtenidos de una fuente pública, como la Central de Deudores del Sistema Financiero del B.C.R.A. y no intervienen en la calificación efectuada respecto de la situación financiera de los deudores (o presuntos deudores), por lo que no pueden ser responsables de los daños ocasionados por causa de los informes erróneos.[30]

En otra línea de análisis, incluso antes de la sanción de la LPDPA, se consideró responsable, conforme el art. 43 de la Constitución nacional, a la entidad dedicada a la prestación de servicios vinculados con la información de morosos, que registró deudores en tal carácter sin verificar las comunicaciones recibidas al respecto, circunstancia agravada por no haber procedido a la debida rectificación, pese a habérselo requerido en forma fehaciente el interesado.[31]

En similar posición, en alguna resolución de la Cámara Civil se entendió que toda empresa de verificación de riesgos crediticios, debe ante una intimación

---

[29] CNCiv, sala E, 19/10/2006, "A., S c/Banco Lloyds S.A. y otro s/daños y perjuicios", elDial AA3A58.
[30] CNCiv, sala A, 11/05/2005, "Maderas y Servicios S.A. y otro c/ Bankboston N.A. y otro s/ daños y perjuicios", elDial AA2AA9.
[31] C7ªCC Córdoba, 27/10/1999, “Delgado, Néstor R. y otros c. Seven S.R.L.”, LA LEY 1999-F,755,; LLC 1999, 1041.

requiriendo información sobre datos personales inexactos y/o falsos referidos a una calificación personal, actuar con la mayor celeridad posible utilizando todos los medios que se encuentren a su disposición (tales como el “fax”, “e-mail” o cualquier otro tipo de procedimiento electrónico) para poder obtener la información precisa de inmediato y sin tener que esperar un plazo prolongado. Una actitud contraria a la descripta –se afirmó-, denota un obrar negligente o descuidado frente al interés concreto y fundamentado del particular, susceptible de producir responsabilidad.[32]

En otro pronunciamiento, también de la justicia Civil, se dijo que “es deber de la empresa que lucra con la emisión de informes de los que surge la eventual solvencia comercial de las personas, instrumentar las medidas necesarias para que la información suministrada se ajuste a la realidad o soportar sus consecuencias, sin que sean los propios sujetos pasivos de la información los que deban aportar los datos pertinentes”.[33]

Más aún, se ha condenado a una empresa proveedora de informes, a responder por los perjuicios ocasionados por que además de haber registrado erróneamente a un usuario de tarjeta de crédito como moroso, sobre la base de un informe falso proporcionado por la entidad emisora de dicha tarjeta al B.C.R.A., si una vez recibida la citada información, omitió notificar de inmediato al interesado para permitirle formular las observaciones que creyera pertinentes, lo que denota un obrar culpable o negligente. En este caso se agregó como fundamento que “un banco de datos -en el caso, el que lleva una empresa de información creditoria- configura una cosa riesgosa de por sí, susceptible de generar responsabilidad civil objetiva para quien la explota -art. 1113, párr. 2°, parte 2ª, Cód. Civil-, a menos que se acredite la culpa de la víctima o un tercero por el cual el dueño o guardián de la misma no deba responder2.[34]

También se ha responsabilizado a empresas de informes crediticios por la

---

[32] CNCiv, sala K, 22/10/2002, “Gutiérrez, Vicente Juan Carlos Demetrio c/ Banco de la Provincia de Buenos Aires y otro”, elDial AA1580.
[33] CNCiv, sala F, 06/02/2002, "Ravina Arturo Octavio c/ Organización Veraz SA s/ daños y perjuicios", LA LEY 2002-C, 74 - DJ 2002-2, 41 - ED 197, 267.
[34] CNCiv, Sala K, 2003/10/08, “Botta, Rodolfo E. c. Citibank N.A. y otros”, LA LEY 08/01/2004, 3.

desactualización de los datos referidos a un juicio.[35] así como por no instrumentar las medidas necesarias para que la información suministrada se ajuste a la realidad, ya que no basta con decir una parte de la verdad y proceder a registrarla para quedar exento de responsabilidad, si la información registrada —por ser falsa o incompleta— afecta la intimidad, privacía o reputación de terceros, dado que los datos no solo deben ser veraces sino también actuales.[36]

9.5. Costas

Un primer paso lo constituyó la imposición de las costas judiciales a los bancos y empresas de informes crediticios cuando la acción de supresión o rectificación de datos obedecía a la conducta renuente del banco o de la empresa de informes crediticios.

Es justificada la imposición de costas a la empresa que suministra datos personales de carácter patrimonial, comercial, crediticio y de cumplimiento de obligaciones, si fue necesaria la interposición de una demanda a fin de rectificar la información existente en los respectivos registros informáticos que se encontraban desactualizados[37].

Similar decisión se adoptó en una condena al Banco Central de la Republica Argentina para que rectificara una información errónea, aplicándosele las costas.[38]

---

[35] CNCiv, sala D, 12/09/2007, “Quintana America Iberia c/ Organizacion Veraz S.A. s/ daños y perjuicios”, Microjuris: MJJ16317

[36] CNCiv, sala L, 08/5/2006,” Bousquet, Ricardo H. c. Organización Veraz S.A. y otros, La Ley Online.

[37] CNACAF sala I, 29/04/1997, “Díaz Cisneros, Adriano c. B.C.R.A. y otro”, LA LEY 1998-C, 373; CNCiv, sala I, 10/11/2000 “R. A. c. Empresa Organización Veraz, LA LEY 2001-B, 625 y DJ 2001-2,487; CNCiv, sala K, 14/08/1997, "Locato, Omar N. c. Organización Veraz S.A.C.M.E.I. s/hábeas data", LA LEY, 1999-B, 852, 1. Agrup. caso 13.688); CNCiv, sala M, 25/02/2002, “A., M. del C. c. Veraz S.A.”, LA LEY 2002-D, 177 y DJ 2002-2, 422; CNCiv, sala C, 13/06/2002, “Saal, Alfredo R. c. Organización Veraz S.A.”, LA LEY 2002-F, 335 y DJ 2002-3, 1089; CCiv. y Com. Mar del Plata, sala 2, 09/04/2002, “Toyas Pittelli, Omar E. y otros y. Citibank N.A. s/habeas data”, JA 2002-III, fascículo n. 10; CNACAF, sala I, 21/04/1999, Finoli, Leonardo Luis c/ B.C.R.A. y otro s/ Habeas Data”, SAIJ sumarios N° K0019989 y K0019990.

[38] CNACCF, sala I, 04/03/2003, “Gutiérrez, Norma S. c. Banco Central de la República Argentina y otro”, LA LEY 2003-F, 48.

Esta solución se mantuvo en casos en que el dato había sido erróneo o desactualizado, aún cuando la cuestión se tornara abstracta al momento de resolver, ya que había sido precisamente la existencia de ese error o falta de actualización la causa del litigio.[39]

En cambio, cuando el dato erróneo había sido corregido al momento de interponer la demanda de habeas data, corresponde cargar con las costas al actor[40].

9.6. Daño resarcible

La reparación integral de los daños sufridos por el obrar antijurídico de quien no efectúa un tratamiento de datos personales observando los recaudos que la ley impone, especialmente el principio de calidad (art. 4 LPDPA) no siempre es posible. El panorama jurisprudencial es mucho más generoso en el reconocimiento del daño moral, que en los rubros que integran el daño material.

9.6.1. Daño moral

En las demandas derivadas de informes crediticios erróneos se ha reconocido en la mayoría de los casos el daño moral.[41]

La jurisprudencia de la Cámara Nacional de Apelaciones en lo Comercial ha considerado como notorio el daño moral ocasionado al estar incluido incorrectamente en un listado de deudores mororos, o ser injustamente inhabilitado como cuenta

---

[39] CNCiv, sala C, 13/06/2002, “Saal, Alfredo R. c. Organización Veraz S.A.”, LA LEY 2002-F, 335 - DJ 2002-3, 1089; CNCiv, sala A, 2001/11/16, “Arroyo, Jorge H. c. Citibank y otro”, LA LEY 2002-B, 314; LA LEY 2002-D, 262 y DJ 2002-1, 323, (en este caso para Veraz y el BCRA las costas se impusieron por su orden).

[40] CCiv. y Com. Mar del Plata, sala 2, 09/04/2002, “Toyas Pittelli, Omar E. y otros y. Citibank N.A. s/habeas data”, JA 2002-III, fascículo n. 10.

[41] CNCom, sala C, 21/05/2002, “Díaz Velar Hugo Alberto c/Banca Nazionale Del Lavoro Sociedad Anónima s/ordinario", elDial AA1136; CNCom, sala B, 11/01/2000, "Del Giovannino, Luis Gerardo c/ Banco Del Buen Ayre S.A. s/ ordinario", LA LEY 2000-F, 657; DJ 2001-1, 337; ED 190, 287; elDial AA7EC; CNCom, sala C, 14/12/2001/, "Boschi, Mario Andrés c/Citibank N.A. s/ordinario", elDial - AAD44 y LA LEY 2002-D.

correntista.[42]

"Haber sido inhabilitado por error y haber permanecido en esa situación no obstante los inútiles esfuerzos realizados, importan por el mero hecho de su acaecimiento, un sufrimiento o un estado de impotencia frente a la entidad, en la que el cliente se debió sentir poco más que un número de cuenta, ya que no sólo debió transitar la vía judicial para que se quedara satisfecho su derecho, sino que debió cumplir una injusta condena en su integridad, antes de obtener la reparación del error del que fue victima."[43]

La circustancia de figurar en un listado de morosos, cuando la información no se ajusta a la realidad es considerada actualmente como causa de daño moral, el que no requiere mayor prueba[44]. Lo mismo se ha aplicado cuando la persona es

---

[42] CNCom, sala B, 11/01/2000, "Del Giovannino, Luis Gerardo c/ Banco Del Buen Ayre S.A. s/ ordinario", LA LEY 2000-F, 657; DJ 2001-1, 337; ED 190, 287; elDial AA7EC: "Haber sido inhabilitado por error y permanecer en esa situación no obstante los múltiples esfuerzos realizados, importa por el mero hecho de su acaecimiento un considerable sufrimiento y un estado de impotencia frente a la entidad, en la que el cliente debió sentirse poco más que un número de cuenta. El agravio moral supone una modificación en el desenvolvimiento de la capacidad de querer o sentir, que se traduce en un modo de estar de la persona diferente de aquél en que se encontraba antes del hecho; esa alteración puede consistir en profundas preocupaciones o estados de irritación que afectan el equilibrio anímico de la persona. El daño moral infligido está dado por la penuria anímica y moral al que fue injustamente expuesto el actor. El reclamo resulta legítimo, además el agraviado debió litigar con una contraparte que negó los hechos y el derecho del accionante a obtener un justo resarcimiento, con lo que ello implicó en cuanto a pérdida de tiempo, humillaciones, desazones y desasosiego durante más de dos años hasta la sentencia definitiva, situación que se prolonga hasta la fecha. Un ciudadano respetado en el ámbito comercial, en forma imprevista e injusta pasó a ser una persona sin crédito e imputada de graves faltas."

[43] CNCom, sala B, 30/12/2002, "Domínguez Alvaro, Eloy c/Banco Río de La Plata SA s/ordinario", elDial - AA14F3.

[44] CNCom, sala B, 11/01/2000, "Del Giovannino, Luis Gerardo c/ Banco Del Buen Ayre S.A. s/ ordinario", LA LEY 2000-F, 657; DJ 2001-1, 337; ED 190, 287; elDial AA7EC; CNCom, sala B, 24/02/2006, "Hager, Enrique Carlos c/Lloyds Bank y otro s/ordinario", elDial AA33D9 y ED 01/08/2006; CNCom, sala C, 12/04/2005, "E., V. M. J. c. Banco Francés", LA LEY 2005-E,42; CNCom, Sala E, 28/02/2005, "Debaisi Efraín José c/ Banco Río de la Plata S.A. y otro s/ ordinario", Diario Judicial.com 19/04/2005; CNCom, sala D, 20/11/2001, "Mazza, Miriam Elizabeth c/ Citibank N.A. s/ ordinario", elDial AAC4B; CNCom, sala B, 09/09/2003,"Rivera, Raul Enrique c/Banco Frances del Río de La Plata SA s/ordinario", elDial AA1B83.

injustamente inhabilitada como cuenta correntista[45].,

Haber sido inhabilitado por error y haber permanecido en esa situación no obstante los inútiles esfuerzos realizados, importan por el mero hecho de su acaecimiento, un sufrimiento o un estado de impotencia frente a la entidad, en la que el cliente se debió sentir poco más que un número de cuenta[46].

También se ha otorgado resarcimiento por daño moral cuando la actitud negligente de la entidad financiera causó un agravamiento de una situación preexistente, por ejemplo una crisis financiera del actor, si bien no del todo imputable al banco demandado, en la medida que éste incidió en el desenlace final cabe tener por configurado un daño moral resarcible."[47]

Hoy es ampliamente mayoritaria la posición que sostiene que el daño moral, en estos casos, no requiere prueba específica alguna, en cuanto ha de tenérselo por demostrado por el solo hecho de la acción antijurídica, consistente en difundir un informe erróneo, o conductas similares.[48]

La circunstancia de ser incluido en un listado de deudores morosos en forma inexacta ocasiona daño que se revela por sí mismo, sin necesidad de acreditarlo, ya que puede valorarse como notorio.[49] Es conocido en general por todos quienes desarrollan actividades financieras, comerciales, industriales, profesionales o laborales, el efecto negativo -justificado o no, ésa es otra historia que no interesa aquí- que tiene para una persona aparecer como deudor moroso en una publicación como la

---

[45] CNCom, sala B, 01/11/2000,"Del Giovannino, Luis Gerardo c. Banco del Buen Ayre s/ordinario", LA LEY 2000-F, 657; DJ 2001-1, 337; ED 190, 287; elDial AA7EC.
[46] CNCom, sala A, 11/04/2003, "Solares Adrián Daniel c/Bansud SA s/sumario", elDial AA17EB.
[47] CNCom, sala C, 26/09/2003, "Vázquez, Viviana Beatriz c/Banco Río De La Plata Sociedad Anónima s/sumario", LA LEY 2004-B,1017; elDial AA1C2B.
[48] CNCiv, sala F, 16/11/2003, “Fallone, Eugenio Donato c/ HSBC Banco Roberts SA s/ daños y perjuicios”, elDial AA1DD0 y Diario judicial.com 20/01/2004.
[49] CNCom, sala B, 11/10/2006, “Tahhan, Mariana c. Banco Río de la Plata”, LA LEY 2007-B, 801; CNCom, sala B, 24/02/2006, “Hager, Enrique Carlos c/Lloyds Bank y otro s/ordinario”, elDial AA33D9 y ED 01-08-2006.

que efectúan las empresas que brindan informes sobre solvencia o riesgo crediticio.[50]

El daño moral radica en el descrédito que provoca una información negativa, porque enseguida circula en plaza la noticia con la consabida sospecha de insolvencia o irresponsabilidad patrimonial de la perjudicada. Es allí donde radica el agravio moral (art. 522 CCiv.) que debe ser resarcido, sin que quepa sostener que semejante descalificación pueda considerarse una molestia normal de la vida negocial.[51]

Se ha considerado que es procedente otorgar una indemnización por daño moral a quien fue erróneamente incluido en un registro de deudores morosos, sin perjuicio que tuviera crédito en diversas instituciones, pues lo que se reclama es una indemnización por el daño moral sufrido y no por la privación de acceso al crédito, pérdida de la "chance" u otro rubro similar.[52]

En otro caso, por cierto no infrecuente, se consideró que "el actuar del banco, que decidió enviarle al actor en forma unilateral una tarjeta de crédito, le remitió resúmenes con saldos deudores por gastos efectuados con tarjetas nunca recibidas por el actor y que informó al B.C.R.A. que el accionante era moroso en el pago del referido plástico, posee entidad suficiente como para causar el daño que se reclama" y que esta conducta fue inexcusable y carente de un mínimo de diligencia (doctrina, Arts. 512, 902, 909 y cctes. Código Civil).[53]

Cuando la institución financiera no tomó las medidas de diligencia, cuidado y

---

[50] CNCom, sala D, 20/11/20010, "Mazza, Miriam Elizabeth c/ Citibank N.A. s/ ordinario", elDial AAC4B.

