Parte III

1144 blanca

Capítulo XII

La protección de datos personales y el proceso constitucional de *habeas data*

Sección 1ª Antecedentes

314. Introducción. Evolución legislativa

314.1. La protección de datos personales es una manifestación novedosa entre los procesos constitucionales. Muchos consideran que se debe a que multiplica las facetas de la intimidad que deben ser resguardadas de la invasión informática que, por su fuerte impacto en la vida privada, necesita de herramientas efectivas que se apoyen en fundamentos constitucionales.

> La preocupación, en los términos actuales, por la intimidad es el resultado de un largo proceso histórico de transformación de la conciencia que comienza con la contrarreforma, pasa por la desvalorización de la conciencia religiosa por los filósofos del siglo XVII (Hobbes, Locke, Descartes, Spinoza) y desemboca en la construcción de la conciencia moral, preparada por Thomasius y concluida por Kant. Con éste la libertad del hombre es la que permite enjuiciar por sí mismo sus acciones y determinar su voluntad a partir de una inclinación a la moralidad que le es innata. Sobre esta concepción del hombre —dice Juan Manuel Fernández López— adquiere sentido la noción actual de intimidad como atributo necesario de su nuevo *status* de libertad-autonomía. La dualidad de la persona (interioridad y socialidad) se traslada a la intimidad que es bidireccional: *ad se* y *ad alteros*. La intimidad si bien hace referencia primariamente a un espacio propio, privativo del individuo, éste solo adquiere su pleno sentido frente a los otros, tanto para oponerlo a ellos como para compartirlo con los demás. Así, la intimidad es simultáneamente condición de la personalidad individual y de la personalidad social.[1]

La tendencia comienza predominantemente en Europa cuando en los años setenta (1970) se dictan las primeras reglamentaciones que procuran dar un régimen al avance tecnológico, que si bien ofrecía un notable despliegue económico y social, también reflejaba un potencial peligro para los derechos de los ciudadanos, principalmente, para aquellos derechos más ligados a la personalidad y dignidad de las personas.

---

[1] Fernández López, Juan Manuel, *El derecho a la privacidad y su frontera en los demás derechos humanos,* en XX Conferencia Internacional de Autoridades de Protección de Datos (1998), Agencia de Protección de Datos, Madrid, p. 133.

En un primer período, cuando el número y costos asociados al funcionamiento de equipamiento computacional suponían su empleo sólo por grandes reparticiones públicas, tiene lugar la promulgación de la primera legislación en la materia. Así, en 1970 se promulga la *Datenschutz,* ley sobre tratamiento de datos personales del Land de Hesse, en la República Federal de Alemania, mediante la cual se pretendía brindar protección a las personas naturales ante la amenaza que representaba el tratamiento informatizado de datos nominativos por las autoridades y administraciones públicas del Estado, los municipios y entidades locales rurales, así como las demás personas jurídicas de derecho público y agrupaciones sujetas a la tutela estatal.

Con posterioridad, cuando ya se contaba con una serie de disposiciones federales y territoriales que regulaban el tema, con pretensiones de generalidad o cierta especificidad, se dicta la Ley Federal de Protección de Datos de la República Federal Alemana de 1977, en la cual se establece una normativa general relativa al tratamiento de datos personales, sea que él se verificara en el sector público o privado.

También responde a este período la *Data Lag 1973/289*, por la cual Suecia imponía un sistema de registro abierto para publicitar los bancos de datos personales relativo a personas físicas realizado por medios automatizados, los que debían ser previamente autorizados para funcionar, asociado a una autoridad de control —la *Datainspektionen*, expresión del *Ombudsman* proyectado al tratamiento de datos— que vela por el respeto de la ley, con facultades inspectoras, normativas y procesales para requerir la aplicación judicial de sanciones.

[…] Después surge la *Loi n.º 78-17 du janvier, relative à l'informatique, aux fichiers et aux libertés,* adoptada en Francia en 1978 que reglamenta el tratamiento automatizado de datos personales referidos a personas físicas realizado por personas naturales o jurídicas de derecho público y privado, si bien admite la aplicación parcial de sus disposiciones al tratamiento mecanográfico de datos nominativos. Asimismo, la ley prevé un órgano de control representativo e interpoderes, la *Commission Nationale de l'Informatique et des Libertés,* encargada de velar por su aplicación, recibir las reclamaciones de los afectados y dotado de potestad reglamentaria, cuyo ejercicio ha garantizado la perdurabilidad normativa.[2]

El 23 de setiembre de 1980 se explana el antecedente más importante para actuar sobre los datos personales, cuando la *Organización para la Cooperación y el Desarrollo Económicos (OCDE)*, organismo multilateral que ha elaborado importantes lineamientos y políticas sobre privacidad y protección de datos, emite la *Recomendación sobre flujo internacional de datos*, que produce un notorio empuje normativo en orden a regulaciones sucesivas.

