LA PROTECCIÓN DE DATOS PERSONALES Y LA AUTODETERMINACIÓN INFORMATIVA COMO RESPUESTA DESDE EL DERECHO ANTE EL PODER INFORMÁTICO*

JUAN MANUEL ACUÑA

SUMARIO: Explicación preliminar. I. El problema: el desarrollo informático y la amenaza a la intimidad. II. El reconocimiento de la amenaza. Los primeros textos normativos. III. Conflicto de derechos: libertad informática vs. derecho a la intimidad. IV. Las respuestas desde el derecho. 1. Los datos sensibles. 2. El habeas data. V. El derecho a la autodeterminación informativa. A modo de conclusión.

EXPLICACIÓN PRELIMINAR

El presente trabajo no tiene finalidades sistematizadoras respecto al tupido escenario de la protección jurídica de datos personales. Nos proponemos llevar adelante una tarea mucho más modesta consistente en presentar al lector una introducción a la

*Agradezco al profesor Guillermo Antonio Tenorio Cueto el tiempo dispensado en la lectura de este trabajo y sus valiosas observaciones.

problemática que motivó el desarrollo por parte de los juristas de categorías jurídicas y mecanismos, con el propósito de defender una serie de derechos fundamentales que pudieran verse amenazados o vulnerados por el poder informático. A continuación esbozaremos el desarrollo normativo de dichas categorías y mecanismos para luego presentar una serie de reflexiones en torno a la autodeterminación informativa buscando es motivar la discusión sobre los márgenes que actualmente tiene la protección de datos personales y contemplar si los mismos deben ser ampliados.

I. EL PROBLEMA. EL DESARROLLO INFORMÁTICO Y LA AMENAZA A LA INTIMIDAD

Los desarrollos actuales de la informática han generado nuevos intereses y posibilidades así como problemas diferentes que se deben afrontar y solucionar. En el campo del derecho se ha trabajado en la búsqueda de respuestas adecuadas a esos problemas planteados por el impacto de la informática en la vida social: contratos informáticos, delitos informáticos, firma electrónica, entre otras cuestiones, son parte del horizonte que ha despertado la imaginación de los juristas en la búsqueda de respuestas satisfactorias que permitan expandir los estrechos marcos tradicionales.

La operación de recolectar, clasificar y administrar información siempre ha existido, lo que ha evolucionado son las técnicas para ejecutar tales actividades.[1] El desarrollo informático con la posibilidad de procesar enormes cantidades de datos con posibilidades inimaginables de interrelación y transferencia ha generado nuevas amenazas a ciertos derechos fundamentales, especialmente—y en lo que interesa en este trabajo— al derecho a la intimidad.[2] Pero esta relación atormentada entre desarrollo tec-

[1] Stiglitz, Rosana M., "Impacto de la Informática en la sociedad", en *Revista La Ley*, Buenos Aires, 1987, p. 859.

[2] Para efectos del presente trabajo, no trazaremos una distinción entre los términos privacidad e intimidad. Cierto sector de la doctrina entiende que la privacidad

nológico y derecho a la intimidad no es una novedad. Como señala acertadamente Fernández Segado,[3] el desarrollo de nuevas circunstancias sociales, concretamente el enorme avance de los medios de comunicación escrita, motivaron el ya famoso artículo de Warren y Brandeis acerca del derecho a la privacidad en el cual los mencionados autores vertieron opiniones como las siguientes. "Fotografías instantáneas y empresas periodísticas han invadido los recintos sagrados de la vida privada y doméstica y numerosos ingenios mecánicos amenazan con hacer buena la predicción según la cual lo que se susurra en el gabinete será proclamado desde los tejados".[4] A finales del siglo XIX los autores avizoraban los efectos devastadores que los adelantos tecnológicos podían tener sobre la privacidad.

---

refiere a aquellas acciones voluntarias de los individuos que no afectan a terceros aunque fueran conocidas por éstos, y que por ello quedan exentas de calificación por parte de la moral pública. En cambio, la intimidad hace referencia a la esfera de la persona exenta del conocimiento de los demás y que así debe ser conservada. Alberto Bianchi, quien no encuentra distinción entre ambos conceptos ha afirmado: "En mi opinión, esta distinción es más aparente que real. No encuentro, ni desde el punto de vista lingüístico, ni del jurídico diferencia relevante alguna entre lo íntimo y lo privado. Ambos dan idea de algo reservado a donde sólo tienen acceso ciertas personas", Bianchi, Alberto, *Habeas Data y derecho a la privacidad*, pp. 161-867. En igual sentido se expresa Eduardo Meins, quien al referirse a la cuestión aquí analizada sostiene que "Sin embargo, creemos que este distingo (entre privacidad e intimidad) carece de efectos jurídicos en nuestro ordenamiento legal, el que al emplear el término vida privada, no excluye el concepto de intimidad", Meins O., Eduardo, "*Consideraciones sobre la acción de habeas data*", en *Derecho a la autodeterminación informática y acción de Habeas Data en Iberoamérica*. Ius et Praxis. Derecho en la Región, Facultad de Ciencias Jurídicas y Sociales, Universidad de Talca, año 3, núm. 1, Chile, 1997. Para efectos de este trabajo y sin dejar de reconocer que sí aceptamos la existencia de diferencias de grado entre ambos términos, los consideraremos como términos que hacen alusión a una esfera de reserva del individuo.

[3] Fernández Segado, Francisco, "El Régimen jurídico del tratamiento automatizado de datos de carácter personal en España", en *Derecho a la autodeterminación informática y acción de Habeas Data en Iberoamérica. Ius et Praxis. Derecho en la Región*, Facultad de Ciencias Jurídicas y Sociales, Universidad de Talca, año 3, núm. 1, Chile, 1997, p. 33.

[4] Warren, Samuel y Brandeis, Louis, *El derecho a la intimidad*, Madrid, Civitas, 1995, p. 25.