[51] CNCom C, sala C, 25/09/2007, “Cassidi Diego Martin c/ Visa Argentina S.A. y otro s/ ordinario”(Microjuris MJJ16104; CNCom, Sala D, 05/06/2007, "Larregui, Mariano c/ Banco Itau Buen Ayre y otro s/ ordinario", elDial AA3FC1.

[52] CNCom, sala E, 16/08/2006, “Guryn, Néstor c. Lloyds Bank S.A”, LA LEY 2006-F, 830 y DJ 2007-02-14, 345.

[53] CNCom, sala B, 30/06/2003, "Treviño Oscar c/Banco de Galicia y Buenos Aires SA s/ ordinario, elDial AA1971: “(el juzgador se pregunta) ... cuál sería la sensación del cliente/consumidor/persona cada vez que recibía un resumen con saldo deudor de una tarjeta de crédito que nunca había solicitado ni recibido, de lo que no es aventurado inferir que la experiencia vivenciada por el actor, le deparó situaciones embarazosas y disvaliosas que seguramente alteraron su equilibrio emocional, por lo que corresponde condenar al banco a la reparación del daño moral (Art. 522 Código Civil), instituto que no requiere el dolo para su aplicación."

previsión pertinentes para no difundir datos erroneos o desactualizados sobre juicios iniciados, se genera la obligación de reparar el daño, que puede ser psicológico, y por lo tanto incluido en el daño moral.[54]

Puede distinguirse también una corriente que –aún minoritaria- opina que la condena a resarcir el daño moral cumple también un efecto ejemplarizador.[55]

Debe existir un adecuado nexo de causalidad para que el resarcimiento del daño moral sea procedente.[56]

9.6.2. Daño material

Para que se admita el resarcimiento del daño material, la exigencia de acreditación en su efectividad y existencia de un adecuado nexo causal es mucho más severa, que en los casos reseñados en que se condenó a resarcir el daño moral, lo que determina que sean menos fecuentes los fallos en los que se ha reconocido tal perjuicio.

En algunos supuestos, adecuadamente planteados, se ha reconocido la pérdida de chance.[57] Así se ha resuelto que la indemnización que corresponde fijar

---

[54] CNCiv, Sala H, 04/09/2002, “Sosa Marcelo c/Citibank S.A. s/Daños y perjuicios", elDial AA135C.
[55] CNCom, sala C, 04/12/2001, "Sorín, Daniel Israel c/Banco Sudameris Argentina S.A. s/ordinario", elDial AABB2; CNCom, sala C, 21/05/2002, "Díaz Velar Hugo Alberto c/Banca Nazionale Del Lavoro Sociedad Anónima s/ordinario", elDial AA1136: "… se tiene en cuenta la doble función que reviste la indemnización por daño moral, como reparación a quien padeció las consecuencias aflictivas y como sanción ejemplar al proceder reprochable de quien las hubo causado; CNCom, sala C, 30/06/1993, "Giorgetti, Héctor R. y otro c/Georgalos Hnos. S. A. s/ordinario", LA LEY 1994-D, 113. En el mismo sentido: Jdo Civ. y Com. Nº 10, Rosario, “A., L. c/ American Express S.A. s/ Daños y perjuicios”, Zeus, 16-12-2003: “la indemnización por daño moral adquiere un doble carácter de reparación o resarcimiento para el damnificado y de sanción ejemplar para el responsable, cuyo monto debe guardar proporcionalidad con el agravio padecido, como modo de restaurar el sufrimiento que tal situación importó para la víctima”; CNCom, sala C, 21/06/2006, “Domínguez Carlos Alberto c/ BankBoston NA”, Diario Judicial.com 30/08/2006.
[56] CNCom, sala A, 11/04/2003, "Romo Armando c/Banco Río de la Plata SA s/Daños y perjuicios", el Dial AA17C8.
[57] CNCom, sala E, 05/09/2006, "Gullo Roberto c/Societe Generale y otro s/ ordinario", elDial AA3995.

debe relacionarse con el daño causado por su inclusión errónea en la base de deudores del B.C.R.A. y su divulgación por Internet, no en concepto de lucro cesante, sino encuadrado en la noción de lo que se ha dado en llamar "pérdida de chance", lo cual constituye un daño cierto que debe ser indemnizado, pero que no se asimila al beneficio dejado de percibir, sino que lo resarcible es la chance misma, la que debe ser apreciada judicialmente según el mayor o menor grado de probabilidad de convertirse en cierta, sin que pueda nunca identificarse con el eventual ingreso perdido, tomando para ello importancia, las presunciones judiciales (art. 163:5 del Código Procesal)

Ejemplos de estos pronunciamientos han sido las condenas obtenidas en el caso de un empresario gastronómico, en el que se dijo “La falta de cuestionamiento respecto al modo en que realizaba el actor sus tareas y la permanencia en la actividad comercial durante un prolongado período ... inducen a considerar que existía una probabilidad cierta de que de no haber existido la arbitraria y errónea decisión adoptada por la entidad bancaria demandada, hubiese continuado del mismo modo su labor.- La situación guarda analogía con los casos de frustración contractual que originaron resarcimientos tasados bajo la óptica "chance" de ganancia, cuya pérdida puede y debe considerarse daño resarcible según una corriente doctrinaria y jurisprudencial ..., e impone valorar la perspectiva de su otorgamiento mediante una ponderación cuidadosa de las circunstancias del caso. La indemnización se fijará sobre la "chance" misma, puesto que no puede olvidarse que lo frustrado es ésta, que por su naturaleza es siempre problemática en su realización”[58].

Otro antecedente fue el de un deportista[59], sobre el que se resolvió que "La frustración del viaje al exterior para participar en un concurso deportivo -en una actividad en la que el actor se encuadra en la más alta categoría, le habría ocasionado al actor la pérdida de la chance de ganar premios -en dinero, inclusive-, honores y prestigio"… "Dados los excelentes antecedentes del actor en la actividad deportiva de su especialidad y su participación en varias competencias, es cuanto menos altamente

[58] CNCom, sala B, 30/12/2002, "Domínguez Alvaro, Eloy c/Banco Río de La Plata SA s/ordinario", elDial AA14F3.
[59] CNCom, sala D,02/07,2003, "Tondini, Claudio Oscar c/ Banco Tornquist SA y otro s/ ordinario", elDial AA18CD.

probable -pues resulta ser el común acontecer de las cosas en un deportista de alto nivel- que el actor haya querido participar en un nuevo torneo, y haya intentado comprar y pagar el pasaje con la tarjeta de crédito bloqueada por un error del Banco aquí demandado (Tornquist SA)." En base a estas consideraciones (se juzgó) suficientemente probado que esa errónea inhabilitación de la tarjeta -error que generó la responsabilidad por culpa del Banco, cuya indiscutible profesionalidad le impone un mayor cuidado en su gestión- provocó, en definitiva, la pérdida de la chance del actor de participar en esa competencia deportiva, daño en el que confluyen tanto aspectos patrimoniales -la chance de obtener algún premio en dinero-, cuanto morales -la pérdida de la chance de obtener el prestigio que significa la obtención de un premio-.- Ese daño debe, desde luego, ser reparado por quien lo provocó", y así también pueden citarse otros casos similares[60].

En el caso de suspensión injustificada de una tarjeta de crédito se ha sostenido que el fundamento de la responsabilidad resulta de la violación del deber del banco de dar el servicio de la tarjeta de crédito emitida por su intermedio a favor del actor, empero lo que técnicamente ha perdido el actor es la chance de disponer de ese crédito, que era una expectativa cierta de contar con crédito para adquirir algún bien o servicio, A este perjuicio se le debe detraer el costo del crédito, de modo que para mensurar el valor, no es el del crédito mismo, sino una ventaja estimada (art. 165 del cód. procesal).[61]

En la mayoría de los casos, el daño material invocado es rechazado por defectos en la acreditación del nexo de causalidad o en la prueba de la existencia del daño material, que como hemos dicho, es habitualmente de mayor exigencia que el

---

[60] CNCom, sala B, 01/04,2003, "Cova Rodolfo José c/Banco Caja de Ahorro S.A. s/ ordinario", elDial AA17C0: "En autos se acreditó la imposibilidad de utilizar el medio de crédito contratado con el banco; este evento le ocurrió estando en un país extraño, y habida cuenta las razones de seguridad que hace que generalmente los viajeros no transporten dinero en efectivo es razonable concluir que la privación del uso de su tarjeta de crédito le causo un grave perjuicio (material y espiritual) durante su estadía en el país centroamericano."; CNCom, Sala C, 03/2007, “Shawn Daniel Eduardo c/ Banco Río de la Plata s/ ordinario”, Diariojudicial.com 16-08-2007.

[61] CNCom, sala E, 21/09/2007, "Lagorio José Antonio c/ Banco Galicia y Buenos Aires SA s/ ordinario", elDial AA4328.

daño moral.[62]

El daño material se ha desestimado por falta de prueba aún en supuestos en los que se ha admitido el daño moral[63].

9.6.3. Daño al crédito e imagen comercial

En general, la jurisprudencia niega el resarcimiento del daño moral a las personas jurídicas. La Corte Suprema ha entendido que no cabe otorgar reparación del daño moral a favor de una sociedad comercial, ya que como su capacidad jurídica está limitada por el principio de especialidad y su finalidad propia es la obtención de ganancias, todo aquello que pueda afectar su prestigio o su buen nombre comercial, o bien redunda en la disminución de sus beneficios o bien carece de trascendencia a los fines indemnizatorios, ya que se trata de entes que no son susceptibles de sufrir padecimientos espirituales[64].

Sin embargo, en voto minoritario, Jorge Bacqué entendió que aún cuando el concepto de daño moral, en tanto se relaciona con la lesión a bienes jurídicos extrapatrimoniales, propios de las personas físicas como son sus afecciones legítimas, no resulta en tales términos apropiado en el caso de las personas jurídicas, debe considerarse que éstas, provistas de subjetividad jurídica, poseen atributos de igual naturaleza extrapatrimonial que, si bien de manera indirecta, les son reconocidos para el logro de sus fines específicos. Esos atributos, como el prestigio, crédito comercial, o el derecho al nombre, son valorizados por la comunidad en que se desenvuelven y su menoscabo genera un daño de características similares a la lesión de los bienes extrapatrimoniales, características de las personas de existencia visible y que deben ser objeto de tutela aun al margen de la existencia de un perjuicio patrimonial actual y

---

[62] CNCom, sala A, 08/06/2006, “Canillas, Gustavo F. c. Citibank NA y ot”, LA LEY 2006-F,828.

[63] CNCom, sala D, 23/04/2003, "Kindsuater, Patricia y otro c/ Diners Club Argentina S.A.C. y de T. y otro s/ ordinario", elDial AA17AE: "Es claro que al no serles dado el préstamo, los actores no vieron disminuido su patrimonio -que quedó exactamente como estaba antes de la negativa-, ni tampoco vieron frustrada una ventaja económica futura -pues la ventaja de tomar un préstamo y hacerse de fondos conlleva la obligación de devolverlo con más sus intereses, réditos cuyo pago convierte a la operación en patrimonialmente negativa para el prestatario …”

[64] CS, 22/03/1990, “Kasdorf, S. A. c. Provincia de Jujuy y otro”, LA LEY1991-A, 52

cierto[65].

En la línea de este voto minoritario algunos tribunales han reconocido el resarcimiento a una persona jurídica por la afectación de su imagen comercial[66], señalando que se trata de un perjuicio patrimonial indirecto, exteriorizado por circunstancias tales como la pérdida de crédito, o la imposibilidad de obtener la renovación de un certificado fiscal, entre otras, ya que tales hechos u otros de similar perfil, globalmente considerados, pueden ser apreciados como configurativos del daño a la imagen comercial de una firma.

En similares pronunciamientos se ha dicho que “las personas jurídicas o de existencia ideal pueden ser sujetos pasivos de perjuicios indirectos si son vulnerados sus derechos extrapatrimoniales como el buen nombre, la probidad comercial y su buena reputación, si repercuten desfavorablemente en el patrimonio..."[67]; o que “las personas de existencia ideal poseen subjetividad jurídica y por ende atributos de naturaleza extrapatrimonial que les son reconocidos para el logro de sus fines específicos, como el prestigio comercial, el crédito o el derecho al nombre, entre otros. Si bien de ello deriva que su menoscabo genere un daño similar a la lesión de los bienes extrapatrimoniales característicos de las personas de existencia visible, ... solo deben ser objeto de tutela cuando exista un perjuicio patrimonial aunque fuere

---

[65] ídem nota supra, voto del Dr. Jorge Bacqué.

[66] CNCom, Sala C, 03/2005, “Arquitectura del Agua SA C/ Banco Francés s/ordinario”, Diario judicial.com 08/04/2005; CNCom, sala E, 22/03/2005, “Construcur S.R.L. C/ Banco Rio de la Plata S.A. s/ ordinario”, Derecho y banca.com/ e-boletin 74. "...Destaco a todo evento que este daño a la imagen, no se asimila al daño moral que pueden sufrir las personas físicas, pues como ha sostenido el máximo Tribunal, su capacidad jurídica está limitada por el principio de especialidad -arts. 35 del Código Civil, y 2 de la 19.550-, y su finalidad propia es la obtención de ganancias -art. 1, ley citada-, por lo que todo aquello que pueda afectar su prestigio o su buen nombre comercial, o bien redunda en la disminución de sus beneficios o bien carece de trascendencia a los fines indemnizatorios, dado que se trata de entes que no son susceptibles de sufrir padecimientos espirituales...Las personas jurídicas o de existencia ideal pueden ser sujetos pasivos de perjuicios indirectos si son vulnerados sus derechos extrapatrimoniales como el buen nombre, la probidad comercial y su buena reputación, si repercuten desfavorablemente en el patrimonio..."; CNCom, sala B, 09/03/2005, “Sattler S.A. C/ Banco Río de la Plata S.A. s/ ordinario” DerechoyBanca.com/ E-Boletin 84.

