# LA TUTELA PROCESAL DE LOS DATOS PERSONALES EN ESPAÑA E IBEROAMÉRICA

Enrique César Pérez-Luño Robledo
*Profesor Ayudante Doctor de Derecho Procesal (Universidad de Sevilla)*

La Constitución española de 1978 establece, en su artículo 18.4, que: "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Este derecho fundamental exigía el correspondiente desarrollo legislativo tendente a especificar y pormenorizar su significado, alcance e instrumentos de tutela.

A ese desarrollo se dirigió la promulgación de la Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

Se intentaba, con dicha norma, evitar los abusos informáticos contra la intimidad, así como contra otros derechos fundamentales[1].

El desarrollo legislativo del artículo 18.4 CE fue necesario por la obligación adquirida tras la ratificación en 1984 del Convenio de protección de datos personales (108) de 1981 del Consejo de Europa, cuyo art.4 exige a los países signatarios establecer en su Derecho interno las normas necesarias para garantizar la eficacia de los principios consagrados en dicho texto. Asimismo, al *Acuerdo de Schengen,* suscrito inicialmente por Alemania, Francia y los países del Benelux en 1985 y desarrollado por un Convenio de aplicación de 19 de Junio de 1990, al que se adhirieron otros Estados de la Unión Europea (España, Italia, Grecia, Portugal...). Dicho tratado internacional se refiere a la supresión gradual de controles

[1] Cfr., GARRIGA DOMÍNGUEZ, A., *La protección de los datos personales en el Derecho español*, con Prólogo, de A.E. Pérez Luño, Universidad Carlos III & Dykinson, Madrid, 1999, pp. 27 y ss.; id., *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2ª, ed., 2009, pp. 36 y ss.; PÉREZ LUÑO, A.E., "La LORTAD y los derechos fundamentales", en *Derechos y Libertade*s, 1993, nº 1, pp. 405 y ss.

entre las fronteras comunes de los países signatarios. Para ello, se regula el flujo de informaciones personales en función de la cooperación policial. El objetivo principal del Sistema de Información Schengen (SIS) es la comunicación de informaciones para el control de las personas "indeseables" y/o "inadmisibles" dentro de las fronteras del "espacio Schengen". Para el logro de ese objetivo entró en funcionamiento una gran base de datos policiales situada en Estrasburgo y sometida a la legislación francesa de protección de datos personales. Al igual que el Convenio del Consejo de Europa exige que para la transmisión de esas informaciones existan en cada país receptor normas internas sobre protección de datos personales que satisfagan los principios del Convenio del Consejo de Europa (arts. 117 y 126)[2].

En fecha posterior, la Unión Europea elaboró la Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de julio 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. En dicha Directiva se pretende armonizar la fluidez de la transmisión de datos en el seno de la Unión Europea para la mayor eficacia de los poderes públicos y desarrollo del sector privado, con la defensa de los datos personales. Para ello se prevé la existencia en cada Estado miembro de una autoridad independiente para garantizar la tutela de los datos personales y velar por la aplicación correcta de la Directiva (art. 28). Asimismo se contempla la existencia de una autoridad comunitaria denominada Grupo de protección de las personas que estará integrada por representantes de las autoridades de control nacionales y un representante de la Comisión, los cuales contribuirán a la interpretación homogénea de las normas nacionales adoptadas en aplicación de la Directiva, así como informarán a la Comisión de los conflictos que puedan surgir entre la legislación y las prácticas de los Estados miembros en materia de protección de datos personales (arts. 30 y 31). La Directiva establece la expresa

[2] Cfr.: LOSANO, M.G., *Il Trattato di Schengen e le frontiere europee* en "Data Manager", 1991, n. 114, pp. 27 y ss.; PÉREZ LUÑO, A.E., *La incorporación del Convenio Europeo sobre protección de datos personales al ordenamiento jurídico español*, en el nº 17 monográfico de "ICADE. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales", sobre *Informática y Derecho*, 1989, pp. 27 y ss.; id., *Libertad informática y leyes de protección de datos personales*, en colab. con M.G. Losano y M.F. Guerrero Mateus, Centro de Estudios Constitucionales, Madrid. 1989, pp. 163 y ss.; SÁNCHEZ BRAVO, A., *La protección del derecho a la libertad informática en la Unión Europea,* con Prólogo de A. E. Pérez Luño, Publicaciones de la Universidad de Sevilla, Sevilla, 1998, pp. 164 y ss.

obligación de los Estados miembros de adaptar las disposiciones legales, reglamentarias y administrativas necesarias para incorporar su texto y darle cumplimiento en los respectivos ordenamientos internos (art. 32)[3].