De hecho, el artículo mencionado, que fuera publicado en la *Harvard Law Review* en su núm. 193 del año 1890, fue un hito en el desarrollo de la privacidad como derecho y un primer intento de contornear sus fronteras impenetrables. Samuel Warren, prestigioso abogado bostoniano, y Louis Brandeis, quien con posterioridad a la publicación de este artículo ocupara el cargo de juez en la Corte Suprema de Justicia de Estados Unidos entre 1916 y 1939, plantearon que el *common law* como sistema jurídico ofrecía un derecho general a la privacidad, o en sus palabras, un "right to be let alone" que permitía obtener protección en caso de violaciones a la vida privada provocadas por la prensa.[5] La novedad del artículo radica, según la opinión de Alberto Bianchi, en sostener que el derecho a la privacidad abarca la protección de ciertos bienes inmateriales como los pensamientos, las emociones, las sensaciones de una persona, cuando hasta ese momento, sólo bienes materiales habían sido objeto de protección.[6]

Debe quedar claro entonces que la preocupación por las influencias de los cambios sociales y tecnológicos sobre la esfera de intimidad del individuo no es nueva, de hecho, los primeros avances teóricos importantes en el campo del derecho a la privacidad fueron motivados por cambios de tal tipo, concretamente por el surgimiento de la prensa como medio masivo de comunicación y sus nuevos "apetitos invasivos".

Pero la "era de las computadoras" ha hecho necesario que el derecho y los juristas —como lo hicieran Warren y Brandeis a finales del siglo XIX— estén a la altura de los nuevos desafíos y ofrezcan respuestas —traducidas no solamente en medios de protección— para evitar la violación de los más caros derechos de la tradición liberal, especialmente, el derecho a la intimidad.

Decíamos líneas arriba que el acopio de datos no es tarea nueva, sin embargo, el almacenamiento de datos bajo las nuevas tecnologías reviste características de novedad. Antes de la implementación de las computadoras para tales efectos, sólo

[5] Fernández Segado, Francisco, *op. cit*., nota 3, p. 34.

[6] Bianchi, Alberto, *op. cit*., nota 2, p. 871.

habían sido utilizados los registros manuales o mecánicos que presentaban serios problemas principalmente por lo engorroso de su manejo a efectos del registro, actualización, consulta y traslado y, por otro lado, en lo referente a los costos operativos pues su manejo requería, entre otras cosas, grandes espacios físicos de almacenamiento y considerable cantidad de personal para su manipulación. Estas características tornaban a estas bases de datos difíciles de manejar, y peligrosas por su fácil desactualización.[7]

La aparente inoperatividad de estos sistemas de acopio de información pudo haber motivado cierta despreocupación por dotar de mecanismos tuitivos a los particulares aunque también, y por qué no decirlo, el derecho y los juristas suelen actuar de manera reactiva, es decir, luego de aparecida la amenaza o problema.

Los desarrollos informáticos han permitido el almacenamiento, tratamiento y transmisión de datos bajo un nuevo sentido: su interconexión.[8] Veamos. Para entender los peligros del acopio informatizado de datos es necesario definir tres términos fundamentales: por un lado, la expresión dato, "alude a un elemento circunscrito y aislado, nombre o nacionalidad etcétera, que no alcanza a tener el carácter de información pues para que se transforme en ella, se requiere la interconexión de datos que, vinculados, se conviertan en una referencia concreta".[9]

Cuando los datos son agrupados con un determinado sentido, organizados de manera sistemática de modo que pueda ser analizado otorgando un sentido diferente al del dato tomado en su singularidad, conforman una base de datos,[10] por último, cuando las bases de datos están organizadas y son accesibles en línea, se transforman en un banco de datos.[11]

Resulta difícil que un dato tenga incidencia real sobre la esfera de intimidad de una persona, pero cuando ese dato es

[7] Puccinelli, Óscar Raúl, *Habeas Data: Aportes para una eventual reglamentación*, pp. 161-913.

[8] *Idem.*

[9] *Idem.*

[10] *Idem.*

[11] *Idem.*

vinculado a otros de manera que da respuesta a una consulta determinada o sirve a un fin específico se ha convertido en información que, dependiendo de qué tipo de información se trate y quien la manipule puede generar una seria afectación a la intimidad de las personas.[12] Concretamente, la amenaza radica en la vinculación de datos. Óscar Puccinelli lo señala claramente: "Aun cuando a los datos almacenados pueda considerárselos inofensivos o carentes de importancia, el hecho es que la suma de ellos conjugados desde una o más bases o bancos de datos permite que se llegue a desnudar la intimidad de las personas haciendo ilusorias las garantías constitucionales".[13] El conocimiento ordenado de datos, concretamente aquellos de carácter personal, puede arrojar un determinado perfil de la persona, que será valorado para las más diversas cuestiones tanto públicas como privadas, desde la obtención de un trabajo hasta la concesión de un crédito. Esto en principio no genera cuando menos intuitivamente mayores inconvenientes, la cuestión es identificar cuáles son aquellos datos que podemos admitir, sean incorporados a un banco de datos y por ello, accesibles por determinados sujetos y con base en los cuales puedan decidirse extremos como los señalados. ¿Estaríamos dispuestos a admitir el almacenamiento de datos tales como religión, inclinación sexual, ideología política, gustos literarios, cinematográficos, culinarios, antecedentes penales, estado de salud, etcétera? La vinculación de datos semejantes permite que quien tenga acceso a ellos, pueda conocer quizá el fuero más íntimo de la persona, su perfil completo y el interrogante que llegado este momento debemos plantearnos es si tenemos derecho a ocultar esos datos.

[12] Davara Rodríguez, Miguel Ángel, *La protección de datos en Europa*, Madrid, Universidad Pontifica Comillas, 1998. Citado por Gozaíni, Osvaldo, en *Derecho procesal constitucional. Habeas Data. Protección de datos personales. Doctrina y jurisprudencia*, Buenos Aires, Rubinzal Culzoni, 2001, p. 114.

[13] Puccinelli, Óscar Raúl, *op. cit*., nota 7, p. 914.

II. EL RECONOCIMIENTO DE LA AMENAZA. LOS PRIMEROS TEXTOS NORMATIVOS

Ya en el año 1968, en el seno de la Conferencia Internacional sobre Derechos Humanos realizada en Teherán, se manifestó preocupación por las afectaciones que los avances tecnológicos pudieran generar en los derechos humanos.[14] Se declaró que la ONU propusiera a los Estados, la elaboración de estudios que sirvieran de impulso a normas que protegieran adecuadamente los derechos de las personas. En el ámbito europeo los estudios indicados dieron como resultado el surgimiento de una serie de leyes que a nivel nacional y local comenzaron a determinar ámbitos y establecer mecanismos de protección. Así, la ley del Land de Hesse (Alemania) del 7 de octubre de 1970 que reguló las bases de datos de su administración y que creaba la figura del comisario para la protección de la información y Suecia con su ley del 11 de mayo de 1973, que creó un registro público de archivos electrónicos de datos personales, estableció el otorgamiento de una licencia a quienes pretendan gestionar un registro de datos personales, suelen ser consideradas naciones pioneras en la protección de datos personales.[15] Francia, en 1978, sancionó la Ley de informática, ficheros y libertades por la cual se creó la Comisión Nacional de informática y Derecho[16] que entre otras funciones, autorizaba la creación de registros de bases de datos del sector público. La ley estableció una serie de principios en los cuales debería incardinarse la actividad de quienes generen y administren bancos de datos,[17] regimentó el denominado derecho de

[14] La Proclamación de Teherán del 13 de mayo de 1968 realizada en el seno de la Conferencia Internacional de Derechos Humanos expresó en su declaración 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".