[67] CNCom, sala E, 22/03/2005, “Construcur S.R.L. C/ Banco Rio de la Plata S.A. s/ ordinario”, http://www.derechoybanca.com.ar/normas/JURIS/74-01.HTM)

indirecto, extremo que deber ser acreditado por el pretensor..."[68] "... En este último fallo se agrega que “el buen nombre, el prestigio, la confianza pública, el crédito tiene un valor económico, pues son el resultado de la organización y el funcionamiento de todos los elementos del fondo de comercio y se reflejan en la obtención de la clientela, que es su finalidad..." y “... dado que solo posee un fin lucrativo, su buen nombre, prestigio, etc., se relacionan con la obtención de ganancias y por tanto carece de todo otro interés que no sea económico y material.”, “por lo que una conducta que afecte esa reputación, fama, buen nombre, prestigio, confianza pública, crédito, está privando o afectando un elemento valioso en el sentido de productor de rédito económico.”[69]

En otro caso, en el que el actor era un acreditado empresario que contaba con un stock aproximado de 10.000 videos en su negocio, se consideró que el informe erróneo afectó su imagen comercial, porque debió negociar con dos empresarios editores de películas que ejercen una actividad prácticamente monopólica - Gativideo y AVH.-, con las que trabajó durante ocho años a crédito concertándose las operaciones por vía telefónica, modalidad operativa que fue suspendida, al ser reputado como un "cliente riesgoso", por lo que debió efectuar sus compras en efectivo durante tres meses hasta que pudo regularizar su situación bancaria[70].

En cuanto a personas físicas, se juzgó que el prolongado tiempo en que figuró en los registros pertinentes la incorrecta información respecto del actor, la gravedad de la calificación ("5" = irrecuperable), como así también el hecho de que la información fuera pública, afectó la honorabilidad, prestigio e imagen pública del afectado por la información errónea, en especial, si se tiene en cuenta que se trata de una persona en

---

[68] CNCom, sala B, 10/03/2004, “Kavigo S.A. c/ Banco Bansud S.A. s/ ordinario” , http://www.derechoybanca.com/normas/JURIS/44-05.HTM, remitiendose a otros antecedentes de la misma sala, 11/08/1997, "Linser S.A.I.C. y de Servicios c/ Banco Ciudad de Buenos Aires s/ ordinario", y de la C.N.Com, sala A, 13/09/1996, “Neuromédica S.A. c/ Banco Francés del Río de la Plata S.A. s/ ordinario", E.D. 173-298.

[69] Ídem cita anterior, donde se cita a Rivera, Julio C., "La prueba del daño sufrido por las sociedades", Revista de Derecho de Daños, pág. 225 y sgtes., T. 4, Ed. Rubinzal Culzoni, Bs. As. 1999, más allá de rechazar el reclamo por que no se acreditó la existencia de daño, que haya quedado reflejada en una merma de las ganancias.

[70] CNCom, Sala A, 11/04/2003, "Solares Adrián Daniel c/ Bansud SA s/sumario", eldial.espress 24/06/2003 y http://www.derechoybanca.com/normas/JURIS/18-01.HTM.

la plenitud de su capacidad laboral y que posee un grupo familiar que, de un modo mediato también se vió afectado por el episodio dañoso.[71]

Un supuesto interesante, fue resuelto por la sala F de la Cámara Civil, ya que si bien se rechazó al resarcimiento por la pérdida o afectación del prestigio comercial de una sociedad anónima, se otorgó, aún cuando reduciéndo lo resuelto en primera instancia, indemnización a título de pérdida de chance, como "lesión al crédito", al entender que la sociedad vio encarecido el costo del crédito por haber figurado erróneamente informada como deudora.[72]

La misma sala entendió que una información errónea, mantenida en registros públicos de deudores morosos durante años, no rectificada a pesar de los reclamos de la coactora, no obstante la inexistencia de un auténtico sustento que la justificara, ha devenido por sí misma en un obrar antijurídico por acción y por omisión lesiva al buen nombre de los actores, ... que es una de las manifestaciones objetivas del honor de las personas.[73]

9.9. Usuarios y fuente de los datos

Nos hemos referido al concepto de "fuente" en el tratamiento de datos personales en el capítulo anterior.

En nuestra opinión, la fuente de la información responde por la calidad de los datos suministrados a agencias, otras entidades o usuarios, porque tiene acceso y suministra información personal de terceros. Estas circunstancias la sujetan al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos.

Similar responsabilidad se extiende al denominado "usuario", en el caso en que

---

[71] CamCivyCom Tucumán, Sala I, 28/04/2005, "Romano Domingo Enrique c/ Banca Nazionale del Lavoro S.A. s/ daños y perjuicios", http://www.derechoybanca.com/normas/JURIS/86-03.HTM..

[72] CNCiv, Sala F, 15/12/2003, "Aguara S.A. y otro c/ Banco de Galicia y Buenos Aires S.A. s/ daños y perjuicios", diario judicial.com 12/02/2004

[73] CNCiv, sala F, 07/09/2004, "Varela, Juan Carlos y otro c./ Lloyds TSB Bank s./ daños y perjuicios", LA LEY online.

éste a su vez entregue la información directamente a un banco de datos u otro operador del sistema, ya que adquirirá la doble condición de usuario y fuente, y es lógico que asuma los deberes y responsabilidades de ambos, para que el sistema de protección de datos tenga consistencia.

En nuestra opinión, en consecuencia, el deber de respetar los principios de tratamiento de los datos personales (art. 4º, ley 25.326), y en el caso especial de los informes crediticios lo previsto en el art. 26 de dicha ley, se extiende a todos los sujetos que intervienen en el procesamiento de tales datos, sean responsables de ficheros, fuente de los datos o usuarios[74].

En consecuencia, todos los actores en la generación de informes crediticios son legitimados pasivos, y no sólo la entidad bancaria que emitió la información dañina. Incluimos a quienes la difunden.

Como hemos señalado anteriormente, las entidades financieras vienen esgrimiendo que no son legitimados pasivos en las acciones sobretodo de habeas data, más allá de la particular visión que mantienen sobre el llamado “derecho al olvido”. Su posicionamiento como “usuarios” apunta a sostener que no están comprendidos en la obligación del art. 26 de suprimir los datos caducos, ya que no son bancos de datos destinados a proveer informes crediticios.

En este aspecto parece no tenerse en cuenta el art. 9 de la ley 25.326, que –en

---

[74] CNCiv, sala B, 07/04/2009, “Sanchez, Miguel A. c/ Banco de Galicia y Buenos Aires y otros », elDial AA52FD: “La Ley 25.326 de Protección de Datos Personales establece específicamente en su artículo cuarto el principio de calidad de los datos, que exige que el responsable del archivo se comprometa activamente para que la información almacenada sea adecuada y pertinente, esté al día, sea exacta, verdadera y, en lo posible, completa, de acuerdo a la finalidad de su registración. Esta disposición tiene sustento constitucional en al artículo 43 de la Carta Magna que crea un derecho sustantivo a exigir veracidad y actualización respecto a los datos volcados de todos aquellos que aparecen registrados en bancos de datos públicos o privados." "Resáltase que estos aspectos adquieren suma importancia cuando se trata de archivos relativos a la solvencia y al riesgo crediticio del titular; no ya por motivos que hacen a la protección de bienes jurídicos inmateriales como el honor o la intimidad, sino porque estos datos tienen la finalidad específica de servir para la adopción de decisiones en el mercado del crédito, en el cual una historia negativa cierra las puertas de acceso al sistema (Cfr. Gils Carbó, Alejandra "Régimen Legal de las Bases de Datos y Habeas Data", Ed. La Ley, Buenos Aires, 2001, p. 150 y sgtes.)."

nuestra opinión torna abstracta- a estos fines, dilucidar si se es responsable o usuario, ya que dice que "*el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado."* y la norma agrega que "*queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad*". Nos parece inexcusable interpretar el concepto de adulteración con el principio de calidad general (art. 4º) y el plazo del art. 26.

Por otro lado, el art. 35 de la misma ley legitima tanto a los responsables como a los usuarios para ser demandados por habeas data.

Ante el argumento de un banco demandado que sostenía que no era una entidad destinada a proveer informes a terceros, lo que excluiría la aplicación del art. 43, tercer párrafo, de la Constitución Nacional, se resolvió que la garantía del habas data alcanza aún aquellos supuestos en los que no interviene una entidad destinada estrictamente a proveer informes (arg. arts. 2 y 33, inc. 1-b, ley 25.326) y que en todo caso, resta siempre la protección genérica del amparo, basada en el ler. párrafo del art. 43, toda vez que se halla en juego la garantía contemplada en el art. 42 de la misma Constitución inherente al derecho de los consumidores a una "información.adecuada y veraz", lo que implica que, sea por la vía del habeas data, específícamente dirigida a la protección de los datos de las personas, o bien por la vía genérica del amparo, esta argumentación del banco resulta estéril[75].

9.10. La nueva ley de defensa del consumidor y los bancos de informes crediticios.

9.10.1. Extensión del concepto de relación de consumo.

La primera consecuencia (consecuencia de qué; habría que decir que la ley incorporó el concepto de relación de consumo, contenido en la cláusula constitucional y que esa incorporación tuvo por consecuencia) que advertimos reside en la

[75] CNCom, sala C, 26/03/2002, "Halabi, Ernesto c/ Citibank NA", elDial AAE44:

ampliación que contiene el Ar.1º, párr. 2º de la ley, en virtud del texto de la ley 26.361, ya que "considera asimismo consumidor o usuario a quien, sin ser parte de una relación de consumo, como consecuencia o en ocasión de ella adquiere o utiliza bienes o servicios como destinatario final, en beneficio propio o de su grupo familiar o social, y (el resaltado es nuestro) a quien de cualquier manera está expuesto a una relación de consumo."

Esta expansión del ámbito de los consumidores incluye, sin duda, a quienes resultan afectados por los informes crediticios; la situación está ahora clara en la ley, más allá de la doctrina jurisprudencial que había resuelto numerosos casos de informes crediticios erróneos encuadrando el tema en el derecho del consumidor a una información adecuada, oportuna y veraz, como hemos señalado precedentemente.

9.10.2. Nuevo paradigma de respeto a los consumidores.

Otra norma que debería cobrar relevancia en esta materia es el nuevo art. 8° bis, sobre "Trato digno y prácticas abusivas", que obliga a los proveedores a garantizar condiciones de atención y trato digno y equitativo a los consumidores y usuarios y abstenerse de desplegar conductas que coloquen a los consumidores en situaciones vergonzantes, vejatorias o intimidatorias.

En especial, la prohibición de utilizar cualquier medio que le otorgue la apariencia de reclamo judicial, en los reclamos extrajudiciales, es –en nuestra opinión- una veda concreta a la utilización de los informes crediticios como procedimiento para el cobro extrajudicial de deudas, al que nos hemos referido también.[76]

En consecuencia, consideramos procedente –cuando se incurra en tales conductas- además de las sanciones previstas en la LPDPA (Artículo 31 y ss.), la aplicación de la multa civil establecida en el artículo 52 bis de la nueva LDC, sin perjuicio de otros resarcimientos que correspondieren al consumidor.

---

[76] Así lo decimos en el capítulo 8, 8.9 Síntesis. Es una práctica aceptaba por bancos y grandes empresas la remisión a los burós de crédito de informes sobre deudas, en muchos casos litigiosas, especulando que el afectado preferirá pagar –aunque no deba o cuestione la obligación- para no ver cercenado su acceso a un crédito que le resulta esencial.

La nueva LDC ha establecido la responsablidad solidaria de los proveedores que sean responsables del incumplimiento, cuando sean más de uno, sin perjuicio de las acciones de regreso que corresponda. No ignoramos que es un tema se trata de una cuestión conflictiva, que ha merecido críticas. Sin embargo, creemos que debería ser tenida en cuenta si se pretende una verdadera protección del consumidor que ve afectados sus intereses por la actuación –activa u omisiva- de diversos actores, que como hemos explicado en el capítulo anterior, integran una red indescindible en la generación de los informes crediticios. La víctima de errores, inobservancia de la calidad en el tratamiento de los datos personales o cualquiera de las conductas que hemos mencionado al inicio de este capítulo, enfrenta –entre otras dificultades- el dilema de elegir a quien demandar judicialmente, pendiendo sobre su ya deteriorado patrimonio una suerte de "espada de Damocles", ya que la prestadora de servicios sobre solvencia crediticia dirá que no tiene la culpa pues el informe lo obtuvo del Banco Central; éste invocará que se limitó a reproducir la información que recibió de las entidades financieras, y finalmente, podría ocurrir que estas hayan caído en estado de falencia. Vale la pena visualizar el conflicto e imaginar soluciones que resuelvan efectivamente el daño causado, sobretodo cuando existe una norma legal que da pie para utilizar la responsabilidad solidaria en un contexto como el que hemos descripto y cuya demostración es innecesaria.

9.10.3. Legitimados pasivos

Continuando con el razonamiento anterior, si ahora el concepto de consumidor se ha expandido, un afectado por informes crediticios erróneos o que no se ajusten al principio de calidad –de acuerdo a los criterios establecidos por la Corte Suprema, antes expuestos- podrá reclamar la reparación de los daños no sólo a quien lo originó, sino también a quienes lo distribuyeron o publicaron, realizando una interpretación funcional del artículo 40 de la ley.

9.10.4. Daño directo

Además, el nuevo Art. 40 bis resulta muy útil al definir como "daño directo" a "todo perjuicio o menoscabo al derecho del usuario o consumidor –entendido en su expresión amplia conforme al nuevo art. 1º- susceptible de apreciación pecuniaria, ocasionado de manera inmediata sobre sus bienes o sobre su persona, como consecuencia de la acción u omisión del proveedor de bienes o del prestador de servicios.

En tal sentido, consideramos que la no observancia del principio de calidad, de acuerdo a los estándares fijados por la Corte Suprema, interpretando la LPDPA, es una acción u omisión del proveedor, que debe analziarse conforme hemos señalado, en los términos del art. 40 y que abarca al presunto acreedor, el banco, la empresa de informes crediticios, el Banco Central y aún el Poder Judicial.

9.10.5. Daño punitivo

Finalmente, consideramos que una inteligente aplicación de la gran novedad que constituye el Art. 52 bis, al introducir en el ordenamiento jurídico positivo argentino el llamado “daño punitivo”, también llamado por la ley “multa civil” puede contribuir decisivamente a sanear el mercado de los informes crediticios.

Esta multa a favor del consumidor no puede superar el máximo de la sanción de multa prevista en el artículo 47, inciso b) de la ley y, en nuestra opinión, debe cumplir una función disuasora de prácticas distorsivas que se observan a diario, fomentadas por el escaso costo económico que la comisión de estas conductas podía acarrear

La novedad de la reforma al establecer que “al proveedor que no cumpla sus obligaciones legales o contractuales con el consumidor, a instancia del damnificado, el juez podrá aplicar(le) una multa civil a favor del consumidor, la que se graduará en función de la gravedad del hecho y demás circunstancias del caso, independientemente de otras indemnizaciones que correspondan”, otorga a los magistrados una inmejorable oportunidad para no sólo reparar el daño, sino también sancionar la conducta impropia, con efectos disuasorios.