La LORTAD tuvo una vigencia efímera. Apenas siete años separan la fecha del 29 de octubre de 1992 en que fue promulgada de la del 13 de diciembre de 1999 en la que se produjo su derogación a través de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPRODA). Esta nueva Ley nació para el cumplimiento y adaptación al ordenamiento jurídico español de lo dispuesto en la mencionada Directiva 95/46 UE.

El 27 de abril de 2016 el Parlamento y el Consejo de la UE aprobaron tres textos normativos básicos para la protección y el tratamiento de los datos personales en el seno de la UE. Se trata del Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de protección de datos) y por el que se deroga la Directiva 95/46/CE; la Directiva 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo; y la Directiva 2016/681 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR)

---

[3] Cfr.: ARENAS RAMIRO, M., *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2006, pp. 275 y ss.
RIPOL CARULLA, S., *El proyecto de Directiva comunitaria sobre protección de datos: una valoración española*, en *Actas del III Congreso Iberoamericano de Informática y Derecho* (Mérida, septiembre 1992) publicadas en "Informática y Derecho", 1994, vol. 4, pp. 321 y ss.
SÁNCHEZ BRAVO, A., "El tratamiento automatizado de bases de datos en el marco de la Comunidad Económica Europea: su protección", *Informática y derecho: Revista iberoamericana de derecho informático*, Nº 4, 1994, pp. 341 y ss.
SÁNCHEZ BRAVO, A., *La protección del derecho a la libertad informática en la Unión Europea,* publicaciones de la Universidad de Sevilla, 2001, pp. 123 y ss.
SÁNCHEZ BRAVO, A., *Internet y la sociedad europea de la información: implicaciones para los ciudadanos,* con Prólogo de A.E. Pérez Luño, publicaciones de la Universidad de Sevilla, 2001, pp. 73 y ss.
PÉREZ LUÑO, A.E., *El concepto de interesado en la Directiva Comunitaria 95/46*, en el vol. col. *La protección del derecho a la intimidad de las personas (fichero de datos)*, Escuela judicial & Consejo General del Poder Judicial, Madrid, 1997, pp. 13 y ss.

para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

Tras más de veinte años de vigencia de la Directiva 95/46, en el que ha cumplido una función relevante para la tutela de los datos personales en el ámbito europeo, se ha culminado ahora el proceso de su necesaria renovación para adaptar la normativa de la UE a las nuevas exigencias y requerimientos de nuestro tiempo.

Para cumplir con ese reto con fecha de 17 de diciembre de 2015 el Comité de Libertades Civiles del Consejo y del Parlamento de la UE, aprobó con 48 votos a favor, 4 votos en contra y 4 abstenciones, una redacción definitiva de los textos del Reglamento y las Directivas de protección de datos. En dicha redacción los aspectos más innovadores respecto a los Proyectos aquí estudiados son los que hacen referencia a un reforzamiento de la posición de los particulares frente a los datos personales almacenados por sociedades multinacionales, con inclusión expresa de su oposición a que esos datos puedan ser utilizados o transmitidos al margen de los supuestos que han autorizado la inclusión en sus ficheros, así como el reconocimiento expreso del derecho al olvido.

Representa un rasgo novedoso de la nueva normativa su propósito de garantizar que el responsable del tratamiento de datos personales responda de la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema de información para resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. Con todo ello, se refuerzan también las garantías de los titulares de los datos personales frente a nuevas formas de agresión a los equipos informáticos que pudieran redundar en una vulneración de los datos que les conciernen.

El Reglamento ahora aprobado, trata de arbitrar fórmulas para facilitar al interesado el ejercicio de sus derechos, incluidos los mecanismos para solicitar y, en

su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar instrumentos para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos.

La actualidad y repercusión mediática del denominado "caso Google", Sentencia del 13 de mayo de 2014 del Tribunal de Justicia de la UE, ha motivado un especial interés del legislador europeo en la regulación del "derecho al olvido".