[15] Fernández Segado, Francisco, *op. cit*., nota 3, p. 36.

[16] *Cfr*. Ley 78/17 del 6-1-78, Capítulo III.

[17] *Cfr*. Ley 78/17, Artículo 1. "La informática debe estar al servicio de cada ciudadano. Su desarrollo debe desenvolverse en el marco de la cooperación internacio-

acceso del particular a los datos contenidos sobre su persona en una de estas bases de datos registradas[18] y prohibía la recolección de los llamados datos sensibles sobre los que discutiremos más adelante;[19] Austria también generó su ley de protección de datos en el mismo año, estableciendo la obligatoriedad del registro para las empresas dedicadas al procesamiento de datos; Inglaterra desde 1974 cuenta con su ley de protección de datos. España ha llevado la punta en cuanto al tratamiento normativo de la protección de datos personales. Su Constitución, del año 1978, estableció en su artículo 18: "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". En desarrollo de la norma constitucional citada, y con cierta dilación, fue sancionada la ley 5/92 denominada Ley Orgánica de Regulación del Tratamiento de Datos (LORTAD) que fuera luego derogada por la ley 15/1999 de protección de datos de carácter personal. En el ámbito regional europeo, la Convención para la Protección de los individuos con relación al procesamiento automático de datos personales conocida como la Convención de Estrasburgo del año 1981 marca un hito en la evolución de los cuerpos normativos referentes a la protección de datos personales. Entre las principales características de este cuerpo normativo podemos mencionar: a) Postula que cada Estado debe garantizar dentro de su espacio el derecho a la vida privada con respecto al tratamiento automatizado de datos de carácter personal entendiendo por "dato de carácter personal" cualquier información relativa a una persona física identificada o identificable, b) abar

---

nal. No debe afectar la identidad humana ni los derechos humanos ni la vida privada ni las libertades públicas y privadas". Artículo 2. "Ninguna decisión judicial, que implicara apreciación sobre el 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".

[18] *Cfr.* artículo 34.

[19] *Cfr.* artículo 31.

car a ficheros tanto públicos como privados, c) identifica los llamados datos sensibles, es decir, aquellos datos de carácter personal que identifiquen origen racial, opiniones políticas, convicciones religiosas, datos relativos a estado de salud y a la orientación sexual, datos todos estos que no podrían tratarse de manera automatizada.

Estados Unidos cuenta desde 1974 con un ordenamiento regulador, la Privacy Act, luego reformada en 2002 que fue una respuesta a la problemática generada por los bancos de datos en poder de las oficinas gubernamentales, problemática consistente en que las personas no tenían conocimiento de qué órgano del gobierno estaba en posesión de sus datos y cuál era el contenido de éstos. La situación se tornaba aún más compleja porque los datos entregados a una determinada agencia bajo compromiso de confidencialidad, eran entregados y compartidos con otras agencias las cuales los usaban para fines diferentes y no aceptados originalmente por el titular del dato. La Privacy Act se propuso erradicar estas prácticas violatorias de la intimidad y dispuso la prohibición a compartir datos entre agencias sin el consentimiento del titular, la prohibición de modificar la finalidad original del acopio de los datos y se otorgó al particular, un recurso para tener acceso a los datos y ordenar su modificación o cancelación ante error o posesión injustificada del dato.[20]

De este primer aluvión legislativo, y siguiendo la enumeración realizada por Altmark y Molina Quiroga[21] pueden ser extraídos una serie de principios y directrices que hoy resultan compartidos y que deben ser tomados en cuenta al regular la materia de protección de datos. Entre ellos, cabe mencionar los siguientes:

a) La recolección de datos debe obedecer a propósitos generales y a usos específicos socialmente aceptables.
b) Los datos deben ser recolectados por medios lícitos.

[20] Bianchi, Alberto, *op. cit*., nota 2, p. 674.

[21] Altmark, Daniel Ricardo y Molina Quiroga, Eduardo, "*Habeas Data", Revista La Ley*, Buenos Aires, 14/03/1996, pp. 1556-1557.

c) La circunstancia de contar con datos de la persona, debe ser informada al sujeto a quien pertenecen los datos recolectados.
d) Los datos deben ser recolectados con el expreso consentimiento del sujeto.
e) Los datos recolectados deben ser exactos, completos y actuales por ello, pesa sobre el recolector la obligación de actualizar, rectificar y cancelar la información cuando correspondiere.
f) La finalidad para la recolección de la información debe ser expresamente declarada por el recolector, no pudiendo ser modificada posteriormente.
g) El sujeto titular de los datos debe dar su expreso consentimiento para que aquellos sean transmitidos a terceros.
h) El gestor del banco de datos tiene la obligación de tomar las medidas de seguridad pertinentes para la preservación del banco de datos.
i) La conservación de los datos debe estar temporalmente limitada.
j) Se debe establecer en cada jurisdicción, un adecuado sistema de control que permita la vigencia de los principios enunciados.
k) Se debe garantizar el derecho de acceso a los datos del sujeto.

Vistos someramente el estado del problema y las primeras medidas legislativas tomadas en aras de la protección de los datos personales, debemos ahondar más en el conflicto esbozado entre la libertad informática y el derecho a la intimidad.