De este modo, el mercado de informes crediticios, cuya importancia nadie discute, observará las pautas y criterios que surgen de la ley y su interpretación por el máximo tribunal de justicia.

De lo contrario, como hemos señalado en numerosas exposiciones y artículos, el sistema de protección de datos personales en el ámbito de los informes crediticios continuará malversado en un sistema de cobranza de deudas que no es económico reclamar judicialmente, o con graves errores que no se subsanan porque es más barato pagar de vez en cuando alguna escasa indemnización que invertir en la mejora de infraestructura, recursos humanos y tecnología para honrar el principio de calidad

ya comentado.

9.10.6. Cadena de responsables

La reforma agrega que “Cuando más de un proveedor sea responsable del incumplimiento responderán todos solidariamente ante el consumidor, sin perjuicio de las acciones de regreso que les correspondan.”

En consecuencia, todos los actores en la generación de informes crediticios son legitimados pasivos, y no solo la entidad bancaria que emitió la información dañina. Incluimos a quienes la difunden.

9.11. Síntesis

El panorama jurisprudencial en materia de responsabilidad derivada de los informes crediticios es aún poco consistente. Existen diferencias en cuanto a quienes están legitimados pasivamente, cuales son los supuestos encuadrables como conducta antijurídica, y qué daños son reparables.

Sin perjuicio de ello, y sobre todo a partir de pronunciamientos de la Corte Suprema de Justicia de la Nación, se ha abierto una interpretación más acorde con las finalidades de la LPDPA, otorgando a los principios rectores del tratamiento de datos personales, y especialmente al principio de calidad, la relevancia que tienen.

También se comienza a advertir un reconocimiento de que estos principios son plenamente aplicables a los informes crediticios.

Si bien es cierto que, en general, sólo se ha condenado a las entidades financieras cuando han incurrido en informes erróneos, exculpando en la mayoría de los casos a los otros actores (empresas de informes crediticios, Banco Central, Poder Judicial), también han existido pronunciamientos en contra de las empresas de informes, y en mucha menor medida, del Banco Central. Queda como asignatura pendiente que el propio Poder Judicial reconozca que la LPDPA también rige en dicho ámbito.

Constituye un avance la doctrina que considera implícita la existencia de daño moral cuando una persona es incluida indebidamente en listados de deudores morosos, o hay reticencia en corregir la situación. Sin embargo, los importes de

condena suelen ser intrascendentes para motivar a los actores del sistema a modificar sus prácticas y evitar que se ocasionen los perjuicios.

Por esta razón, promovemos la aplicación de multas civiles, por lo menos hasta que estos actores del sistema reconduzcan sus procedimientos y entiendan que es obligación de todos ellos observar, principalmente, los recaudos de calidad en el tratamiento de datos personales dirigidos a evaluar la solvencia o el riesgo crediticio.

Capítulo 10. Conclusiones.

Hemos investigado el área de la protección de datos personales, también conocida como autodeterminación informativa y relevado los principios y reglas que rigen en dicho campo, para poder establecer las consecuencias que se derivan de su inobservancia, en particular la responsabilidad derivada de la difusión de informes sobre solvencia crediticia.

También se incluye a la protección de datos personales, autodeterminación informativa o libertad informática como parte del núcleo de los derechos denominados de "tercera generación".

Estos derechos de tercera generación se presentan como una respuesta al fenómeno de lo que se ha denominado “contaminación de las libertades” *–pollution des libertés–* término con el que en algunos sectores de la teoría social anglosajona se hace alusión a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías.

Además de la autodeterminación informativa o libertad informática integran el plexo de los derechos de tercera generación el derecho a la paz, los derechos de los consumidores, el derecho a un medio ambiente sano y el derecho a una calidad de vida, derechos éstos dirigidos a potenciar la esfera de libertades del individuo en la era tecnológica. Se mencionan también como derechos de tercera generación a la autodeterminación, la independencia económica y política, la identidad nacional y cultural, a la coexistencia pacífica, al entendimiento y confianza, a la cooperación internacional y regional, la justicia internacional, el uso de los avances de las ciencias y la tecnología, la solución de los problemas alimenticios, demográficos, educativos y ecológicos.

En síntesis, coincidimos con quien afirma que el derecho fundamental a la protección de los datos de carácter personal, como derecho de la llamada tercera generación, es uno de los exponentes del conflicto tecnología-Derecho, cuya razón de ser reside en dar al individuo la posibilidad efectiva de disponer y controlar los datos que le conciernen.

La reseña de los documentos (recomendaciones, declaraciones, tratados

europeos, directivas y reglamentos) indican que existe una clara preocupación internacional por los efectos que produce el tratamiento de datos personales, y las principales pautas o criterios que se encuentran en los mismos constituyen elementos orientadores y de consulta imprescindible cuando se analice la aplicación de la normativa argentina en esta materia. Como se irá corroborando al relevar otros sectores del derecho comparado, la moderna construcción de protección de los datos personales o autodeterminación informativa, como se prefiera, excede largamente el ámbito de la tutela a la intimidad o vida privada, aún cuando claramente la contiene.

3. Los países europeos, como se ha visto, han adaptado sus legislaciones internas a la Directiva del Parlamento Europeo y el Consejo de Ministros de la Unión Europea, en el marco de la Comunidad Europea de 1995.

Las principales coincidencias las encontramos en el reconocimiento de un conjunto de principios y reglas específicas para el tratamiento de los datos de carácter personal, enunciados en el Convenio de Estrasburgo de 1981, y que con mayor o menor grado de detalle han sido incorporados a las normas nacionales.

En una breve reseña de estos principios mencionamos la existencia de una autoridad ú órgano de control especial, con diverso rango y características según los países, pero con la exigencia de independencia del órgano ejecutivo; los principios de licitud, calidad, consentimiento, conocimiento o información y participación, instrumentados mediante los derechos de acceso, actualización, rectificación y supresión, que comentamos en particular en el capítulo 6.

Sin perjuicio de ello, cabe aclarar que no todas las leyes se ocupan particularmente de los informes crediticios, situación que ha preocupado más a los países latinoamericanos, y desde otra perspectiva a Estados Unidos.

Finalmente, la normativa comunitaria europea procura armonizar la protección de la intimidad y otros derechos personales, con la particular evolución hacia la autodeterminación informativa que hemos señalado, y la libre circulación de los datos personales y las mercaderías. Desde este punto de vista, no siempre la conciliación de ambos objetivos se ha inclinado a favor de la protección de datos.

La aceptación de las exigencias de Estados Unidos luego de los atentados a las Torres Gemelas se produjo, de algún modo, con la Directiva 2006/24/CE de 15 de

marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, que modificó la Directiva 2002/58/CE (relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas), tema que excede los alcances de este trabajo, pero es válido aclarar que se estableció, en esta última directiva, que "se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado (pero) no se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas".

Desde el inicio de la década de los setenta, el Congreso de los Estados Unidos ha aprobado numerosas leyes para proteger la privacidad en varios sectores, aunque varias leyes o estatutos han estipulado la recolección gubernamental de la llamada información sensible, práctica que se ha intensificado luego de los atendados del 11 de setiembre de 2001 con la conocida como Patriot Act, que ha modificado en forma sustantiva la legislación vigente en torno a la privacidad en línea e incrementado la facultad de los organismos de impartición y administración de justicia para autorizar la instalación de equipos de intervención telefónica y dispositivos de rastreo, así como la instalación de dispositivos que canalicen, envíen y señalen la información de las computadoras.

Varias constituciones de los países de América Latina, con enfoques a veces distintos, han incorporado el derecho a acceder y en su caso obtener su rectificacion o modificación, de los datos personales, ya sea bajo la vía procesal del denominado hábas data, como una variante de la tutela del derecho a la intimidad, o con mayor grado de desarrollo, en los términos del moderno concepto de autodeterminación informativa.

Este proceso es relativamente reciente y se inicia a fines de los ochenta en Brasil y se ha ido desarrollando en mediados de la última década del siglo pasado, en Colombia, Perú, Paraguay, Ecuador, Venezuela, Guatemala, Nicaragua, Bolivia y Honduras, por lo menos hasta el momento de escribir este documento.

En cuanto a las legislaciones nacionales, su orientación es más diversa. Brasil ha reglamentado el procedimiento de habeas data, pero luego ha incorporado en el

Código de defensa del consumidor reglas asimilables al principio de calidad de los datos.

Las normas de Chile, Colombia, Paraguay, al estilo de la ley argentina, efectúan una regulación general del tratamiento de datos personales.

Perú no solo ha reglamentado el habeas data, sino que ha sancionado normas en materia de centrales de informes crediticios, lo mismo que México.

Uruguay, Panamá, Venezuela, El Salvador y Panamá en cambio, han destinado su legislación, con diverso alcance, a los informes crediticios o de solvencia.

Aunque el proceso latinoamericano está menos extendido que el europeo, el tema de la protección de datos está presente en la agenda de la mayoría de los países, independientemente de la existencia o no de legislación específica.

En tal sentido, la Red Iberoamericana de Protección de Datos, constituída en 2003, a impulso de la Agencia Española de Protección de Datos, en su VI encuentro, llevado a cabo en el 2008 aprobó una declaración en la ciudad de Cartagena (Colombia) en mayo de 2008, que recoge los principios rectores que aparecen en la mayoría de los documentos internacionales y legislaciones nacionales mencionados.

Argentina es considerado en el contexto de naciones de América Latina como uno de los países que cuenta con una legislación más avanzada en materia de protección de datos personales, situación que le ha permitido ser calificada por el Grupo creado por el art. 30 de la Directiva europea 95/46 como país que cumple con las exigencias de dicha normativa. En el año 2003 la Unión Europea ha otorgado a la normativa argentina la adecuación en los términos de la Directiva N° 95/46/CE, según Decisión de la Comisión Europea C(2003) 1731 del 30 de Junio de 2003.

Ello no es óbice para señalar que se trata de una legislación poco conocida en el ámbito judicial, y de escasa aplicación integral, sobre todo en cuanto a los principios que la informan.

Para el supuesto de analizarse una reforma, sería recomendable tener en cuenta la reciente ley colombiana, que es mucho más detallada en diversas cuestiones que la norma nacional no tuvo en cuenta, además de la evolución que el tema ha

tenido desde los casi diez años de su sanción.

El tratamiento de los datos personales tiene una gran incidencia en la actividad económica, y afecta en especial diversos aspectos que merecen protección, sin perjuicio del tradicional derecho a la intimidad, como son el prestigio e imagen de un comerciante o empresario, el acceso al crédito y lo que podríamos denominar el derecho a un “buen nombre” en el ámbito de los negocios.

Buenos Aires, setiembre de 2009

Bibliografía

Textos

- Acciai, Riccardo, “Privacy e banche dati pubbliche”, Cedam, Milan, 2001.

Adams, Elbridge, L., “The Right to Privacy and its Relation to the Law of Libel”, 39 American Law Review, 37, January – February 1905. y pp 37 – 58, citado por Puente de la Mora.

- Aldazábal, Benito J., “Acoso ilegítimo de la A.F.I.P. a abogado que defiende contribuyentes. Un fallo ejemplarizador”, LA LEY 1999-E, 608.
- Alexy, Robert, “Los Derechos Fundamentales en el Estado Constitucional Democrático”, en Carbonell, Miguel (Edit.), Neoconstitucionalismo(s), 2ª Edición, Trotta, Madrid, 2005.

Alexy, Robert, “Teoría de los Derechos Fundamentales”, Centro de Estudios Políticos y Constitucionales, Madrid, 2001.

- Alferillo, Pascual E., “Reflexiones sobre el "Habeas data" en la ley adjetiva de San Juan”, LLGran Cuyo, 2000-533.
- Alpa, Guido e Bessone, Mario, “Banche dati telematica e diritti della persona”. Cedmam, Padova, 1984.
- Alpa, Guido, “La disciplina dei dati personali”, Seam, Milán, 1998.
- Altmark, Daniel R. y Molina Quiroga, Eduardo, "Habeas Data y reforma constitucional", I Congreso Internacional de Informática y Derecho, Mérida; España 1995, En Informática y Derecho, UNED, Dir. Valentín Carrascosa López, vol. 11 y 12.

Altmark, Daniel R. y Molina Quiroga, Eduardo, "Habeas Data", LA LEY 1996-A, 1554.

- Altmark, Daniel Ricardo y Molina Quiroga, Eduardo, “Régimen jurídico de los bancos de datos”, Editorial Depalma, Colección “Informática y Derecho”, volumen 6.

Álvarez B. de Bozo, Miriam; Ávila Hernández, Flor María; Peñaranda Quintero Héctor Ramón, “La libertad informática: derecho fundamental en la Constitución Venezolana” Universidad del Zulia (LUZ). Maracaibo. Venezuela, Organización Mundial de Derecho e Informática (OMDI). Maracaibo. Venezuela, http://www.ulpiano.com/bol8_venezuela.htm.

- Álvarez Echagüe, Juan Manuel, “El hábeas data en materia tributaria: Posibilidad de acceso del contribuyente a los datos del Fisco”, LA LEY 2003-D, 1036.
- Álvarez Larrondo, “Obligaciones de los bancos de datos prestadores de servicios de información crediticia. Una importante modificación legislativa que, por tardía, ve limitada su aplicación práctica”, LA LEY, 2008-A,1103.

Amadeo, Mario, "La Constitución de los Estados Unidos de América Anotada con

Jurisprudencia", Ed. Kraft, Buenos Aires, 1949.

- Antik, Analía; Ramunno, Luis A., “Hábeas data. Comentarios sobre los bancos de datos privados destinados a proveer informes”, LA LEY 2000-B, 1164.
- Arrabal de Canals, Olga, en “Derecho a la información, Habeas data e Internet”, Armagnague, Juan Fernando (Dir.) Abalos, Maria G. y Arrabal de Canals, Olga (Coord), Ed. La Rocca, Buenos Aires, 2002.
- Astudillo de Matiello, María Teresa, “Acerca de los límites de la jurisdicción de Alzada, el Hábeas data, la doctrina de los actos propios y la prueba”, LLGran Cuyo 2003 (abril).
- Baigorria, Claudia E., “Algunas precisiones sobre la procedencia del hábeas data”, LA LEY 1996-C, 472.
- Balsa, Maria, “Las bases de datos de las entidades financieras. El Habeas data y el derecho a la información”, en Anuario de Derecho Comercial 11, Fundación de cultura universitaria, Montevideo, 2006.
- Barbier, Eduardo Antonio, “Litigiosidad en la actividad bancaria”, ed. Astrea, Buenos Aires, 2008.

Bayo, Oscar, “Habeas data. Un derecho constitucional en su adecuado cauce como resultado de una decisión elogiable.”, LLC 1995, 945.