Así, el Reglamento establece que los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un "derecho al olvido" si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento.

Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho, aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

Para una mayor garantía jurídica del "derecho al olvido" en el entorno *on-line*, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los

responsables del tratamiento que estén elaborando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

En la medida en que en una sociedad democrática sea necesario y proporcionado para salvaguardar la seguridad pública, incluida la protección de la vida humana especialmente en respuesta a catástrofes naturales u ocasionadas por el hombre, la prevención, investigación, y el enjuiciamiento de infracciones penales o de violaciones de normas deontológicas en las profesiones reguladas, otros intereses públicos de la Unión o de un Estado miembro, especialmente un importante interés económico o financiero de la Unión o de un Estado miembro, o la protección del interesado o de los derechos y libertades de otros, el Derecho de la Unión o la legislación de los Estados miembros pueden imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación y supresión o al derecho a la portabilidad de los datos, al derecho a oponerse, a las medidas basadas en la elaboración de perfiles, así como a la comunicación de una violación de datos personales a un interesado y a determinadas obligaciones afines de los responsables del tratamiento.

La Directiva 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, permite el establecimiento de un marco de protección de datos que garantiza un alto nivel de protección de los derechos de los individuos a la vez que se respeta la naturaleza específica del ámbito de cooperación policial y judicial en materia criminal.

Su finalidad principal se cifra en conseguir que los datos personales utilizados dentro del ámbito de cooperación policial y judicial en materia criminal, sean tratados de modo que se garantice un nivel adecuado de seguridad y confidencialidad, en particular impidiendo el acceso sin autorización a dichos datos o el uso no autorizado de los mismos y del equipo utilizado en el tratamiento,

teniendo en cuenta el desarrollo técnico existente y la tecnología, los costes de ejecución con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse.

El nuevo marco regulatorio europeo establecido por esta Directiva pretende asegurar una protección de datos consistente y de alto nivel para mejorar la confianza mutua entre las autoridades policiales y judiciales de los diferentes Estados miembros de la UE, contribuyendo así a una mayor libertad de flujo de datos y una efectiva colaboración entre las autoridades policiales y judiciales.

Esta Directiva, al igual que el Reglamento, hallaron su fundamento en el artículo 16, apartado 2, del Tratado de Lisboa, que es una nueva base jurídica específica para la adopción de normas relativas a la protección de las personas físicas con respecto al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos, y por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y de normas relativas a la libre circulación de estos datos.

En definitiva, esta nueva Directiva de la UE, se propone garantizar un nivel uniforme y elevado de protección a las personas físicas titulares de los datos. Al propio tiempo, desea conjugar esta finalidad garantista con el reforzamiento de la confianza mutua entre las autoridades policiales y judiciales de los distintos Estados miembros y facilitando la libre circulación de datos y la cooperación entre las autoridades policiales y judiciales.

En la misma fecha que el Reglamento y la Directiva ya analizados, la UE promulgó la Directiva 2016/681 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. Este texto normativo tiene su antecedente en el "Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano", que data del año 2010 y fue elaborado por el Consejo Europeo.

El objeto de esta nueva Directiva consiste entre otras cosas, en garantizar la seguridad, proteger la vida y la seguridad de los ciudadanos y crear un marco jurídico para la protección de los datos PNR en lo que respecta a su tratamiento por las autoridades competentes.

En este texto se establecen algunas garantías básicas en materia de protección de datos. Entre ella, reviste especial interés la que en el ámbito del tratamiento de los datos PNR, hace referencia a que los Estados miembros velarán para que el responsable de la protección de datos tenga acceso a todos los datos tratados por la UIP (unidad única de información sobre los pasajeros). Si el responsable de la protección de datos considera que el tratamiento de un dato cualquiera no ha sido lícito, podrá remitirlo a la autoridad nacional de control (art. 6.7).

En definitiva, se ofrece una garantía general del sistema consistente en la obligación de los Estados de la UE para velar por que sus UIP apliquen las medidas y los procedimientos técnicos y organizativos adecuados para garantizar el elevado nivel de seguridad correspondiente a los riesgos que entrañen el tratamiento y las características de los datos PNR (art. 13.7).