III. CONFLICTO DE DERECHOS: LIBERTAD INFORMÁTICA VS. DERECHO A LA INTIMIDAD

El derecho a la intimidad puede ser entendido como "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".[22]

Los avances informáticos y las libertades informáticas redimensionadas, han puesto en jaque al derecho a la intimidad y obligado a una serie de replanteos en atención al riesgo que para la persona significa la generación de grandes bancos de datos y el entrecruzamiento de la información, esto último, logrado a partir del desarrollo de la telemática, es decir, "la exponencial combinación entre la tecnología de la informática y las telecomunicaciones, que ha permitido no sólo concentrar y recuperar información sino además, entrecruzar la información que sobre una persona existe en bancos de datos de diferente naturaleza, permitiendo estructurar perfiles de personalidad que superan los datos que sobre una persona se registran en cualquiera de las informaciones entrecruzadas".[23] Las posibilidades que brindan los desarrollos tecnológicos, han generado para quienes operan los datos posibilidades otrora inimaginables de poder tanto económico como político pues, el conocimiento de los perfiles de las personas permite regular, controlar, vigilar e inducir el comportamiento.[24]

En este punto estamos ante un posible conflicto entre los derechos de quienes operan los datos de carácter personal y el sujeto a quien refieren dichos datos. Los primeros se encuentran amparados para el manejo de datos por derechos constitucionales reconocidos que de modo más o menos directo tutelan dichas actividades, por ejemplo, los derechos a trabajar y ejercer el comercio, la inviolabilidad de papeles privados y, en términos generales, los derechos intelectuales. Estos derechos conforman un

[22] Fernández Sessarego, Carlos, *Derecho a la identidad personal*, Buenos Aires, Astrea, 1992, p. 163.

[23] Altmark y Molina Quiroga, Daniel Ricardo, y Molina Quiroga, Eduardo, *op. cit.*, nota 21, p. 1556.

[24] Sagüés, Néstor Pedro, en "Habeas Data: su desarrollo constitucional", en varios autores, *Lecturas andinas constitucionales*, núm. 3. Comisión Andina de Juristas, Perú, 1994.

"derecho informático" de base constitucional que da pie a las actividades reseñadas.[25]

Ese conjunto de derechos que amparan la labor de los operadores de datos, pueden entrar en colisión con los derechos constitucionales de las personas con cuyos datos cuentan, particularmente con el derecho a la intimidad, pensemos en una base de datos que acumule información referida a preferencias sexuales, religión, raza, etcétera. Hoy existe acuerdo en que datos del tipo de los enunciados no deberían estar en una base de datos, sea esta pública o privada por cualquier razón. Pero la cuestión es un poco más compleja pues se podría contestar desde el otro lado que, por ejemplo, la base de datos sobre portadores de VIH de tal hospital público debe contar con la información sobre la forma de contagio de cada uno de sus pacientes, o que la iglesia tal debe contar con un registro de sus feligreses para un mejor servicio parroquial, o que el instituto nacional de estadísticas debe contemplar el porcentaje de afro-americanos. Incluso ante datos en principio inofensivos podrían surgir objeciones, por ejemplo, pensemos en que la oficina de inteligencia del gobierno tiene una base de datos sobre los gustos literarios de sus habitantes. En principio las preferencias literarias resultan inofensivas por sí solas, pero llegaríamos a la conclusión contraria, tomando en cuenta el acopiador, si reconocemos que en América Latina durante los gobiernos dictatoriales, era suficiente el contar con un libro prohibido en las bibliotecas personales para ser objeto de persecución y aniquilación. Este breve ejercicio de problematización nos permite reconocer que ante el conflicto de derechos aquí presentado no existe respuesta sencilla. Sin embargo, el derecho ha dado algunas respuestas que permitirían arrojar cierta luz sobre este escenario de confusión.

[25] *Idem.*

IV. LAS RESPUESTAS DESDE EL DERECHO

Desde el derecho, amen de las regulaciones mencionadas, se han ofrecido algunas recetas para tutelar la privacidad de las personas. De entre ellas, nos interesa resaltar dos, la instalación en el discurso de los denominados "datos sensibles" y la creación de una garantía o mecanismo de carácter tuitivo que se ha desarrollado satisfactoriamente en América Latina durante los años noventa denominada "*Habeas Data*".[26]

1. Los datos sensibles

Dentro de la clasificación de los datos personales se suele distinguir entre aquellos datos que no afectan la sensibilidad de la persona de aquellos que la afectan. Los primeros, serían "aquellos que conforman información irrelevante o anodina que por sus características no permiten herir los sentimientos más íntimos de la persona ni afectan su derecho a la privacidad, se trata del dato rutinario, que se ofrece sin complicaciones o se obtiene de fuentes fácilmente accesibles".[27]

Los segundos, a los que se ha llamado datos sensibles "son aquellos que de difundirse ponen en conocimiento de quien los conoce datos de contenido privado que, salvo manifestación expresa del afectado, socavan la intimidad de la persona".[28]

Los datos sensibles son en general, aquellos referidos a la salud, condición racial y social, pensamientos, hábitos y costumbres de las personas y suelen ser agrupados en tres grupos:

1. Los datos sobre ideología, religión o creencia: que no pueden ser divulgados salvo autorización expresa del afec-

[26] Sagüés, Néstor Pedro, *op. cit.*, nota 24.

[27] Gozaini, Osvaldo Alfredo, Derecho procesal constitucional. Habeas Data. Protección de datos personales. *Doctrina y jurisprudencia*, Buenos Aires, Rubinzal Culzoni, 2001, p. 232.

[28] *Ibidem*, p. 233.

tado. No se admite la obligatoriedad en el suministro de esta clase de información.
2. Datos sobre el origen racial, la salud y la vida sexual.
3. Los datos sobre la historia de la persona entre los que destacan los referidos a infracciones administrativas, antecedentes penales y crediticios que admiten registro, pero sometidos a ciertas condiciones, especialmente temporales.[29]

Los datos mencionados pertenecen a una categoría especial pues con su reserva se atiende específicamente a la protección del derecho fundamental a la privacidad o intimidad personal. La catalogación de estos datos como sensibles implica dotarlos de cierto grado de protección que abarca desde la confidencialidad hasta la secrecía.

A primera vista puede parecer contradictorio establecer el secreto sobre ciertos datos evidentes como la raza, el color, el culto religioso o la simpatía política, que suelen ser practicados en actos públicos. Junto a esos datos, se encuentran otros que podrán ser secretos o públicos de acuerdo con lo que disponga el sujeto, por ejemplo, la preferencia sexual o el estado de salud. Sin embargo, se puede observar a simple vista que los datos sensibles conforman las razones que han motivado los actos más grandes de discriminación y persecución. La preservación de estos datos mediante la reserva, dejando la decisión sobre su divulgación exclusivamente en cabeza del sujeto activo, pretende dar cuenta de la nefasta utilización de la que pueden ser objeto y reforzar las vallas establecidas contra la discriminación. Al parecer, el que los actuales textos constitucionales contengan enérgicas proscripciones contra la discriminación por motivos de raza, religión, creencias, razones políticas o preferencias sexuales no es suficiente. Se necesita reforzar dicha proscripción con la imposibilidad de acopiar datos sensibles en bases de datos públicas o privadas como una estrategia antidiscriminatoria preventiva.