- Bazán, Víctor, “El hábeas data ante una interesante muestra de activismo judicial”, LLLitoral, 2000-458.
- Bazán, Víctor, “El hábeas data ante una visión jurisdiccional restrictiva”, LA LEY 1999-A, 204.
- Bazán, Víctor, “Habeas data, registros de cumplimiento o incumplimiento de obligaciones patrimoniales, y saneamiento del crédito: la copa medio llena o medio vacía”, LA LEY 1999-F, 295.
- Bazán, Víctor, “La ardua tarea judicial de imaginar el sendero procedimental por el que discurrirá la acción de hábeas data”, LLGran Cuyo, 1998-419.

Bazán, Víctor, “La protección de datos personales y el derecho de autodeterminación informativa en perspectiva de Derecho comparado”, LL Gran Cuyo, 2005-junio, 453.

- Beckerman, Jorge, "Banco de Datos y responsabilidad objetiva", (Congreso Internacional de Informática y Derecho, AABA-ADIJ, Bs.As., octubre 1990.
- Beheran, Roberto, “El amparo y las acciones de ejecución y prohibición en Entre Rios”, Delta Editora, Paraná, Entre Ríos, Argentina. 1995.

Bergel, Salvador D., "El habeas data: instrumento protector de la privacidad", Revista de Derecho Privado y Comunitario, Ed. Rubinzal Culzoni Nº 7, Derecho Privado en la reforma constitucional, Santa Fe, 1994.

- Bianchi, Alberto B., “El hábeas data como medio de protección del derecho a la información objetiva en un valioso fallo de la Corte Suprema”, LA LEY 1998-F, 297.

Bianchi, Alberto, “Habeas data' y derecho a la privacidad", ED, 161-866.

- Bidart Campos, Germán J. “¿Habeas data, o qué? ¿Derecho "a la verdad", o qué?”, LA LEY 1999-A, 212.

- Bidart Campos, Germán J., “La investigación por la desaparición de personas en una causa penal por privación de libertad”, LA LEY 1998-E, 215.
- Bidart Campos, Germán, “El derecho de petición, de acceso a la información y el recurso de insistencia en el derecho colombiano”, ED, 166-41.
- Boada, Claudio Daniel, “Hábeas data. Instituciones públicas de educación superior. Acerca de la sanción de la ley 25.200”, LA LEY 2000-E, 1247.

Boletín de Jurisprudencia Constitucional Nº 33, de 1984, Revista Derecho Público Contemporáneo Nº 7, de la Agrupación de Abogados de la Contraloría General de la República de Colombia.
Bortolotto, Verenna, “Protección de Datos Personales contenidos en las Bases de Datos Informatizadas y no Informatizadas obrantes en el Poder Judicial Uruguayo”, Revista Derecho Informático Alfa Redi 96, julio 2006.

- Busto Lago, José Manuel, en “Tratado de responsabilidad civil”, Reglero Campos, L. Fernando (Coordinador), Ed. Thomson-Aranzadi, Pamplona, 2006 (3ª.edición).
- Cafferata, Juan Carlos, “La acción de hábeas data”, LLC 1996, 313.
- Campanella de Rizzi Elena M. y Stodart de Sasim, María, "Derecho a la Intimidad e Informática”, LA LEY, 1984-B-667.
- Carranza Torres, Luis R. “¿Necesita Córdoba una ley provincial de hábeas data?”, LLC 2001, 241.

Carrascosa López, Valentín, "Derecho a la Intimidad e Informática", Informática y Derecho UNED, 1-1992.

- Cattaruzza, Adriano, Galbiati, Roberto, Panieri, Bruno, Zampetti, Andra, “La privacy informatica”, Ed. Buffetti, Roma, 1997.

Cerda Silva, Alberto, “Autodeterminación informativa y leyes sobre protección de datos”, Revista chilena de Derecho Informático Nº 3 Diciembre 2003. Universidad de Chile. Facultad de Derecho,
http://www.derechoinformatico.uchile.cl/CDA/der_informatico_completo/...

- Chirino Sánchez, Alfredo, “El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales”, Editores del Puerto, Buenos Aires, 1997.

Cifuentes, Santos, "Acciones procesales del art. 43 de la Constitución Nacional", LA LEY 1999-A, 258.

- Cifuentes, Santos, “Acciones procesales del artículo 43 de la Constitución Nacional - Naturaleza personalísima de los datos informáticos de la persona”, LA LEY 1999-A, 258.
- Cifuentes, Santos, “Derecho personalísimo a los datos personales”, LA LEY 1997-E, 1323.

Cifuentes, Santos, “Derechos personalísimos”, Editorial Astrea, 2da, edición, Buenos Aires, 1995.
Cifuentes, Santos, “El derecho a la intimidad”, E.D. 57-832.

- Cifuentes, Santos, “Protección inmediata de los datos privados de la persona. Hábeas data operativo”, LA LEY 1995-E, 293.
- Cifuentes, Santos, “Reconocimiento jurisprudencial del derecho a los datos personales informáticos y del hábeas data en su verdadero fin tutelar”, LA LEY 1999-E, 151.
- Colautti, Carlos E. “Reflexiones preliminares sobre el "Habeas data", LA LEY 1996-C, 917.

Colley, Thomas, "The elements of Torts", 2a edición, 1988, p. 29.
Consejo para la consolidación de la Democracia, “Reforma constitucional-Examen preliminar del Consejo para la consolidación de la Democracia”, Eudeba, Buenos Aires, 1986.

- Conway, Graciela M. “Las medidas de seguridad en los bancos de datos”, LA LEY 2002-D, 1237.
- Corasaniti, Giuseppe, “Diritto e tecnologie dell´informazione” Liberta Universita Internazionales degli Studio sociali Roma No. 11, Giuffre Editore, 1990.

Coronel Carcelén, Felipe Francisco, “La protección del derecho a la vida privada en internet y otros medios de comunicación electrónicos” (borrador de tesis UCPChile), http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/coronel.pdf/

- Correa, Carlos y otros, "Informática, Libertad y Derechos Humanos", en Correa, Nazar Espeche, Czar de Zalduendo y Batto, “Derecho Informático”, Depalma, Buenos Aires, 1987.
- Craig, John DR, “Privacy & employment law”, Hart Publishing, Oxford, Portland Oregon, 1999.
- Cuffaro, Vincenzo y Ricciuto, Vincenzo, “La disciplina del trattamento dei dati personali”, G.Giappichelli editores, Turin, 1997.
- Curá, José María “Los datos personales a la espera de protección”, LA LEY, 2003-A, 1282.
- Davara Rodríguez, Miguel Ángel, “Derecho Informático”, Aranzadi, Pamplona, 1993.

De Cupis, Adriano en "I Diritto della personalitá", Giuffre, Milán, 1982.

- De Cupis, Adriano, “I diritti Della personalita”, tº I, en “Trattato di diritto civile e commerciale”, Cicu. Antonio; Messineo, Francesco, vol. IV, Giuffre, Milán, 1959.

De Cupis, Adriano, Instituciones de Derecho Privado”, Giuffre editore, Milán, 1983.
Declaración de la Asociación de Abogados de Buenos Aires del 06/06/2001, http://www.aaba.org.ar/

- del Peso Navarro, Emilio y Ramos González, Miguel Ángel “LORTAD-Análisis de la Ley”, ed. Díaz de Santos, Madrid, 1998.
- del Villar, Rafael “Consideraciones económicas de la regulación de Sociedades de Información Crediticia: El Caso de México”, ponencia presentada en Seminario-Taller sobre Datos Personales, Internet y Sistemas Judiciales 8 y 9

de julio de 2003, Costa Rica.
http://www.iijusticia.edu.ar/Seminario_Taller/textos.htm

Denninger, Erhard, en Pérez Luño, Antonio (director de la edición), “Problemas actuales de la documentación y la informática jurídica”, Editorial Tecnos S.A., 1987, Madrid.

- Di Vito, Aldo M. Guerendiain, Hilario J., “La ley de Habeas data. Aspectos Procesales. Aportes doctrinarios y jurisprudenciales”, LA LEY 2001-F, 1362.

Díaz Maynard, Daniel, Informe del proyecto de ley de “Derecho a la información y acción de hábeas data”, presentado ante el Parlamento de la República Oriental del Uruguay, http://www.parlamento.gub.uy/repartidos/camara/d2002060114-01.htm.

- Díaz Molina, Iván, "El Derecho de Privacy en el Common Law y en el Derecho Civil (estudio comparativo)", en Boletín de la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Córdoba, año XXVII, citado por Rivera.

Díaz Molina, Iván, “El derecho a la vida privada”, LA LEY 126-985.
Dresner, Stewart H. "Panorama de la legislación europea sobe protección de datos personales". trad. de Santiago Ripoll Carulla, en Informática y Derecho, N° 6/7, Mérida, España: UNED - Centro Regional de Extremadura, 1994.

- Dubié, Pedro “El hábeas data financiero”. LA LEY 2002-B, 1009.
- Dubié, Pedro “Uso por terceros de información de acceso público irrestricto - Quid del consentimiento previo de la persona”, LA LEY 1999-F, 919.
- Dubié, Pedro, “Análisis del debate parlamentario del hábeas data con relación a la información crediticia”, JA 1999-II-882.
- Duprat, Diego A., “Los datos sensibles y el hábeas data (Hábeas data y derecho a la intimidad)”, JA 1998-I-774.
- Egües, Alberto J., ”El "right to privacy" y el "habeas data" comercial”, LA LEY 2000-C, 1272.
- Eguiguren P., Francisco J, “Poder judicial, Tribunal constitucional y Habeas data en el constitucionalismo peruano”, Centro de Estudios Constitucionales México-Centroamérica, Instituto de Investigaciones jurídicas UNAM, México, 1999.
- Ekmekdjian, Miguel Ángel “El hábeas data en la reforma constitucional”, LA LEY 1995-E, 946.
- Espinoza Espinoza, Juan, “Derecho de la responsabilidad civil”, Gaceta jurídica, Lima, Peru, 2006.
- Estadella Yuste, Olga, "La protección de la intimidad frente a la transmisión internacional de datos personales", Ed. Tecnos, Centre d’Investigació de la Comunicació, Generalitat de Catalunya, Barcelona, 1995.

F.A.C.A., XIV Conferencia Nacional de Abogados, Santa Fé, Paraná, octubre 2003.

- Falcón, Enrique M, "Hábeas Data, concepto y procedimiento", Abeledo Perrot, Bs. As., 1996.
- Falcon, Enrique, “Tratado de la prueba. Civil, comercial, laboral, penal, administrativa”, Ed. Astrea, Buenos Aires, 2003.

- Farina, Juan M., “Defensa del consumidor y del usuario. Comentario exegético de la ley 24.240 con las reformas de la ley 26.361”, Ed. Astrea, Buenos Aires, 2008.
- Fenoll-Trousseau, Marie-Pierre y Haas, Gerard, “Internet et protection des dones personelles”, Litec, Paris, Francia, 2000.
- Fernández Hierro, José Manuel, “Responsabilidad civil judicial”, Ed. Aranzadi, Pamplona, 1987, 18-23 y 32-35

Fernández Sessarego, Carlos, "El Derecho a la Identidad Personal y otras figuras", Ed. Astrea, Buenos Aires, 1992,
Ferreyra Rubio, Delia Matilde, “El Derecho a La Intimidad:
Análisis del artículo 1071 bis del Código Civil a la luz de la doctrina, la legislación comparada y la jurisprudencia”, Editorial Universidad, Buenos Aires, 1982.

- Flores, Oscar, “La Corte Suprema Norteamericana y una sentencia que, acotando el poder de los Estados, afianza el derecho a la privacidad”, LA LEY 2000-D, 403.
- Frosini, Vittorio, “Informatica, diritto e societa”, Giuffre, Milán, 1977.
- Frosini, Vittorio, su ponencia: "La organización informática del Estado y la libertad del ciudadano", al IV Congreso Iberoamericano de Informática y Derecho en pos de la integración, Bariloche, mayo 1994.
- Frossini, Vittorio, "Informática y Derecho", Ed.Themis, Bogotá, Colombia, 1988.
- Gallardo, María Cecilia Soria Olmedo, Karina Flori, José Luis, “Habeas data”, LA LEY 1998-A, 977.
- Gallardo, Roberto Andrés López (h.), Mario Justo “¿Existe la acción de "Habeas data" en la República Argentina?”, LA LEY 1998-C, 232.
- Gallo, Paolo, “Pene private e responsabilita civile”, Ed. Dott.A. Giuffre, Milán, 1996.

García González, Aristeo, “La protección de datos personales. Derecho fundamental del Siglo XXI. Un estudio comparado”, Revista Derecho Informático – Alfa Redi Nº 100, noviembre 2006.

- García Pita y Lastres, José Luis, “Las entidades de crédito y sus operaciones”, en “Tratado de derecho mercantil”, Olivencia, Manuel; Fernández Novoa, Carlos y Jiménez de Parga (dir.) Jiménez Sanchez (Coord), Marcial Pons, Madrid, 2006.
- Garriga Domínguez, Ana, “La protección de los datos personales en el derecho español”, Dykinson, Madrid, 1999.
- Gesualdi, Dora M., “Responsabilidad civil. Factores objetivos de atribución. Relacion de causalidad”, Ed. Hammurabi, José Luis Depalma, Buenos Aires, 2000.
- Ghersi, Carlos; Weingarten, Celia, “Historia clínica”, Ed. Nova tesis, Santa Fe, 2005.
- Gil Domínguez, Andrés, “La verdad: Un derecho emergente”, LA LEY 1999-A, 219.
- Gils Carbo, Alejandra M., “Régimen Legal de las Bases de Datos y Hábeas Data”, Editorial La Ley, Buenos Aires 2001.

Goldenberg, Isidoro H, “La tutela de la vida privada”, LA LEY 1976-A,576.

- González, Joaquín V., “Manual de la Constitución Argentina”, Ed. Angel Estrada y Cia, Buenos Aires, 25ª ed., 1897.
- Gordillo, Agustín, “Habeas data”, LA LEY, 1998-C, 372.
- Gordillo, Agustín, “Los ápices frustratorios de las garantías constitucionales de una sociedad democrática”, LA LEY 1998-B, 537.
- Gozaíni, Osvaldo Alfredo, “El consentimiento para el uso de los datos personales”, LA LEY 2001-C, 781.
- Gozaíni, Osvaldo Alfredo, “El particular, el Estado y las empresas de venta de información crediticia frente al hábeas data”, LA LEY 2000-D, 1290.
- Gozaíni, Osvaldo Alfredo, “La afiliación partidaria como dato sensible que se puede difundir”, LA LEY 2002-F, 1437.
- Gozaíni, Osvaldo Alfredo, “Ley 25.326 de protección de datos personales”, LA LEY 2003-C, 1139.
- Grimalt Severa, Pedro, “La responsabilidad civil en el tratamiento automatizado de datos personales”, Ed. Comares, Granada, 1999.