Como balance de las nuevas disposiciones de la UE en materia de protección de datos puede afirmarse que el Parlamento y el Consejo europeos han tratado de establecer unas medidas y mecanismos de garantía de los datos personales tratando que las mismas no se vean afectadas por la necesidad de los Estados de responder a los atentados terroristas y las actividades de la criminalidad internacional organizada. La grave inquietud cívica y política que motivaron los últimos atentados terroristas perpetrados en Europa por organizaciones vinculadas al fundamentalismo islámico han creado un síndrome de alarma entre los ciudadanos de Europa. Hace algunos años el sociólogo alemán Ulrich Beck[4] definió a las sociedades actuales como "sociedad del riesgo". En los momentos actuales parece que nos hallamos ante una situación en la que podría hablarse de unas "sociedades del miedo". Esta nueva circunstancia obliga a los poderes públicos europeos a tomar medidas de protección y seguridad, pero ese tipo de medidas no puede vaciar de contenido las garantías de la libertad que constituyen el fundamento axiológico de la propia UE. Por ello, en los textos aquí analizados se advierte esa búsqueda de un equilibrio adecuado entre las medidas de seguridad que requieren las sociedades actuales para luchar contra el terrorismo y la criminalidad y la tutela de las libertades que, en las sociedades tecnológicas europeas, tiene un capítulo de decisiva importancia en la garantía de los datos personales y, en concreto del *habeas data*.

[4] BECK, U., "La sociedad del riesgo mundial: en busca de la seguridad perdida", Trad. Cast., Paidós, Barcelona, 2008.

En España la adaptación de estas normas emanadas por la UE en el año 2016 han supuesto la aprobación por las Cortes Generales españolas de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La recepción jurídica de la tutela de los datos personales ha tenido un desarrollo especialmente relevante en el constitucionalismo iberoamericano contemporáneo. La recepción en estos países de las normas constitucionales de España y Portugal sobre la defensa de la intimidad frente a la informática, han producido una experiencia normativa específicamente dedicada a la tutela constitucional de la protección de datos. Por la actualidad e interés de estas manifestaciones del Derecho comparado a protección de datos, así como por no haber sido objeto, todavía de una atención doctrinal en la bibliografía jurídica española, se apuntarán aquí algunas de las manifestaciones básicas de dicha experiencia normativa constitucional. Además, la recepción de dicha tutela a la protección de datos en el constitucionalismo latinoamericano constituye el marco más amplio y relevante en la recepción de esta categoría jurídica en el Derecho constitucional comparado. Ello se debe, en gran medida, a las reformas de los textos constitucionales y a los periodos constituyentes iniciados en Iberoamérica tras el derrocamiento de las dictaduras militares y la consiguiente instauración de Estados de Derecho. Por este motivo, estas nuevas Constituciones han prestado especial atención a la garantía de los derechos fundamentales, así como a elaborar un sistema de derechos y libertades acorde con las nuevas exigencias de la sociedad actual que, es la sociedad de las NT y las TIC. Por todo ello, la protección de datos personales, como instituto característico de los derechos de la tercera generación, ha tenido cumplida y detallada reglamentación en los renovados textos constitucionales de las Repúblicas latinoamericanas.

Así, en la Constitución de Guatemala de 1985, se dispuso: art. 31. "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. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos".

Dos años más tarde, en 1987, la Constitución de Nicaragua proclamó: art. 26. "Toda persona tiene 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].

Un año más tarde, la Constitución del Brasil de 1988 modificará esa tendencia de establecer únicamente un derecho de control sobre los datos o pregonar que la informática no deberá afectar a la intimidad de las personas, y sin establecer los principios relativos al tratamiento de los datos ni reconocer un derecho al control de los mismos, regulará la garantía específica de acceso a los datos personales, utilizando expresamente la terminología de *"habeas data"*. Así, se declara en el art. 5. LXXII. "Se concederá *habeas data*: a) para asegurar el conocimiento de informaciones relativas a la persona del solicitante, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para rectificar datos, cuando no se prefiriera hacerlo por procedimiento secreto, judicial o administrativo". A su vez, en el precitado artículo 5, apartado LXXVII, se prescribe: "Son gratuitas las acciones de *habeas corpus* y *habeas data* en la medida que la ley disponga los actos necesarios para el ejercicio de la ciudadanía. l. Serán de aplicación inmediata las normas definidoras de los derechos y garantías fundamentales. 2. Los derechos y garantías indicados en esta Constitución no excluyen otras que deriven del régimen y principios adoptados por ella o de los tratados internacionales en que la República Federativa del Brasil sea parte". Además de estas normas, que regulan el núcleo esencial del *habeas data* brasileño, la Constitución brasileña trae otras, reguladoras de aspectos secundarios, relativos a la competencia judicial para el enjuiciamiento de acciones de este tipo.