[29] *Ibidem*, p. 234.

Veamos como en diferentes ámbitos se ha regimentado la protección de la intimidad a través de la protección de los datos sensibles.

En Argentina, el artículo 7 de la ley 25.326 de Protección de datos personales establece: "Ninguna persona puede ser obligada a proporcionar datos sensibles. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la iglesia católica, las asociaciones religiosas y las organizaciones políticas y sindicales, podrán llevar un registro de sus miembros. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas". Obsérvese como el principio general es que la recolección de esta clase de datos sólo procede mediando consentimiento expreso del titular de los mismos. Por otro lado, la finalidad de la recolección se encuentra acotada por cuanto debe mediar un interés general que aunque concepto laxo, permite erradicar un número importante de otras finalidades. Por último y muy importante de resaltar, cuando esta clase de datos deba ser recolectada con fines estadísticos o científicos (finalidad de interés general que no excluye por supuesto el consentimiento del titular) deberán ser tratados como datos innominados es decir, sin referencia a la persona del titular.

En el ámbito europeo, la directiva 95/46 del 24/05/1995 sobre protección de personas físicas en el tratamiento de datos personales y libre circulación de datos ha establecido en su artículo 8: "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 datos relativos a la salud o a la sexualidad". La Directiva europea sobre protección de datos personales (Convenio 108 del Consejo de Europa) establece

en su artículo 5: "Les données à caractére personnel rélévant lorigine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les dones à caractère personnel relatives á la santé ou à la vie sexuelle, ne peuvent éter traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Ill en est de même des dones à dones à caractère personnel concernant des condamnations pénales".

España, mediante la Ley orgánica de tratamiento de datos estableció disposiciones referidas a los datos sensibles de singular importancia. Así, dispone su artículo 6.1 que el tratamiento automatizado de datos de carácter personal requerirá el consentimiento del afectado. En opinión de Fernández Segado, este consentimiento adquiere, ante los datos sensibles contornos reforzados pues ante ellos se requiere que el consentimiento sea prestado de manera expresa y por escrito, pero además, cuando los datos sensibles sean referidos a la raza, la salud y la vida sexual, su recopilación estará además sujeta a una habilitación especial. La LOTAR afirma el principio de no obligatoriedad respecto a la declaración de datos sensibles (principio también recogido por la ley argentina), en opinión del autor citado ello significa que al momento de proceder a recabar los datos, el particular debe ser advertido de que puede negarse a proporcionarlos.

Estas normas enunciadas a guisa de ejemplo demuestran la especial protección de la cual gozan hoy en día en el derecho comparado los datos sensibles. Al afirmar el principio de no obligatoriedad se reafirma, aunque con excepciones, por lo menos respecto a esta clase de datos, el derecho de autodeterminación informativa al cual nos referiremos más adelante.

Antes de dar por finalizada esta sección referida a datos sensibles, es necesario aclarar que el criterio que los distingue de los no sensibles tomando en cuenta el dato en sí y no su contexto o el parecer del sujeto a quien el dato refiere no resulta pacífico. En tal sentido, señala Puccinelli que existe cierto consenso respecto a aquellos datos que no serían en principio registrables, hablamos de los datos sensibles. Ellos conformarían lo que el autor

comentado denomina datos "objetivamente no registrables".[30] Junto a ellos, se encontrarían aquellos datos denominados en otra parte de este trabajo como datos anodinos que en principio podrían ser considerados "objetivamente registrables", pero estos datos, aun cuando no se refieran a información sensible, tomando en cuenta su potencial al ser manipulados por los operadores con las tecnologías disponibles para, por ejemplo, la determinación de perfiles del más diverso tipo, la calificación de objetivamente registrables se puede tambalear. Como se ha expresado, "información objetivamente registrable, almacenada y elaborada por determinados sujetos aun cuando no se refiera a la información sensible, puede llegar a desnudar casi cualquier aspecto de la vida de las personas haciendo ilusorias las garantías constitucionales".[31]

Amén de lo indicado, lo cierto es que el haber rodeado de especial protección a los datos sensibles, ha permitido a su vez, reforzar el marco de seguridad sobre el derecho fundamental a la intimidad y ésta ha sido una respuesta eficiente del derecho frente a la amenaza informática. En la última sección del presente trabajo analizaremos si la mediación del consentimiento del sujeto en el registro de un dato que haga a su persona en una base de datos puede ser también considerada para el registro de datos "no sensibles".

2. El Habeas Data

A. Su naturaleza. La problemática en la cual se inscribe

Los textos constitucionales actuales contemplan el derecho a la intimidad y a la privacidad y ello implica para los Estados una obligación negativa consistente en un no hacer, es decir, en no realizar acciones mediante las cuales vulnerar esos derechos im-

[30] Puccinelli, Óscar Raúl, *op. cit.*, nota 7, p. 921.
[31] Idem.

plica en definitiva una obligación de abstención. Pero, como observa Carlos Ayala Corao, ante la redefinición del papel del Estado a la luz del paradigma del Estado constitucional de derecho, las funciones ya no son las típicas del Estado liberal decimonónico es decir, no intervencionistas. El papel del Estado en el Estado constitucional se ha redefinido y su obligación de proteger los derechos fundamentales ya no sólo se cumple mediante labores de abstención, ahora se requiere el cumplimiento de obligaciones de carácter positivo tales como el establecer leyes tuitivas y poner a disposición del particular los medios y mecanismos necesarios para que el sujeto, en un papel activo, pueda actuar en defensa de sus derechos.[32]

Por otro lado, el derecho a la intimidad como separación entre el individuo y la sociedad, planteaba la idea de un sujeto aislado, en palabras de Fernández Segado, "en la actualidad, el derecho a la intimidad ya no implica solamente el derecho a negar información, sino el derecho a pretenderla. El derecho a la privacidad ya no es entendido en su fase negativa de rechazo de la intromisión ajena en la vida privada, por el contrario se reconoce a cada persona el ejercicio de un control sobre el uso que pueda hacerse de los propios datos personales recogidos en un archivo electrónico de un centro de proceso de datos. La libertad informática encierra en sí un derecho a la autotutela de la propia identidad informática, cuya primera exigencia es la protección de los datos informáticos personales frente a aquellas personas no autorizadas para conocerlos, procesarlos, modificarlos o difundirlos, razón por la que el primero de los contenidos cuya formación viene exigida por la efectividad de la nueva libertad es el acceso al banco de datos, con el fin de, por un lado, poder disponer de toda la información almacenada en un archivo elec-