Guahnon, Silvia y Somer, Marcela, “Hábeas data: procedimiento aplicable. ¿Derecho a una tutela efectiva y temprana versus Derecho de defensa en juicio?”, Revista de Derecho Procesal Nº 5, Rubinzal Culzoni, 2000, p.199

Guastavino, Elías, “Irregular tramitación de la ley de la intimidad”, LA LEY 1975- A-1270.

Guerrero Picó, María del Carmen, “El derecho fundamental a la protección de datos personales en la Constitución Europea”, Revista de Derecho Constitucional Europeo (REDCE), Universidad de Granada http://www.ugr.es/~redce/

Hassemer, Winfred y Sánchez, Alfredo Chirino, “El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales”, Editores del Puerto, Buenos Aires, 1997, p. 172

Hassemer, Winfried, Theorie und Soziologie des Verbrechens, Frankfurt a. M., 1973.

Heredero Higueras, “La Directiva comunitaria de protección de los datos de carácter personal”, Aranzadi, Pamplona, 1997.

- Herran Ortiz, Ana Isabel, “La violación de la intimidad en la Protección de Datos Personales”, Dykinson, Madrid, 1998.

Hondius, Frits W., “A decade of international data protection”, “Netherlands of International Law Review”, vol. 30, n° 2, 1983.

- Itzcovich Griot, Alejandro, "Hábeas data. Un gran paso y una tarea pendiente", LA LEY Actualidad, 27-10-1994.

Kemelmajer de Carlucci, Aída R. en Belluscio, Augusto C. (Director) – Zannoni, Eduardo A. (Coordinador), “Código Civil y leyes complementarias. Comentado, anotado y concordado”, tomo 5, Editorial Astrea, Buenos Aires, 1994.

- Kemelmajer de Carlucci, Aida, “¿Conviene la introducción de los llamados “daños punitivos” en el derecho argentino?”, Academia Nacional de Derecho y Ciencias Sociales de Buenos Aires, separata anticipo de Anales, año XXXVIII, No. 31, 1993,
- Kiper, Claudio M., “Proceso de daños”, t.II, Ed. La Ley, Buenos Aires, 2008.

Knavs, Verónica; Herrán, Maite, “La responsabilidad bancaria por error de información.

Alcances de la reparación", LA LEY2007-A, 455.
Kommers, Donald, The Constitutional Jurisprudence of the Federal Republic of Germany, Durham, Londres, 1989, pág. 332.
Lasson, Nelson B., "The History and Development of the Fourth Amendment to the United States Constitution", Baltimore; John Hopkins University Press, 1937.
Leonfanti, María Antonia, " El derecho a la intimidad en la Argentina ", LA LEY, 1975-B-1319.
Levy, Leonard W., "Origins of the Fourth Amendment"; Political Science Quarterly, Vol. 114, N° 1, p. 84, Academy of Political Science, New York, 1999, citado por Egües.

- Livellara, Silvina, "Habeas data e información crediticia. La eventual responsabilidad civil de las entidades financieras y del banco central de la república argentina por cesión y publicidad de datos inexactos", El Dial DC2A7.

Llambías, Joaquín, "Código Civil Anotado", t. II-B, ed. 1992.
Lobato de Paiva, Mario Antônio, "Responsabilidad civil del Estado por daños provenientes de la circulación de datos en los sitios de Internet de los tribunales"("A difusão de informações judiciais na Internet e seus efeitos na esfera trabalhista") http://jus2.uol.com.br/doutrina/texto.asp?id=4672

- Lopes Meirelles, Hely,"Mandado de seguranca", Ed.Malheiros, San Pablo, Brasil, 1996, 17ª. Edición actualizada por Wald, Arnoldo.
- López Herrera, Edgardo, "Los daños punitivos", Abeledo Perrot, Buenos Aires, 2008.
- López Herrera, Edgardo, "Teoría general de la responsabilidad civil", Lexis Nexis Argentina, Buenos Aires, 2006.
- Manes, Paola, "Il consenso al trattamento dei dati personali", CEDAM, Modena-Pavia, 2001.
- Martorello, Beatriz; Guahnon, Silvia, "Cuestiones procesales para la interposición del hábeas data", LA LEY 1999-B, 586.

Masciotra, Mario, "El hábeas data. La garantía polifuncional", Librería Editora Platense, La Plata, Argentina, 2003.

- Meoro, Mario Clemente y Cavanillas Mugica, Santiago, "Responsabilidad civil y contratos en Internet", Ed. Comares, Granada, 2003.
- Michaud, Martin, "Le droit au respect de la vie privee dans le conterxte mediatique: de Warren et Brandeis a l´informatique", Ed. Wilson & Laffleur Itee, Montreal, 1996.

Molina Quiroga Eduardo "El tratamiento de los datos judiciales y los informes crediticios", http://www.cpacf.org.ar/
Molina Quiroga, Eduardo, "Los datos de salud en la ley 25.326 de Protección de Datos Personales". LexisNexis 0003/010495 ó 0003010502 –JA 2004-II-1395.
Molina Quiroga, Eduardo, "Protección de datos personales como derecho autónomo: principios rectores. Informes de solvencia crediticia: uso arbitrario. Daño moral y material", http://www.eldial.com, 7, 8 y 9/5/2003.
Molina Quiroga, Eduardo, "Prestigio e imagen del comerciante. Protección de datos personales", en Código de Comercio y normas complementarias. Análisis doctrinario y jurisprudencial, Director Raúl A. Etcheverry, Coordinación: Héctor O. Chomer, Editorial Hammurabi de José Luis de Palma, Buenos Aires, 2005.

- Morello, Augusto M. "Los contenidos de la pretensión procesal penal y de la

garantía de "hábeas data", LA LEY 1998-F, 365.
- Mosset Iturraspe, Jorge (Dir.); Kemelmajer de Carlucci, Aida (Coord.); Ghersi, Carlos A.; Stiglitz, Gabriel, Parellada, Carlos, “Responsabilidad civil”, Ed. Hammurabi- José Luis Depalma, Buenos Aires, 1992.
- Mosset Iturraspe, Jorge, “Estudios sobre responsabilidad por daños”, Tomo I, Ed. Rubinzal Culzoni, Santa Fe, 1980.
- Mosset Iturraspe, Jorge; Wajntraub, Javier H., “Ley de defensa del consumidor. Ley 24.240”, Ed. Rubinzal Culzoni, Santa Fe, 2008.

Muñoz Machado, Santiago, "La regulación de la red. Poder y Derecho en Internet", Taurus. Madrid, 2000.

- Murillo de la Cueva, Pablo Lucas, “La protección de datos en la administración de justicia”, en “Derecho a la intimidad y nuevas tecnologías”, Cuadernos de Derecho Judicial, IX -2004, Consejo General del Poder Judicial, Escuela Judicial, España, Madrid, 2004.

Murillo de la Cueva, Pablo, “El derecho a la autodeterminación informativa: la protección de los datos personales frente al uso de la informática”, Tecnos, Madrid, 1990.
Muruzábal, Claudio, “Más allá del hábeas data, la otra cara de la privacidad”, Infobae, 28/11/2003.

- Niger, Sergio, “Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali”, Cedam, Padova, Italia, 2006.

Nino, Carlos S., “Fundamentos de Derecho Constitucional”, Ed. Astrea, Buenos Aires, 1992.

- Nota de Redacción “Las costas en el Habeas data”, LA LEY 2001-B, 625.

Novoa Monreal, Eduardo, "Derecho a la vida privada y libertad de información", Editorial Siglo XXI.

- Padilla, Miguel M., “La directiva 95/46/CE de la Unión Europea”, LA LEY 1999-B, 970.
- Palazzi, Pablo “El hábeas data y el "derecho al olvido", JA 1997-I-33.
- Palazzi, Pablo “El hábeas data y el consentimiento para el tratamiento de datos personales”, JA 1999-IV-399.

Palazzi, Pablo A, “Informes comerciales”, Ed. Astrea, Buenos Aires, 2007.

- Palazzi, Pablo A., “El derecho del titular de información personal a aclarar un dato controvertido por la vía del hábeas data”, LA LEY, 2007-C, 129.

Palazzi, Pablo A., “El Habeas data en el derecho argentino”, Revista Electrónica Internacional Venezolana de Derecho e Informática-REIVDI Nº 1, enero-abril 1999 http://www.omdi.et/
Palazzi, Pablo A.,”Habeas data y protección de datos en Latinoamérica” http://comunidad.derecho.org/

- Palazzi, Pedro “El hábeas data en la Constitución Nacional (La protección de la privacidad en la era de la información)”, JA 1995-IV-710.
- Pascuzzi, Giovanni, “Il diritto dell´era digitale, Il Mulino, Bologna, 2002.
- Pérez Asinari, María Verónica “Notas sobre la Conferencia de protección de datos personales organizada por la Comisión Europea”, LA LEY Actualidad, 18/03/2003.

Pérez Bustamente, Laura, “El derecho de acceso al consumo como derecho subjetivo”, http://www.astrea.com.ar/
Pérez Luño, Antonio Enrique, “Intimidad y protección de datos personales: del hábeas corpus al hábeas data”, en García San Miguel, Luis (comp.) Estudios sobre el derecho a la intimidad, Madrid, 1992.
Pérez Luño, Antonio Enrique, “La Tercera Generación de los Derechos Humanos”, Thomson-Aranzadi, Madrid, 2006.
Pérez Luño, Antonio Enrique, “Nuevas Tecnologías, Sociedad y Derecho: El Impacto Socio-jurídico de la Nueva Tecnología de la Información”, Fundesco Madrid, 1987.

- Peyrano, Guillermo F, “El principio del consentimiento en el “sistema de protección de los datos personales. Las condiciones de su validez y la posibilidad de revocación del consentimiento prestado”, ponencia presentada en la XIV Conferencia Nacional de Abogados (F.A.C.A.) Santa Fe-Paraná, 2004.

Peyrano, Guillermo F., "Bancos de datos y tratamiento de datos personales: análisis de algunas problemáticas fundamentales", JA 18/4/2001, p. 6
Peyrano, Guillermo F., "Bancos de datos" y tratamiento de datos personales. Análisis de algunas problemáticas fundamentales (Parangón de las previsiones de la ley argentina 25.326 con las disposiciones de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal” española y con la ley Nro.19.628 sobre "Protección de datos de carácter personal" de la República de Chile)”, http://www.derecho.org/

- Peyrano, Guillermo F., "Datos sensibles: perfiles y regulaciones. El impacto del desarrollo tecnológico", ED, boletín Nº 10.651 del 13/12/2002.
- Peyrano, Guillermo F., "El principio del consentimiento en el sistema de protección de datos personales. Condiciones de validez y posibilidad de revocación del consentimiento prestado. El derecho de oposición", Zeus, t. 92, 7216, 7217, http://www.editorial-zeus.com.ar/

Peyrano, Guillermo F., “Los datos a afectarse, su falsedad y exactitud, la legitimación pasiva y los alcances de la sentencia, en la acción de protección de datos de carácter personal. las connotaciones de un fallo ante las problemáticas que plantea la acción de “hábeas data”, Lexis Nexis 04/09/2002, JA 2002.III, fascículo n. 10.
Peyrano, Guillermo F., “Nuevas problemáticas del tratamiento de datos personales. El tratamiento de informaciones que proporcionan datos personales por parte de medios periodísticos a través de Internet”, JA 7-04-2004, Lexis Nº 0003/010468.

- Peyrano, Guillermo F., “Reflexiones sobre la responsabilidad civil por los daños ocasionados por el tratamiento de datos de carácter personal”, JA 2004-II-1428.
- Picasso, Sebastián y Wajntraub, Javier H., “La protección de los datos personales en un acertado decisorio”, Semanario Jurídico 1999-11-179.

- Picasso, Sebastián, “El Banco Central y la imposición de costas en la acción de hábeas data”, LA LEY 2002-D, 261.
- Picasso, Sebastián, “El hábeas data en la Ciudad de Buenos Aires”, LA LEY, 2003-A, 1253.
- Pizarro, Daniel Ramón, “Responsabilidad civil por riesgo creado y de empresa, Contractual y extracontractual”, Parte especial, tomo II, Ed. La Ley, Buenos Aires, 2006, 159-181
- Pizarro, Ramon Daniel, “Daño moral. Prevencion. Reparacion. Punicion”, Ed. Hammurabi de José Luis Depalma, Buenos Aires, 2004.
- Proal, Frederic, “La responsabilice du fournisseur d´informtion en reseau”, Presse universitaires d´Aix Marseille, Faculté de Droit et de Science Politique, Aix en Provence, CEDEX, 1997.

Proser y Keeton, "The Law of Torts"; p. 849, 5ª edición, West Publishing, St. Paul, USA, 1984, citados por Egües.
Puccinelli, “El hábeas data en Iberoamérica”, Temis, Bogotá, Colombia,1999.
Puccinelli, Oscar Raúl, “Protección de datos de carácter personal”, Ed. Astrea, Buenos Aires, 2004.

- Puccinelli, Oscar Raúl, “Tipos y subtipos de Habeas data en el derecho constitucional latinoamericano - A propósito del Habeas data peruano para acceder a información pública”, LA LEY 1997-D, 215.

Puccinelli, Oscar, “El habeas data en Brasil”, http://www.astrea.com.ar/
Puente de la Mora, Ximena, “Privacidad de la información personal y su protección legal en Estados Unidos”, Revista Derecho Informático – Alfa Redi Nº 097, agosto 2006.

- Quispe Merovich, Carina, “El hábeas data y los sistemas de información (Reflexiones acerca de la nueva garantía constitucional)”, LA LEY 1996-A, 1056.

Ramella, Pablo, "El Derecho a la Intimidad", LA LEY 140-1175.

- Rapetto, Umberto, “La tutela dei dati personali”, EPC, Roma, 1997.

Reyes Krafft, Alfredo Alejandro, “Protección de datos personales en México. Génesis legislativa”, Revista Derecho Informático - Alfa Redi Nº 100 noviembre 2006.
Rezzónico, Juan Carlos "Principios Fundamentales de los Contratos", Astrea, Buenos Aires, 1999.
Riande Juárez, Noé Adolfo, “La desprotección de los Datos Personales”, Centro de Información Documental del Ministerio de Economía, Argentina, Infoleg/ Derecho y Nuevas Tecnologías.

- Rigaux, François, “Libre circulation des données et protection de la vie privée dans l’espace européen”, separata de “Festchrift für Ulrich Drobnig”
- Ripoll Carulla (ed.), Bacaria Martrus, Jordi (coord.) “Estudios de protección de datos de carácter personal en el ámbito de la salud, Agencia de Protección de datos Personales de Cataluña, Ed. Marcial Pons, Madrid, 2006.
- Rivas, Adolfo A., "El amparo y la nueva Constitución de la República Argentina", LA LEY 1994-E, 1330.

Rivera, Julio César, "Derecho Civil, Parte General, Temas". Ed. Abeledo Perrot, Buenos Aires, 1987.
Rivera, Julio César, "Instituciones de Derecho Civil", t. II.
Rivera, Julio César, “Derecho a la intimidad”, LA LEY 1980-D,912.
Rivera, Julio César, Belluscio-Zannoni, en Belluscio, Augusto C. (Director) – Zannoni, Eduardo A. (Coordinador), “Código Civil y leyes complementarias. Comentado, anotado y concordado”, tomo 5, Ed. Astrea, Buenos Aires, 1994.