La Constitución brasileña no traza un dispositivo autónomo que contemple el derecho de conocer y de rectificar datos personales, sino que ese derecho es otorgado en la misma disposición normativa que instituye los instrumentos de su tutela. La norma constitucional tuvo, por tanto, una finalidad de garantía procesal de la situación jurídica de los afectados por injerencias indebidas en sus datos personales.

[5] Sobre la regulación de *habeas data* en Guatemala y Nicaragua, vid.: PIZZOLO, C., "El *habeas data* en el Derecho constitucional latinoamericano", en el vol. col. *La defensa de la intimidad y de los datos personales a través del habeas data,* a cargo de GOZAINI, O. A., EDIAR, Buenos Aires, 2001, pp. 65 y ss.

Según los comentaristas de este texto, el precepto constitucional tendía a la tutela de los ciudadanos frente a las informaciones manipuladas y ocultas en los archivos de inteligencia gubernamental, por lo general distorsionadas u obtenidas por métodos arbitrarios. La protección de datos fue incorporada a la Constitución brasileña de 1988 como consecuencia de la proyección de las disposiciones sobre protección de datos personales contenidas en la Constitución de Portugal de 1976, las cuales fueron establecidas, en gran medida, con el fin de permitir el acceso a las informaciones que se encontraban en poder de la arbitraria y violenta policía política, creada por Oliveira Salazar.

De manera similar, en la Policía brasileña y el Servicio Nacional de Informaciones se ocupaban de determinar quiénes eran los opositores al régimen de facto que culminó en 1985, y de perseguirlos. Por ello, con la misma finalidad que motivó la incorporación de la norma portuguesa, y en la inteligencia de facilitar el ingreso a tales archivos y permitir actuar sobre ellos, se consagró la tutela de los datos personales.

Una vez promulgada la norma constitucional, el ya citado artículo 5, apartado LXXII, fue desarrollado por vía reglamentaria diez años más tarde[6].

La Constitución colombiana de 1991 incorporó reglas relativas al tratamiento de datos personales, aunque no siguió el esquema brasileño, estableciendo: art. 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de los datos se respetarán la libertad y demás garantías consagradas en la Constitución".

El derecho reconocido en el art. 15 fue defendido rápida y reiteradamente a través de la acción de tutela consagrada en el art. 86 de la Constitución, y debido al sistema mixto de control de constitucionalidad imperante en ese país, la Corte Constitucional tuvo oportunidad de emitir una buena cantidad de

[6] CRETELLA JUNIOR, J., *Os "writs" na Constituçao de1988,* Forense Universitaria, Río de Janeiro, 1989, pp. 133 y ss.; LOPES MEIRELLES, H., *Mandado de segurança, açao popular, habeas data,* Malheiros Editores, Sau Paulo, 1991, pp. 153 y ss.

fallos sumamente valiosos donde desarrolla muy puntualmente –a falta de una ley especial– los principios que deben respetarse en el tratamiento de datos personales.

Un año después, la Constitución paraguaya de 1992 incorpora la siguiente previsión: art. 135. "Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos".

La norma fue incluida a partir de la propuesta de una comisión formada por investigadores, magistrados y docentes, que tomaron al instituto de la disposición contenida en el art. 31 de la Constitución guatemalteca y de las reglas incorporadas en la Carta brasileña de 1988 y la Constitución colombiana de 1991.

Entre las motivaciones que llevaron a aprobar el texto paraguayo, se tuvieron presente aquellas que impulsaron la tutela de los datos personales en el Brasil. Se quiso evitar que las informaciones en poder de la Policía no quedaran fuera de control por parte de las personas concernidas, con la consiguiente tutela judicial de éstas[7].

En la Constitución peruana de 1993, se tipifica el *habeas data* como una acción y define, aparte el contenido del derecho a la protección de los datos personales.