[32] Ayala Corao, Carlos, "La legitimación del derecho a la autodeterminación en Venezuela. Derecho a la autodeterminación informativa y *Habeas Data* en Iberoamérica", en *Ius et Praxis. Derecho en la región*, Chile, Universidad de Talca, año 3, núm. 1, 1997, p. 153.

trónico sobre la propia personalidad y, por otro, poder rectificar ciertos datos concernientes a la misma".[33]

En la inteligencia de lo señalado por Fernández Segado se inscribe el proceso de *Habeas Data*, es decir, en el marco de la libertad informática que entonces no sólo se entroniza en cabeza de los operadores de datos sino también, en cabeza del titular de los datos y en virtud de la cual, los sujetos no sólo pueden impedir que ciertos datos no sean incorporados a una base de datos sino modificar o suprimir de dicha base los datos que no autorice almacenar. De esta forma, la libertad informática permite, en cierto sentido, actualizar los contenidos del derecho a la intimidad e identidad.

B. Concepto y finalidad primaria

La experiencia en materia del establecimiento de mecanismos tuitivos para la protección de los datos personales no ha sido uniforme. En Europa se ha recurrido al establecimiento de derechos y deberes a partir de leyes sobre tratamiento de datos personales y de acciones judiciales y administrativas. Estados Unidos ha generado acciones específicas más volcadas a la protección de la intimidad. En América Latina, se ha creado un verdadero proceso constitucional ya sea propio o derivado como una subespecie del amparo, el *Habeas Data*.

Así, *el Habeas Data* es un proceso judicial expedito cuyo principal y primario objeto es actualizar el derecho a la libertad informática, mediante el ejercicio del derecho a la información y que se manifiesta en una serie de derechos derivados que en opinión de Sagüés[34] pueden ser sistematizados de la siguiente manera:

- *Derecho de acceso*. El sujeto tiene derecho a saber qué información consta sobre él en un banco de datos.

[33] Fernández Segado, Francisco, *op. cit*., nota 3, p. 47.
[34] Sagüés, *op. cit*., nota 24, pp. 862-863.

- *Derecho a la actualización*. El sujeto tiene derecho a que los datos que consten sobre él en un banco de datos estén actualizados (Ej.: si aparece como deudor que se deje constancia sobre la liquidación de la deuda).
- *Derecho de rectificación*. El sujeto tiene derecho a que la información que conste sobre él en un banco de datos sea fiel y veraz.
- *Derecho a la confidencialidad*. El sujeto tiene derecho a que la información que haya proporcionado permanezca oculta para terceros.
- *Derecho de exclusión*. El sujeto tiene derecho a cancelar la información sensible que sobre él aparezca en una cierta base de datos.

C. Breves apuntes sobre su desarrollo en América Latina

El *Habeas Data* fue contemplado por primera vez y con dicho nombre en el ámbito latinoamericano en la Constitución de Brasil de 1988[35] al establecer su artículo 5: "Se concederá *Habeas Data*: a) para asegurar el conocimiento de informaciones relativas a la persona de quien lo pide, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público, b) para la rectificación de los datos cuando no se prefiera hacerlo en proceso reservado judicial o administrativo".

Colombia por su parte, incluyó este instituto en su Constitución a partir de la reforma de 1991 estableciendo su artículo 15: "Toda persona tiene el 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".[36]

[35] Eguiguren, P., Francisco J., "El Habeas Data" y su desarrollo en el Perú. Derecho a la autodeterminación informativa y Habeas Data en Iberoamérica", en Ius et Praxis Derecho en la región, Chile, Universidad de Talca, año 3, núm. 1, 1997, p. 122.

[36] Cifuentes Muños, Eduardo, "El Habeas Data en Colombia. Derecho a la autodeterminación informativa y Habeas Data en Iberoamérica", en Ius et Praxis. Derecho en la región, Chile, Universidad de Talca, año 3, núm. 1, 1997.

La República de Paraguay se inscribió en esta misma senda al contemplar el *Habeas Data* a nivel constitucional en su artículo 135 que determina: "Toda persona podrá tener acceso a la información y a los datos que sobre sí misma y 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. Podrán solicitar ante el magistrado competente, la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaren ilegítimamente sus derechos".[37]

La Constitución peruana integró la garantía constitucional del *Habeas data* en el año 1993 en su artículo 200 bajo el siguiente texto: "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 artículo 2, incisos 5, 6 y 7 de la Constitución".

La reforma constitucional realizada en Argentina en 1994, incorporó el proceso constitucional de *habeas data* como una subespecie de amparo en su artículo 43, en los siguientes términos: "Toda persona podrá interponer esta acción (amparo) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o 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 periodísticas".[38]

Venezuela no cuenta con texto expreso constitucional que contemple el *Habeas data*, sin embargo, dicho proceso fue incluido pretorianamente en el año 1994 y en virtud de la cláusula de numerus apertus que contiene el artículo 50 de su Constitución.[39]

[37] Eguiguren, P., Francisco, *op. cit.*, nota 35.

[38] Sagüés, Néstor Pedro, "*El Habeas Data en la Argentina*". Derecho a la autodeterminación informativa y Habeas Data en Iberoamérica", en *Ius et Praxis*. *Derecho en la región*, Chile, Universidad de Talca, año 3, núm. 1, 1997.

[39] Ayala Corao, Carlos, *op. cit.*, nota 32, p. 152.

D. Clases de *Habeas Data*

Líneas arriba, hacíamos mención a las diversas finalidades del *habeas data*. Pues bien, ellas han determinado la identificación de diversos tipos de *habeas data* de acuerdo con esas diferentes finalidades. Sagüés[40] identifica los siguientes tipos:

- *Habeas data informativo*. Su finalidad es sencillamente recabar datos, información obrante en archivos públicos o privados. El mismo admite tres subespecies: el *habeas data* exhibitorio cuya finalidad es tomar conocimiento del o los datos registrados; el *habeas data* finalista, mediante el cual se pretende tomar conocimiento acerca de por qué y para qué se encuentran registrados los datos; y por último, el *habeas data* autoral, por el que se procura averiguar la identidad del productor de los datos.
- *Habeas data aditivo o actualizador*. Su finalidad es lograr la completitud y actualización de los datos obrantes en un registro determinado. Este *habeas data* es necesario, por ejemplo, para actualizar las bases de datos de deudores, tomando en cuenta que los burós de créditos normalmente son renuentes a actualizar dicha información alegando razones de seguridad del crédito y de paso estigmatizan a un deudor que ya no es tal.
- *Habeas data rectificador*. Con él se persigue la eliminación de datos falsos.
- *Habeas data reservador*. Busca ordenar al titular del registro mantener la confidencialidad de los datos por cuanto su divulgación puede causar perjuicios al titular del mismo.
- *Habeas data cancelatorio*. Destinado a proteger la información sensible y persigue la eliminación de este tipo de información de los registros de datos.