- Rocha Campos, Adolfo “Acción de amparo y Habeas data”, LLLitoral, 1998-2-507.
- Rocha Campos, Adolfo, “Actualidad en la jurisprudencia sobre habeas data”, LA LEY 2000-F, 1174.
- Rossi, Jorge Oscar, “Para la tutela efectiva para las victimas de pequeños daños”, Foro de Córdoba Nº 117, Año XIX, octubre 2007.
- Rovira Suerio, Maria E., “La responsabilidad civil derivada de los daños ocasionados al derecho al honora, a la intimidad personal y familiar y a la propia imagen”, Ed. Cedecs, Barcelona, 1999.
- Rufino, Marco, “Reseña sobre Habeas Data”, JA 1996-III-1102.

Ruiz, Miguel, “El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico”, RDCE , Nº 14, Enero-Abril 2003.
Sagües, Néstor P, "El hábeas data contra organismos estatales de seguridad”, LA LEY, 2000-A, 352.
Sancho Villa, Diana, “La Ley uruguaya de protección de datos personales de 24 septiembre 2004 (1ª parte): ámbito de aplicación y principios de protección”, Revista de la Agencia de Protección de Datos de la Comunidad Autónoma de Madrid, noviembre 2004, http://www.datospersonales.org/
Schvartz, Liliana , “Algunos fallos orientadores en materia de responsabilidad civil de las empresas dedicadas a la difusión de datos crediticios”, http://www.elDial.com (08-03-2005).
Schvartz, Liliana, LOS INFORMES COMERCIALES. Régimen jurídico. Argentina, Perú, México, Brasil, Chile, Paraguay, Colombia, Ed. Lumiere, Buenos Aires, 2003.
Shapiro, Andrew, "The control revolution" (1999)."El mundo en un clic", trad. Francisco Ramos, Grijalbo. Barcelona, 2001.

- Slaibe, María Eugenia Gabot, Claudio, “La reciente reglamentación de la ley de Habeas Data”, ADLA 2002-A, 1583.
- Slaibe, María Eugenia y Gabot, Claudio, “El hábeas data y los informes comerciales: el quid de la confidencialidad y el consentimiento”, LLC 2000, 1423.
- Slaibe, María Eugenia y Gabot, Claudio, “Hábeas data: su alcance en la legislación comparada y en nuestra jurisprudencia”, LA LEY 2000-B, 27.
- Slaibe, María Eugenia y Gabot, Claudio, “La discriminación en los informes comerciales frente a la nueva regulación del "habeas data", LA LEY 2001-B, 790.
- Slaibe, María Eugenia y Gabot, Claudio, “Una nueva restricción a la garantía constitucional del habeas data. Entrecruzamiento de datos en un informe de riesgo crediticio”, LA LEY 2001-C, 661.
- Steizel, Sergio, “Habeas data: los nuevos tipos penales en la ley 25.326”, LA LEY 2001-F, 1295.

Stiglitz, Rosana M , "Impacto de la Informática en la sociedad" (Protección de datos personales. Derecho a la intimidad)", LA LEY 1987-E-859.
Tanús, Daniel Gustavo, "La protección de los datos personales de salud y la ley 25.326", Revista Derecho y Nuevas Tecnologías, Nº 4-5, Editorial Ad-Hoc, Buenos Aires, 2003.

- Tellez Aguilera, Abel, "Nuevas tecnologias. Intimidad y Proteccion de datos, Edisofer, Madrid, 2001.
- Tobías, José W., "Derecho de las personas", Ed. La Ley, Buenos Aires, 2009.

Uicich, Rodolfo Daniel, en "Los bancos de datos y el Derecho a la intimidad", Editorial Ad Hoc, Buenos Aires, 1999.

- Ull Pont, Eugenio, "Derecho público de la Informática (Protección de datos de carácter personal)", UNED, Madrid, 2000.
- Urioste, Mercedes de, "Protección de datos personales", Investigaciones 1, Subsecretaría de investigación en derecho comparado de la CSJN. Buenos Aires, 1998.

V Congreso Iberoamericano de Informática y Derecho, La Habana, Cuba, 1996.

- Vanossi, Jorge R., "El hábeas data: no puede ni debe contraponerse a la libertad de los medios de prensa", ED, 159-948.

Vázquez Ferreyra, Roberto, "El derecho a la intimidad, al honor y a la propia imagen (Con especial referencia a la legislación española y a propósito de un fallo del Tribunal Supremo Español)", J.A, 1989, agosto 2 Nº 563.

- Velazquez Bautista, Rafael, "Protección jurídica de datos personales automatizados", Ed. Colex, Madrid, 1993.

Warren, Samuel y Brandeis, Louis, "El derecho a la intimidad", Civitas, Madrid, 1995.

- Wetzler Malbrán, Germán, "Algunos aspectos de la información crediticia" LA LEY 2002-F, 1368.

Wierzba, Sandra M., "Protección de Datos de Salud en Procesos Judiciales. Transparencia judicial y confidencialidad de datos de litigantes con VIH-SIDA:¿existe oposición entre tales principios?"

- Zannoni, Eduardo A., "El daño en la responsabilidad civil", Ed. Astrea, Buenos Aires, 2005 (3ª.edic.).

Sitios visitados en Internet:

http:// www.uc3m.es/
http://200.91.68.20/scij/busqueda/jurisprudencia/jur_repartidor.asp
http://abiweb.obh.hu/
http://asamblea.racsa.co.cr/
http://basedoc.superservicios.gov.co/

http://curia.europa.eu/
http://eur-lex.europa.es
http://europa.eu.int/
http://gecti.uniandes.edu.co/
http://infoleg.mecon.gov.ar/
http://informatica-juridica.com/
http://lac.derechos.apc.org/
http://laws.justice.gc.ca/
http://pdba.georgetown.edu/Constitutions/
http://sip.parlamento.gub.uy/leyes/
http://www.actualicese.com/
http://www.adc.org.ar/
http://www.agpd.es/
http://www.anfitrion.cl/actualidad/
http://www.apec.org/
http://www.argentina.gov.ar/argentina/portal/
http://www.asamblea.gob.pa/
http://www.assembleiadarepublica.pt/
http://www.bcra.gov.ar/
http://www.bibliojuridica.org/
http://www.boe.es/
http://www.cajpe.org.pe/
http://www.camdipsalta.gov.ar/
http://www.canlii.org/
http://www.cervantesvirtual.com/
http://www.cidh.oas.org/
http://www.cnil.fr/
http://www.cnpd.pt/
http://www.congreso.gob.pe/
http://www.constitucion.es/
http://www.constitucional.gov.co/corte/
http://www.constitution.org/
http://www.corpece.org.ec/
http://www.corteconstitucional.gov.co/
http://www.cpdp.bg/
http://www.cpsr-peru.org/bdatos/
http://www.dataprotection.gov.cy/
http://www.dataprotection.gov.gg/
http://www.dataprotection.ie/
http://www.datatilsynet.dk/
http://www.defensoria.gob.sv/
http://www.diputados.gob.mx/
http://www.diputados-catamarca.gov.ar/
http://www.diputadosmisiones.gov.ar/
http://www.diputadossanluis.gov.ar/
[1]http://www.dpa.gr/
http://www.embajada-ungria.org/
http://www.epic.org/privacy/
http://www.europarl.europa.eu/
http://www.export.gov/safeharbor/
http://www.ftc.gov/credit/
http://www.ftc.gov/privacy/
http://www.fuhem.es/

http://www.garanteprivacy.it/garante/
http://www.giodo.gov.pl/
http://www.gob.gba.gov.ar/
http://www.habeasdata.org/
http://www.hcdsc.gov.ar/
http://www.ifai.org.mx/
http://www.iijusticia.edu.ar/Reglas_de_Heredia.htm
http://www.informatica-juridica.com/
http://www.interamericanusa.com/
http://www.jujuy.gov.ar/
http://www.juridicas.unam.mx/
http://www.jus.gov.ar/dnpdpnew/
http://www.justiniano.com/
http://www.lapampa.gov.ar/
http://www.larioja.gov.ar/
http://www.legifrance.gouv.fr/
http://www.legilux.public.lu/
http://www.legislatura.gov.ar/
http://www.legislaturaformosa.gov.ar/
http://www.legisrn.gov.ar/
http://www.legistdf.gov.ar/
http://www.legsanjuan.gov.ar/
http://www.lexum.umontreal.ca/
http://www.leyes.com.py/
http://www.mipunto.com/
http://www.misiones.gov.ar/
http://www.neuquen.gov.ar/
http://www.oas.org/juridico/
http://www.oecd.org
http://www.oefre.unibe.ch/
http://www.opsi.gov.uk/
http://www.parlamento.gub.uy/
http://www.parlamento.pt/
http://www.personuvernd.is/
http://www.pgr.go.cr/
http://www.poderjudicial.gub.uy/
http://www.privacy.ca.gov/
http://www.privacy.gov.au/
http://www.privacycommission.be/
http://www.privcom.gc.ca/
http://www.procon.sc.gov.br/
http://www.profesorgentile.com.ar/
http://www.registrocivil.cl/
http://www.santa-fe.gov.ar/
http://www.senado.gov.br/
http://www.senadoctes.gov.ar/
http://www.superfinanciera.gov.co/
http://www.sup-trib-delsur.gov.ar/
http://www.tietosuoja.fi/
http://www.tribunalconstitucional.es/
http://www.tribunet.com.ar/
http://www.tsj.gov.ve/
http://www.tucuman.gov.ar/

http://www.uaipit.com/
http://www.uc3m.es/
http://www.ulpiano.com/
http://www.un.org/
http://www.unhchr.ch/
http://www.usdoj.gov/
http://www4.law.cornell.edu/
https://www.agpd.es/
https://www.planalto.gov.br/
https://www.registrocivil.cl/

Fallos citados

- C1aCont. Adm. Córdoba, 29-03-1995, Flores, Marcela A. c. Provincia de Córdoba", LLC 1996, 316.

C1aCont. Adm., Córdoba, 29-03-1995, "García de Llanos, Isabel c. Caja de Jubilaciones Pensiones y Retiros de Córdoba", LLC, 1995-948.
C7ªCIV. y Com. Córdoba, 1999/10/27, "Delgado, Néstor R. y otros c. Seven S.R.L.", LA LEY 1999-F,755 y LLC 1999, 1041.
CCiv. y Com. La Matanza, sala I, 2001/07/05, "Bressan, Walter Darío c/Banco Galicia y Bs.As. s/daños y perjuicios (ordinario)", elDial AAC6E.
CCiv. y Com. Mar del Plata, sala 2, 2002/04/09, "Toyas Pittelli, Omar E. y otros y. Citibank N.A. s/habeas data", JA 2002-III, fascículo nº 10.
CCiv. y Com. San Isidro, sala I, 21/06/1996, "Depaolini, Angela M. c. Organización Veraz", LLBA 1996, 1082.
CFed. Bahía Blanca, sala I, 30-12-1994, "Gutiérrez, Héctor R. c. Casino Militar del Personal Superior de la Base Naval Puerto Belgrano", LA LEY, 1996-A, 314.
CNACAF, sala I, 1997/04/29, "Díaz Cisneros, Adriano c. B.C.R.A. y otro", LA LEY 1998-C, 373.
CNACAF, sala I, 1999/04/21, "Finoli, Leonardo Luis c/ B.C.R.A. y otro s/ Habeas Data", SAIJ sumarios N° K0019989 Y K0019990.
CNACAF, sala III, 1999/12/22, "M., M. c. Fidelitas S. A. y otros", LA LEY 2001-B, 791.
CNACAF, sala IV, 05-09-1995, "Farrel, Desmond A. v. B.C.R.A. y otros", JA 1995-IV-350.
CNACAF, sala IV; 17-05-2001, "B., G. O. y otro c. M.I", LA LEY, 2001-D, 812
CNACCF, sala I, 2003/03/04, "Gutiérrez, Norma S. c. B.C.R.A. y otro", LA LEY 2003-F, 48.
CNCiv, sala A, 08-09-1997 "Pochini, Oscar de Jesús y otro c/Organización Veraz SA s/habeas data" LA LEY 1988-B, 3.
CNCiv, sala A, 2001/11/16, "Arroyo, Jorge H. c. Citibank y otro", LA LEY 2002-B, 314; LA LEY 2002-D, 262 Y DJ 2002-1, 323.
CNCiv, sala A, 2005/05/11, "Maderas y Servicios S.A. y otro c/ Bankboston N.A. y otro s/ daños y perjuicios", elDial - AA2AA9
CNCiv, sala B, 07/04/2009, "Sanchez, Miguel A. c/ Banco de Galicia y Buenos Aires y otros », elDial AA52FD

- CNCiv, Sala C, 03/06/2004, "D., C, A. c. Lloyds Bank TSB Bank", LA LEY 19/10/2004, 5.

CNCiv, sala C, 2002/06/13, "Saal, Alfredo R. c. Organización Veraz S.A.", LA LEY 2002-F, 335 y DJ 2002-3, 1089.
CNCiv, sala D, 2007/09/12, "Quintana America Iberia c/ Organizacion Veraz S.A. s/ daños y perjuicios", Microjuris: MJJ16317.
CNCiv, sala D, 23/02/1999, "Lascano Quintana, Guillermo V. c. Veraz S.A.", LA LEY 1999-E, 152; LA LEY 2000-B, 679; RCyS 1999, 792 y DJ 1999-3, 760.

CNCiv, sala E, 2006/10/19, "A., S c/Banco Lloyds S.A. y otro s/daños y perjuicios", elDial AA3A58.
CNCiv, sala F, 06-07-1995, “B. de S., D. A. c. Sanatorio Greyton S. A.”, LA LEY, 1996-C, 473, y ED 165-257.
CNCiv, sala F, 2002/02/06, "Ravina Arturo Octavio c/ Organización Veraz SA s/ daños y perjuicios -sumario-", LA LEY 2002-C, 74 - DJ 2002-2, 41 - ED 197, 267.
CNCiv, sala F, 2003/11/06, “Fallone, Eugenio Donato c/ HSBC Banco Roberts SA s/ daños y perjuicios”, elDial AA1DD0; Diario judicial.com 20/01/2004.
CNCiv, sala F, 2005/07/08, “S., J. C. c/ Banco Itaú Buen Ayre SA s/ daños y perjuicios” , elDial AA2CBC.
CNCiv, sala H, 04/09/2002, “Sosa Marcelo c/Citibank S.A. s/Daños y perjuicios", elDial AA135C.
CNCiv, sala H, 25/09/1995, “Rossetti Serra, Salvador v. Dun & Brandstreet S.R.L”, JA 1995-IV-355.
CNCiv, sala I, 10/1172000, “R. A. c. Empresa Organización Veraz”, LA LEY 2001-B, 625 y DJ 2001-2,487.