Así, dispone dicha Constitución, en su art. 200 que: "Son garantías constitucionales... 3) La acción de *habeas 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 art. 2° de la Constitución". Dicho artículo

[7] En relación con las disposiciones constitucionales de Colombia y Paraguay reguladoras del *habeas data*, cfr. PUCCINELLI, O. R., "El *habeas data* en las Constituciones indoamericanas. Marco constitucional, jurisprudencial y legislación argentina", en el vol. col. *La defensa de la intimidad y de los datos personales a través del habeas data,* a cargo de GOZAINI, O. A., EDIAR, Buenos Aires, 2001, pp. 93 y ss.

establece que: ... "5) Toda persona tiene derecho 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 su pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. 6) A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal o 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...".

Esta reglamentación constitucional puede considerarse como novedosa y acertada, en especial, porque incluye al *habeas data*, cuya misión es la de acceder a información pública, por parte de las personas cuyos datos personales se hallan archivados en ficheros administrativos. Un sector de la doctrina, no obstante, criticó dicha disposición por su excesiva amplitud. A las críticas de la doctrina se le sumó las de los medios de comunicación, que entendían coartada su libertad de expresión por una garantía excesiva y casi exorbitante del derecho al honor y a la intimidad, en detrimento de la libertad informativa.

Las presiones fueron tales que el propio legislador constitucional autor de la norma fue quien propició la reforma de la Constitución en este aspecto. Como lo indica Francisco Eguiguren Praeli, esas críticas provocaron la reforma constitucional operada por la ley 26.470 y promovida por el partido mayoritario parlamentario. Tras dicha reforma constitucional, se suprimió la posibilidad de recurrir al *habeas data* como acción procesal para la rectificación de informaciones de los medios de comunicación. No obstante, dicha institución se mantuvo como derecho de acceso a los datos personales contenidos en archivos informáticos públicos, por parte de las personas concernidas[8].

Quedó así estructurado el *habeas data* como acción procesal para acceder a los datos personales y como vía para controlar la información pública, dicha regulación constitucional, resulta de indiscutible utilidad para la defensa de los

[8] EGUIGUREN PRAELI, F., "El *habeas data* y su desarrollo en el Perú", ponencia presentada en el *Seminario Internacional sobre la Acción de Habeas data,* organizado por la Universidad de Talca, Chile, entre el 9 y 11 de abril de 1997 Publicada en *Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú*, 1997, n. 51, pp. 308 y ss.; ORTECHO VILLENA, V.J. *Jurisdicción y Procesos constitucionales. Habeas Corpus y Amparo. Habeas data, Acción popular. Acción de Cumplimiento. Inconstitucionalidad*, Editorial Rhodas, Lima, 2003, pp. 179 y ss.

derechos fundamentales, en especial de la intimidad, frente a los principales tipos de injerencia y abusos perpetrados por una indebida utilización de los sistemas informáticos públicos.

La regulación constitucional peruana influyó en los subsiguientes textos constitucionales promulgados en Iberoamérica, a partir de entonces.

A poco de dictada la Constitución peruana, y en medio de los debates doctrinales y políticos que sobre ella tuvieron lugar, en 1994 se produce la reforma constitucional argentina y el *habeas data* fue incluido, aunque sin ser rotulado así, como acción y como subtipo de amparo en el art. 43, tercer párrafo, de la nueva Constitución de la República de Argentina.

El mencionado art. 43 de la Ley Superior Argentina prescribe: "... Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

La norma ha tenido un amplio desarrollo jurisprudencial, con fallos en especial los resueltos por la Corte Suprema de Justicia de la Nación que le han otorgado una amplitud al instituto y lo han llevado a exceder considerablemente los contornos establecidos en el art. 43 constitucional. Inclusive, ha sido objeto de permanente debate en el Congreso nacional, donde varios proyectos han sido tratados, y de los dos que obtuvieron sanción por el Congreso, el primero fue objeto de veto total presidencial, y el segundo, sancionado el 4 de octubre de 2000 se convirtió en ley, aunque sufrió un veto parcial en aspectos que no afectan a la dimensión procesal del *habeas data*[9].