[40] Sagüés, Néstor Pedro, "Subtipos de *Habeas Data*", Revista La Ley, Buenos Aires, 1995-IV, pp. 352-353.

E. Derechos protegidos

No siendo pacífica la doctrina en identificar los derechos fundamentales efectivamente protegidos por *el habeas data*, esbozaremos aquellos derechos que consideramos tutela y que en definitiva exceden el originario ámbito planteado de la intimidad informática.

En primer lugar, este instrumento protector pretende tutelar el derecho a la intimidad es decir, el derecho a preservar la esfera de la persona que debe quedar exenta del conocimiento generalizado de los demás. La intimidad se encontraría en el vértice de la protección pues a partir de las vulneraciones a la misma se pueden afectar otros derechos que a continuación mencionaremos.

El derecho a la identidad personal resulta también objeto de protección del *habeas data* por cuanto los datos registrados en la medida que versen sobre la persona tienden a identificar características de la identidad de cada uno. Los errores en dichos datos pueden ocasionar deformaciones en la identidad de los sujetos registrados, por ello, la posibilidad de corregir datos erróneos permite preservar la identidad del sujeto registrado.[41]

Es también objeto de protección, como decíamos líneas atrás, el derecho a la información, cuya garantía es necesaria como primer paso para el ejercicio de los demás derechos enunciados en esta sección.[42] Sobre este derecho se ha pronunciado el Tribunal Constitucional Español al afirmar: "la garantía de la intimidad adopta hoy un contenido positivo en forma del derecho al control sobre los datos relativos a la propia persona. La llamada li-

[41] *Cfr.* Puccineli, *op. cit.*, nota 7, p. 926. De acuerdo con el autor, el permitir accionar sobre datos falsos, se está protegiendo adicionalmente otros derechos tales como el honor, la reputación y la propia imagen que pueden afectarse por vía de falsedad.

[42] En tal sentido afirman Altmark y Molina Quiroga: "El objeto primario de la acción de habeas data sería entonces garantizar que una persona pueda tener acceso, es decir, tomar conocimiento o enterarse, de la información de carácter personal referida a dicho sujeto y contenida en determinado registro", *op. cit.*, nota 21, p. 1562.

bertad informativa es, así también, derecho a controlar el uso de los mismos datos insertos en un programa informático".[43]

Por último, el *habeas data* protege el derecho a la autodeterminación informativa, al cual nos referiremos en la última sección de este trabajo.

La protección de los datos sensibles como zona de reserva y el establecimiento de garantías para la protección de los datos personales han sido las dos principales aportaciones que la imaginación jurídica ha aportado para intentar amortiguar los efectos de la colisión entre desarrollo informático y, fundamental aunque no exclusivamente, los derechos fundamentales enunciados. Sin embargo, establecen contornos estrechos respecto a un nuevo derecho que se está perfilando desde ciertas legislaciones y sobre todo desde la labor de ciertos tribunales, se trata del derecho a la autodeterminación informativa.

V. EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA. A MODO DE CONCLUSIÓN

El derecho a la intimidad plantea la necesidad de mantener en reserva una serie de datos, concretamente los denominados sensibles, esto es, mantenerlos fuera del conocimiento y recolección y en caso de que hayan sido recolectados sin mediar las excepciones admitidas por los diversos ordenamientos, exigir su supresión del archivo en el cual se encuentren. El ámbito de total libertad quedaría circunscrito a dichos datos, en cuanto a lo demás, es decir, los datos considerados anodinos, parecería que el sujeto no tiene la fuerza suficiente como para vencer a los titulares de las bases de datos quienes legítimamente pueden esgrimir derechos tales como la libertad de trabajar, la propiedad sobre dichos datos, etcétera. Frente a esta situación, se erige el derecho a la autodeterminación informativa que consistiría en el reconocimiento al individuo de unas facultades de disposición y deci-

[43] Tribunal Constitucional Español. Sala Primera. Sentencia 254/1993.

sión respecto a sus propios datos personales. Este derecho, reconocería al sujeto la facultad de decidir cuándo y cómo está dispuesto a permitir que sea difundida su información personal o a difundirla él mismo. En tal sentido señala Herrán Ortiz, "mediante el derecho a la autodeterminación informativa no se protegen solamente los datos que se consideran sensibles, sino también aquellos que sin pertenecer a dicha esfera son susceptibles de daños a su imagen o al ejercicio pleno de sus derechos. Este nuevo derecho parte del principio de que ha de ser el sujeto quien decida qué datos pueden ser almacenados, por quién y para qué fines".[44]

Si tomamos en cuenta las reales posibilidades de la informática, nuestra tranquilidad en este tema no puede descansar exclusivamente en la prohibición de recolectar datos sensibles sin el consentimiento del sujeto. Como señala la autora citada, la información relativa al ocio, a los comercios, a la educación de los hijos, no son inocuas en lo que se refiere a la imagen externa de cada uno de nosotros. Dicha información, debidamente entrelazada, puede decir mucho acerca de una persona, sus gustos, apetitos, en definitiva su persona. La libertad irrestricta en el manejo de datos como los mencionados, tiende a generar una sociedad panóptica en la cual el sujeto es permanentemente observado, sus gustos registrados, conformando de ese modo el perfil del individuo que creo no existe razón comercial que pueda anteponerse al derecho de cada quien a preservar ese perfil dentro del ámbito público más estrecho posible. Quizá se nos permita cierta dosis de sutileza, el conocer los perfiles de conducta de las personas permite observar gustos, generarlos y marcar tendencias, lo cual resulta un modo elegante de denominar a la manipulación social. Esto nos genera ciertos interrogantes: ¿qué tan libre puede ser el desarrollo de la personalidad cuando sus elecciones obedecen a tendencias elaboradas con base en el conocimiento de los perfiles individuales y sociales?, o ¿qué grado de libertad se puede crear cuando las elecciones sociales, políti-

[44] Herrán Ortiz, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, Madrid, Dykinson, 1999, citado por Gozaíni, *op. cit*., nota 27, p. 107.

cas o económicas son impuestas previamente en virtud del conocimiento que sobre las preferencias o tendencias se tiene?