- CNCiv, sala K, 08/10/2003, “Botta, Rodolfo E. c. Citibank N.A. y otros”, LA LEY 08/01/2004, 3.

CNCiv, sala K, 1997/08/14, "Locato, Omar N. c. Organización Veraz S.A.C.M.E.I. s/hábeas data", LA LEY, 1999-B, 852
CNCiv, sala K, 22-10-2002, “Gutiérrez, Vicente Juan Carlos Demetrio c/ Banco de la Provincia de Buenos Aires y otro s/daños y perjuicios”, elDial - AA1580, LA LEY 2002-F, 781, DJ 2002-3, 883.
CNCiv, sala L, 2006/03/31, "Rodríguez, Pedro Ruben c/Ford Credit Compañía Financiera S.A., s/daños y perjuicios", elDial - AA334B.
CNCiv, Sala L, 2006/05/08, “Bousquet, Ricardo H. c. Organización Veraz S.A. y otros”, La Ley Online.
CNCiv, sala M, 2002/02/25, “A., M. del C. c. Veraz S.A”, LA LEY 2002-D, 177 y DJ 2002-2, 422.
CNCiv, sala: L, 2007/11/01, “Galarza Valeria Romina c/ Banco Credicoop Cooperativo Limitado s/ daños y perjuicios – ordinario”, Microjuris MJJ16858.

- CNCiv., sala A, 08-09-1997, “Pochini, Oscar y otro c. Organización Veraz S. A., LA LEY, 1998-B, 3.
- CNCom, sala A, 10-09-1997, “Munditol S.A. y otros c. Allianz Ras Argentina Sociedad de Seguros”, LA LEY 1999-D, 744 - DJ 1999-3, 938.

CNCom, sala A, 2003/04/11, "Romo Armando c/Banco Río de la Plata SA s/Daños y perjuicios", elDial AA17C8.
CNCom, sala A, 2003/04/11, "Solares Adrián Daniel c/Bansud SA s/sumario", elDial AA17EB
CNCom, sala A, 2006/06/08, “Canillas, Gustavo F. c. Citibank NA y otro”, LA LEY 2006-F,828.
CNCom, sala B, 1999/09/20, "Banesto Banco Shaw SA c/ Dominutti, Cristina", JA 2000-IV-811.
CNCom, sala B, 1999/11/24, "Molinari, Antonio F. C/ Tarraubella Compañía Financiera SA", Doctrina Societaria, ed. Errepar, tº XI, pag. 905, JA, revista n° 6235 del 28-2-2001.
CNCom, sala B, 2000/11/01,"Del Giovannino, Luis Gerardo c. Banco del Buen Ayre s/ordinario", LA LEY 2000-F, 657; DJ 2001-1, 337; ED 190, 287; elDial AA7EC.
CNCom, sala B, 2002/12/30, "Domínguez Alvaro Eloy c/Banco Río de La Plata SA s/ordinario", elDial - AA14F3.
CNCom, sala B, 2003/02/14, "Buschiazzo, Juan A. y otro c/Banco Bansud SA y otro s/ordinario”, elDial - AA166D.

CNCom, sala B, 2003/04/01, "Cova Rodolfo José c/Banco Caja de Ahorro S.A. s/ ordinario", elDial - AA17C0.
CNCom, sala B, 2003/04/11 "Litvak, Adolfo y otro c/ Bansud S.A. y otro s/ Sumario", elDial AA17DD.
CNCom, sala B, 2003/06/30, "Treviño Oscar c/Banco de Galicia y Buenos Aires SA s/ ordinario", elDial - AA1971.
CNCom, sala B, 2003/09/09, “Rivera, Raul Enrique c/Banco Frances del Río de La Plata SA s/ordinario" elDial AA1B83.
CNCom, sala B, 2003/10/08, "Caruso, Pablo Daniel c/Banco Francés SA s/ordinario”, elDial AA1CF9.
CNCom, sala B, 2003/10/17, "Garnica José Redolfo y otro c/Banco Itau Buen Ayre SA s/ordinario", elDial AA732.
CNCom, Sala B, 2005/02/14, “Palavecino, Mariela c. Banco de Galicia y Buenos Aires”, LA LEY 2005-C, 456 y DJ 16/11/2005, 830.
CNCom, sala B, 2005/03/09, “Sattler S.A. C/ Banco Río de la Plata S.A. s/ ordinario”, E-Boletin 84, DerechoyBanca.com.
CNCom, sala B, 2006/02/24, “Hager, Enrique Carlos c/Lloyds Bank y otro s/ordinario”, elDial AA33D9 y ED 01-08-2006.
CNCom, sala B, 2006/10/11, “Tahhan, Mariana c. Banco Río de la Plata”, LA LEY, 2007-B, 801.
CNCom, sala B, 23-11-1995, "Giacchino, Jorge c/ Machine & Man", LA LEY 1997-D, 859
CNCom, sala B, 30/12/2008, “González, Alberto Israel y otro c. Banco de Galicia y Buenos Aires S.A.”, LA LEY2009-B, 548.
CNCom, sala C, 03/2005, “Arquitectura del Agua SA C/ Banco Francés s/ordinario”, Diario judicial.com, 08/04/2005.
CNCom, sala C, 1993/06/30, "Giorgetti, Héctor R. y otro c/Georgalos Hnos. S. A. s/ordinario", LA LEY 1994-D, 113.
CNCom, sala C, 2001/05/02, "Martín, José Luis c/Banco Roberts Sociedad Anónima s/Ordinario", elDial - AA890.
CNCom, sala C, 2001/12/04, "Sorín, Daniel Israel c/Banco Sudameris Argentina S.A. s/ordinario", elDial AABB2.
CNCom, sala C, 2001/12/14, "Boschi, Mario Andrés c/Citibank N.A. s/ordinario", elDial - AAD44.
CNCom, sala C, 2002/03/26, “Halabi, Ernesto c/ Citibank NA”, elDial AAE44 y Diario Judicial.com, 04-04-2002.
CNCom, sala C, 2002/05/21, “Díaz Velar Hugo Alberto c/Banca Nazionale Del Lavoro Sociedad Anónima s/ordinario", elDial AA1136.
CNCom, sala C, 2003/08/08, "Polito, Francisco Antonio c/Banco Bansud Sociedad Anónima s/sumario", elDial - AA1A5B.
CNCom, sala C, 2003/09/26, "Vázquez, Viviana Beatriz c/Banco Río de la Plata Sociedad Anónima s/sumario", LA LEY 2004-B,1017; elDial AA1C2B.
CNCom, sala C, 2005/04/12, “E., V. M. J. c. Banco Francés”, LA LEY 2005-E,42.
CNCom, sala C, 2006/06/21, “Domínguez Carlos Alberto c/ BankBoston Na”., Diariojudicial.com 30/08/2006.
CNCom, sala C, 2007/03, “Shawn Daniel Eduardo c/ Banco Río de la Plata s/ ordinario”, Diariojudicial.com 16-08-2007.
CNCom, sala C, 2007/06/28, “Torri Marta Laura c/ Bankboston N.A. s/ amparo”, Microjuris: MJJ14105..
CNCom, sala C, 2007/07/06, “Carballo Alberto Rubén c/ Hexagon Bank Argentina S.A s/ amparo”, Microjuris: MJJ14558, Diariojudicial.com 07-08-2007.
CNCom, sala C, 2007/09/25, “Cassidi Diego Martin c/ Visa Argentina S.A. y otro s/ ordinario”, Microjuris: MJJ16104.

CNCom, sala C,14/07/2006, Sak, Liliana S. c. Citibank NA (LA LEY 2007-A, 456.
CNCom, sala D, 05/06/2007, "Larregui, Mariano c/ Banco Itau Buen Ayre y otro s/ ordinario", elDial AA3FC1.

- CNCom, sala D, 11/10/2002 "Fusto, Liliana Antonia c/ Organización Veraz Sociedad Anónima s/amparo", Diario Judicial.com 13-12-2002.
- CNCom, sala D, 13-05-1996, “Figueroa Hnos. S. A. c. Banco de la Provincia de Santiago del Estero”, LA LEY, 1997-E, 1003.

CNCom, sala D, 2000/11/07, "Vasen, Hugo Fernando c/ Citibank N.A., s/ Ordinario". elDial AA732.
CNCom, sala D, 2001/08/10, "Bachrach, Pedro c/ Banco Central de la República Argentina s/ ordinario". ElDial AAA3D.
CNCom, sala D, 2001/11/20, "Mazza, Miriam Elizabeth c/ Citibank N.A. s/ ordinario", elDial AAC4B.
CNCom, sala D, 2003/04/23, "Kindsuater, Patricia y otro c/ Diners Club Argentina S.A.C. y de T. y otro s/ ordinario", elDial - AA17AE.
CNCom, sala D, 2003/07/02 "Tondini, Claudio Oscar c/ Banco Tornquist SA y otro s/ ordinario", elDial - AA18CD.
CNCom, sala D, 2005/06/27, "Svampa Ana María c/ Banco Francés del Río de la Plata S.A. s/ ordinario", elDial AA2CA6.
CNCom, sala D, 2005/09/01, “Cardinale, Miguel A. y otro c. Banco de Galicia y Buenos Aires”, LA LEY 2006-A,287,
CNCom, sala D, 2005/10/19, "Sejas Mariana Paula c/ Bankboston N.A. s/ sumario", elDial AA2FAD.
CNCom, sala D, 2005/11/10, Valenti, Edmundo c/ Banco Francés S.A. s/ ordinario, derechoybanca.com 104-3.
CNCom, sala E, 1999/12/15,“Álvarez, Jorge Oscar c/Banco Roberts SA”, JA-2000-III-503.
CNCom, sala E, 2003/06/03, "Perlman Manuel c/ Bank Boston SA y otro s/ ordinario", elDial AA19C6.
CNCom, sala E, 2003/10/17,“Martínez, Nelly Aida c/Lloyds **Bank** s/ordinario”, Diario Judicial.com 21/01/2004 y La Ley Online.
CNCom, sala E, 2005/02/28, “Debaisi Efraín José c/ Banco Río de la Plata S.A. y otro s/ ordinario”, Diario Judicial.com 19/04/2005.
CNCom, sala E, 2005/03/22, “Construcur S.R.L. C/ Banco Rio de la Plata S.A. s/ ordinario”, E-Boletin 74- Derecho y banca.com
CNCom, sala E, 2006/08/16, “Guryn, Néstor c. Lloyds Bank S.A.”, LA LEY 2006-F, 830.
CNCom, sala E, 2006/09/05, "Gullo Roberto c/Societe Generale y otro s/ ordinario", elDial - AA3995.
CNCom, sala E, 2007/09/21, "Lagorio José Antonio c/ Banco Galicia y Buenos Aires SA s/ ordinario", elDial AA4328.
CNCom., sala C, 2000/08/18, “Scarpia, Juan C. c. Organización Veraz S.A”, LA LEY 2001-B, 298.
CNCom., sala E, 07/11/2007, "Segretin, Carlos c/ ABN Amro Bank NV Sucursal Argentina s/sumarísimo", elDial AA4597
CNPenal Económico, sala B, 25-09-1997, “Dirección General Impositiva”, LA LEY 1999-A, 204.

- Corte Constitucional de Colombia, Sentencia C 1011/08, en expediente PE 029 http://vlex.com/vid/colombia-ley-proteccion-datos-50034442

Corte Constitucional de Colombia, Sentencia T-414/92
http://www.ulpiano.com/habeasdata_fallos_colombia.htm

- CSJ Costa Rica, sala Constitucional, sentencia 2000-01119, 01-02-2000, http://*www.poder*-judicial.go.cr/salaconstitucional.

CSJ Costa Rica, sala Constitucional, sentencia 12695/2003, http://*www.poder*-judicial.go.cr/salaconstitucional.

CSJ Salta, 02-11-1998, “Rocco, Juan C c. Banco Mayo Coop. Ltdo”, LA LEY 1999-E, 904 y LLN.O.A, 199-234.

- CSJN, 05/04/2005, Recurso de hecho, "Martínez, Matilde Susana c/ Organización Veraz S.A.", LA LEY 2005-B, 743; RCyS 2005, 806 - DJ 2005-1, 1020; Fallos 328:797.

CSJN, 06-03-2007, “Organización Veraz S.A. v. Estado Nacional”, JA 2007-II-732, y LA LEY 2007-B, 303; DJ 21/03/2007, 692; RCyS 2007-IV, 37; Fallos 330:304.

CSJN, 09-03-1999, Matimport S.A. s/ medida precautoria”, LA LEY 2000-B, 31; DJ 2000-1, 25; RU 2000-3, 13; ED 182, 1303; RCyS 1999, 879.

CSJN, 11/12/1984, “Ponzetti de Balbín, Indalia c. Editorial Atlántida, S. A.”, LA LEY 1985-B, 120.

CSJN, 15-10-1998, “Urteaga, Facundo R. c/ Estado Mayor Conjunto de las FFAA s/amparo”, LA LEY 1998-F,237.

CSJN, 16-09-1999, “Ganora, Mario E y otra”, LA LEY, 2000-A, 355; 2000-B, 29 - DJ, 2000-1-1328.

CSJN, 21-22-2006, "Di Nunzio, Daniel F. c/ The First National Bank of Boston y otros s/ hábeas data", LA LEY 2007-C, 131.

Jdo Civ. y Com. Nº 10, Rosario, “A., L. c/ American Express S.A. s/ Daños y perjuicios”, Zeus, 16-12-2003.

- Jdo. Civ., Com. y Minas Nº 12, Mendoza, 03-11-1997, “Huertas, Juan C. c/ CO.DE.ME”, VJ, 1998-6-99 y LL Gran Cuyo 1998, 975.

Jdo. NCAF Nº 3, 02-11-1995, “Nalib Yabrán, Alfredo E. v. Estado Nacional”, JA 1996-III-1102.

JNPICom Nº 14: (Sec 27), 07-11-2003, "Depaolini, Angela Mabel C/ Citibank N.A. S/ sumario", DiarioJudicial.com, 14-11-2003.

SC Estados Unidos, 01-12-2000, “Janet Reno, Procuradora General de los Estados Unidos y otros”, http://supct.law.cornell.edu/supct/html/98-1464.ZO.html

- SCJMdza, sala I, 16-02-2009, “Albares Raúl c. Banco de Galicia”, LLGran Cuyo 2009 (marzo), 157; LA LEY 2009-B, 247, LLGran Cuyo 2009 (abril), 223.

SCJMdza, sala I, 17-11-1997, “Costa Esquivel, Oscar A. c. CO. DE. ME.”, DJ, 1998-3-864.

- STJ Entre Ríos, 22/12/2000 “O, M.N. c. Compañía Financiera Argentina SA”, LL Litoral 2001-424.

STJ Entre Ríos, sala 1ª, 08-11-1994, “R. R., J. E. v. Banco Francés del río de la Plata”, JA 1996-III-1102.

TSJ Venezuela, Sala Constitucional, 28-06-2006, expediente GP01-O-2004-000026,http://www.tsj.gov.ve/decisiones/scon/Junio/1281-260606-05-1964.htm/

Indice