[9] Cfr.: FLORES DAPKEVICIUS, R., Amparo *habeas corpus y habeas data*, Faira Editor, Montevideo-Buenos Aires, 2011, pp. 130 y ss.
PALAZZI, P. A., "EL *habeas data* en el Derecho constitucional argentino", en el vol., col., *.La defensa de la intimidad y de los datos personales a través del habeas data,* a cargo de GOZAINI, O. A., EDIAR, Buenos Aires, 2001, pp. 25 y ss.
PIERINI, A., LORENCES, V., TORNABENE, M.I., *Habeas data*. *Derecho a la intimidad*, Editorial Universidad, Buenos Aires, 1999, pp. 65 y ss.

En 1997, La República del Ecuador reformó su Constitución. Entre los aspectos innovadores de dicha reforma, destaca la disposición constitucional que establece en el artículo 30, la tutela de los datos personales en los siguientes términos: "Toda persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma o sobre sus bienes consten en entidades públicas o privadas, así como conocer el uso que se haga de ellos y su finalidad". "Igualmente, podrá solicitar ante el funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquéllos si fueren erróneos o afectaren ilegítimamente sus derechos". "Se exceptúan los documentos reservados por razones de seguridad nacional".

Esta norma constitucional fue objeto de un desarrollo reglamentario por la Ley del Control Constitucional que data también de 1997.

Un año después, en 1998, se sucede una nueva reforma constitucional y se regula la protección de los datos personales en los siguientes términos: art. 94. "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, 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".

La norma ha tenido hasta el momento escaso uso, atento a ser reciente y a la carencia de antecedentes jurisprudenciales que provocaran un desarrollo específico.

En 1999, la ahora "República Bolivariana de Venezuela" reforma su Constitución, e inserta las siguientes previsiones: art. 27. "Todos tienen derecho a ser amparados por los tribunales en el goce y ejercicio de los derechos y garantías constitucionales, aun de aquellos inherentes a la persona que no figuren expresamente en esta Constitución o en los instrumentos internacionales sobre derechos humanos".

"El procedimiento de la acción de amparo constitucional será oral, público, breve, gratuito y no sujeto a formalidad, y el juez competente tendrá potestad para restablecer inmediatamente la situación jurídica infringida o la situación que más se asemeje a ella. Todo tiempo será hábil y el tribunal lo tramitará con preferencia a cualquier otro asunto".

A su vez, se proclama en el art. 28 que: "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 aquéllos, 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".

Se alude también a la protección de datos personales, cuando se regulan las atribuciones del Defensor del Pueblo. Así, el art. 281 prescribe: "Son atribuciones del Defensor del Pueblo... 3. 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".

Esta norma tiene a su favor algunos aspectos que deben considerarse acertados en la reglamentación del *habeas data*. En primer término, el de ampliar la acción de *habeas data* a la información de datos personales contenidos en ficheros informatizados privados, no restringiéndola a los de titularidad pública. Es sabido que la agresión a la intimidad, perpetrada desde soportes informáticos, no es privativa del sector público, sino que puede partir de personas o entidades privadas, sin que sus efectos sean menos lesivos para la garantía de los datos personales, que aquellas que parten de abusos administrativos. En segundo lugar, el de extender la garantía de confidencialidad de la fuente de la información a otras profesiones distintas del periodismo, y en tercer lugar, que constituye una novedad distintiva, el reconocimiento de la facultad del Defensor del Pueblo de interponer la acción de *habeas data*[10].

[10] PÉREZ-LUÑO ROBLEDO, E. C., "El procedimiento de habeas data: El derecho procesal ante las nuevas tecnologías", Dykinson, Madrid, 2017, pp. 133 y ss.

Además de los países mencionados, otros países latinoamericanos que no cuentan con el diseño de una garantía específica en el plano constitucional, como Costa Rica, Chile y México han promulgado leyes relativas al tratamiento de datos personales.

Del análisis crítico de las experiencias normativas que conforman actualmente la tutela procesal de los datos personales en España e Iberoamérica, así como de las elaboraciones doctrinales que han sido objeto de estudio en el curso de este trabajo, se puede concluir la novedad, la relevancia presente y la proyección futura de esta categoría jurídica.

## Bibliografía

ARENAS RAMIRO, M., El derecho fundamental a la protección de datos personales en Europa, Tirant lo Blanch, Valencia, 2006.

BECK, U., La sociedad del riesgo mundial: en busca de la seguridad perdida, Trad. Cast., Paidós, Barcelona, 2008.

CRETELLA JUNIOR, J., Os "writs" na Constituçao de1988, Forense Universitaria, Río de Janeiro, 1989.