Lo que queremos sugerir en estas líneas es que la posibilidad de eliminar datos personales no debe quedar limitada exclusivamente a los datos sensibles. Aquí es donde el tradicional derecho a la intimidad resulta rebasado por el nuevo derecho a la autodeterminación informativa.

La propuesta a la luz de este nuevo derecho consistiría en que el ámbito de libertad informativa del sujeto no debería quedar circunscrita al fuero íntimo. Se trataría de hacer prevalecer la libertad informativa de cada individuo.

La Corte Constitucional Colombiana, en su sentencia SU-082 del 1o. de marzo de 1995 estableció: "el núcleo esencial del *habeas data* estriba en la defensa del derecho a la autodeterminación informativa, en cuya virtud la persona a la cual se refieren los datos que reposan en un archivo público o privado está facultada para autorizar su conservación, uso y circulación".[45]

Nótese la expresión utilizada por la Corte Constitucional, en su fallo no hace alusión a algún tipo específico de información sino a cualquier tipo de dato. Estas son las pretensiones del derecho a la autodeterminación informativa, total y absoluto control de la persona sobre los datos que a ella hacen, tanto respecto a bases públicas como privadas, que la decisión sobre la circulación de los datos sobre cada quien, repose en cada uno y que la publicidad de dichos datos sea una decisión propia y consentida de cada persona.

En este punto debemos establecer una distinción entre bases de datos públicas y privadas pues se requiere tratamiento diverso para ambas. Evidentemente y de manera especial en lo referido a bases de datos públicas o bajo control y vigilancia pública como las oficinas de crédito, registros penales, sanitarios, policiales, etcétera, el sujeto titular del dato no podrá disponer su no-inclusión en dicha base pero sí su rectificación o cancelación, pues existen ciertas razones de interés público que ameritan

[45] Eguiguren, P., Francisco, *op. cit*., nota 35, p. 7

ser atendidas, como la seguridad del comercio, la seguridad en general o la salubridad pública, entre otras. Estas bases públicas deberán ser establecidas previamente por ley, lo que implica forzar al Estado a expresar las razones, es decir, a justificar que dichos datos deben ser administrados y mediando la obligación de parte de la oficina pública respectiva de mantener la confidencialidad de los datos. Por supuesto, es de esperar que en ocasiones, las razones expresadas no sean necesariamente atendibles o razonables. El aceptar esto implica admitir que el derecho a la autodeterminación informativa tendría límites como todo derecho, límites establecidos en aras de la protección de otros bienes jurídicos considerados valiosos e, insistimos, mediante ley, límites que obedecen a razones fuertes y que serán ejercidos dentro de ciertos parámetros como los enunciados. El Tribunal Constitucional Español, en la sentencia 254/1993, estableció límites para las bases de datos públicas y consiguientemente amplió los límites de ejercicio del derecho a la autodeterminación informativa al sostener: "Si, como acepta dialécticamente en sus alegaciones, el derecho fundamental a la intimidad puede justificar en determinados casos que un ciudadano se niegue a suministrar a las autoridades determinados datos personales, no se ve la razón por la que no podría justificar igualmente que ese mismo ciudadano se oponga a que esos mismos datos sean conservados una vez satisfecho o desaparecido el legítimo fin que justificó su obtención por parte de la administración, o a que sean utilizados o difundidos para fines distintos y aun ilegales o fraudulentos o incluso a que estos datos personales que tiene derecho a negar a la administración. Toda información que las administraciones públicas recogen y archivan ha de ser necesaria para el ejercicio de las potestades que les atribuye la ley y ha de ser adecuada para las legítimas finalidades previstas por ella".[46] Como se puede apreciar, en el caso de las bases de datos públicas, los límites existen y provienen de la autodeterminación informativa. Amén de lo dicho, no negaremos que respecto a las bases de datos pú-

[46] Tribunal Constitucional Español, Sala Primera. Sentencia 254/1993

blicas se plantean grandes dificultades en torno al equilibrio entre fines sociales y libertades personales que Amitai Etzioni expresa de la siguiente manera: "Behind these observations, lies the assumption that good societies carefully balance individual rights and social responsabilities, autonomy and the common good, privacy and concerns for public safety and public health, rather than allow one value or principle to dominate. Ones we accept the concept of balance, the question arises as to how we are to determine whether our polity is off balance and in what direction it needs to move, and to what extent, to restore balance".[47]

La cuestión es diferente respecto a las bases privadas. En primer lugar, no encontramos a simple vista causas que justifiquen en grado superlativo la recolección de datos por parte de bases privadas como las existentes para justificar la existencia de bases públicas. Se suele argumentar que las bases privadas ayudan, entre otras cosas, al desarrollo del comercio y evidentemente nadie puede dudar de ello, sin embargo, en este punto se actualiza con toda fuerza la necesidad del consentimiento del titular de los datos que es la persona sobre quien versan los datos. Si la autodeterminación informativa puede, aunque con limitaciones, ser antepuesta frente a las bases públicas, debe retomar toda su fuerza frente a las bases privadas. Es decir, creemos que es el propio sujeto titular de los datos quien debe decidir en qué circuito comercial quiere ser incluido.

Las cuestiones expuestas nos permitirían vislumbrar el siguiente panorama. La recolección de datos es permitida para fines lícitos, es decir, permitidos por el ordenamiento jurídico y en segundo lugar su recolección sólo puede tener lugar mediando consentimiento del titular de los datos o autorización de la ley. A partir de aquí, se desprenden una serie de obligaciones para los administradores de las bases de datos que van desde el tratamiento y custodia responsable, pasando por la confidencialidad, el secreto absoluto y la obligación de indemnizar al sujeto titular

[47] Etzioni, Amitai, The Limits of Privacy, Basic Books, 1999, p. 184.

de los datos en caso de incurrir en violaciones a la intimidad o incluso, proponemos, por la obtención de beneficios económicos por la utilización de datos sin el consentimiento del titular de los mismos.

Derecho de autodeterminación informativa y consentimiento del sujeto se encuentran inextricablemente unidos. Cualquier sistema de protección de datos personales debe, en nuestra opinión, contener este derecho si la pretensión es realmente proteger. La no-aceptación de este derecho volverá ilusoria la preservación de los ámbitos de libertad personal ante las nuevas tecnologías de acopio y procesamiento de información.