EGUIGUREN PRAELI, F., "El habeas data y su desarrollo en el Perú", ponencia presentada en el Seminario Internacional sobre la Acción de Habeas data, organizado por la Universidad de Talca, Chile, entre el 9 y 11 de abril de 1997 Publicada en Revista de la Facultad de Derecho de la Pontificia Universidad Católica del Perú, 1997, n. 51.

FLORES DAPKEVICIUS, R., Amparo habeas corpus y habeas data, Faira Editor, Montevideo-Buenos Aires, 2011.

GARRIGA DOMÍNGUEZ, A., La protección de los datos personales en el Derecho español, con Prólogo, de A.E. Pérez Luño, Universidad Carlos III & Dykinson, Madrid, 1999.

GARRIGA DOMÍNGUEZ, A., Tratamiento de datos personales y derechos fundamentales, Dykinson, Madrid, 2ª ed., 2009.

LOPES MEIRELLES, H., Mandado de segurança, açao popular, habeas data, Malheiros Editores, Sau Paulo, 1991.

LOSANO, M. G., Il Trattato di Schengen e le frontiere europee en "Data Manager", 1991, n. 114.

ORTECHO VILLENA, V.J. Jurisdicción y Procesos constitucionales. Habeas Corpus y Amparo. Habeas data, Acción popular. Acción de Cumplimiento. Inconstitucionalidad, Editorial Rhodas, Lima, 2003.

PALAZZI, P. A., "EL habeas data en el Derecho constitucional argentino", en el vol., col., La defensa de la intimidad y de los datos personales a través del habeas data, , a cargo de GOZAINI, O. A., EDIAR, Buenos Aires, 2001.

PEREZ LUÑO, A.E., "La LORTAD y los derechos fundamentales", en Derechos y Libertades, 1993, nº 1.

PÉREZ LUÑO, A.E., El concepto de interesado en la Directiva Comunitaria 95/46, en el vol. col. La protección del derecho a la intimidad de las personas (fichero de datos), Escuela judicial & Consejo General del Poder Judicial, Madrid, 1997.

PÉREZ LUÑO, A.E., La incorporación del Convenio Europeo sobre protección de datos personales al ordenamiento jurídico español, en el nº17 monográfico de "ICADE. Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales", sobre Informática y Derecho, 1989.

PÉREZ LUÑO, A.E., Libertad informática y leyes de protección de datos personales, en colab. con M.G. Losano y M.F. Guerrero Mateus, Centro de Estudios Constitucionales, Madrid, 1989.

PÉREZ-LUÑO ROBLEDO, E. C., El procedimiento de habeas data: El derecho procesal ante las nuevas tecnologías, Dykinson, Madrid, 2017.

PIERINI, A., LORENCES, V., TORNABENE, M.I., Habeas data. Derecho a la intimidad, Editorial Universidad, Buenos Aires, 1999.

PIZZOLO, C., "El habeas data en el Derecho constitucional latinoamericano", en el vol. col. La defensa de la intimidad y de los datos personales a través del habeas data, a cargo de GOZAINI, O. A., EDIAR, Buenos Aires, 2001.

PUCCINELLI, O. R., "El habeas data en las Constituciones indoamericanas. Marco constitucional, jurisprudencial y legislación argentina", en el vol. col. La defensa de la intimidad y de los datos personales a través del habeas data, a cargo de GOZAINI, O. A., EDIAR, Buenos Aires, 2001.

RIPOL CARULLA, S., El proyecto de Directiva comunitaria sobre protección de datos: una valoración española, en Actas del III Congreso Iberoamericano de Informática y Derecho (Mérida, septiembre 1992) publicadas en "Informática y Derecho", 1994, vol. 4.

SÁNCHEZ BRAVO, A., "El tratamiento automatizado de bases de datos en el marco de la Comunidad Económica Europea: su protección", Informática y derecho: Revista iberoamericana de derecho informático, Nº 4, 1994.

SÁNCHEZ BRAVO, A., Internet y la sociedad europea de la información: implicaciones para los ciudadanos, con Prólogo de A.E. Pérez Luño, publicaciones de la Universidad de Sevilla, 2001.

SÁNCHEZ BRAVO, A., La protección del derecho a la libertad informática en la Unión Europea, publicaciones de la Universidad de Sevilla, 2001.