La recomendación contiene ocho (8) principios complementarios de cuidado nacional y cuatro (4) de aplicación internacional que son considerados como los estándares mínimos a seguir para la obtención, el procesamiento de datos y el libre flujo transfronterizo de datos para los sectores público y privado.

Los ocho (8) principios de aplicación a nivel nacional son los siguientes:

---

[2] CERDA SILVA, Alberto, "Mecanismos de control en la protección de datos en Europa", *Revista Ius et Praxis*, 12 (2), Talca, 2006, pp. 221/251.

1. *El principio de "límite de obtención*", consistente en la imposición de límites para la recopilación de datos personales a través de medios apropiados y legales haciéndolo del conocimiento y obteniendo el consentimiento.

2. El principio de "*calidad de los datos*", que establece la importancia de asegurar la exactitud, totalidad y actualización de los datos.

3. El principio del "*propósito de descripción*", que resuelve especificar el fin de recabar información en el momento en el que se lleva a cabo la recolección y el subsecuente uso limitado del cumplimiento de dichos propósitos u otros que no sean incompatibles con aquellos propósitos especificados en cada ocasión.

4. El principio del "*límite de uso*", relativo a no divulgar los datos personales o aquellos utilizados para propósitos distintos a los contemplados en el principio anterior, a excepción de que haya consentimiento, o autorización otorgada por una autoridad contemplada en ley.

5. El principio de "*protección a la seguridad*", referido a proteger los datos personales e información, mediante mecanismos razonables de seguridad en contra de riesgos tales como pérdida, acceso no autorizado, destrucción, utilización, modificación o divulgación de datos.

6. El principio de "*imparcialidad*", vinculado con el establecimiento de políticas generales de imparcialidad sobre desarrollos, prácticas y propósitos con respecto a los datos personales, asegurando la transparencia en el proceso de obtención de información y estableciendo los propósitos para su utilización.

7. El principio de "*participación individual*", con respecto al derecho que tiene un individuo de obtener del controlador de datos la confirmación de tener o no los datos del individuo; que el controlador de datos se lo haya comunicado en un tiempo y forma.[3]

314.2. El quince (15) de diciembre de 1989 la Asamblea General de Naciones Unidas dicta la Resolución 44/132 donde atiende la decisión de la Comisión de Derechos Humanos del 6 de marzo de 1989, y la resolución 1989/78 del Consejo Económico y Social titulada "*Principios rectores sobre la utilización de ficheros computarizados de datos personales*".

De la resolución se desprende el proyecto de estudiar y concretar un sistema de protección integral sobre datos de las personas.

PRINCIPIOS RECTORES PARA LA REGLAMENTACIÓN
DE LOS FICHEROS COMPUTADORIZADOS DE DATOS PERSONALES

Las modalidades de aplicación de los reglamentos relativos a los ficheros computadorizados de datos personales se dejan a la libre iniciativa de cada Estado con sujeción a las siguientes orientaciones:

---

[3] VELASCO SAN MARTÍN, Cristos, "Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México?", *Boletín de Política Informática*, nº 1, México, 2003, pp. 1 y ss.

A. PRINCIPIOS RELATIVOS A LAS GARANTÍAS MÍNIMAS QUE DEBERÍAN PREVERSE EN LA LEGISLACIÓN NACIONAL

1. *Principio de la licitud y lealtad*

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

2. *Principio de exactitud*

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

3. *Principio de finalidad*

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

4. *Principio de acceso de la persona interesada*

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

5. *Principio de no discriminación*

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

6. *Facultad de establecer excepciones*

Sólo pueden autorizarse excepciones a los principios 1 a 4 si son necesarias para proteger la seguridad nacional, el orden público, la salud o la moral pública y, en particular, los derechos y libertades de los demás, especialmente de personas perseguidas (cláusula humanitaria), a reserva de que estas excepciones se hayan previsto expresamente por la ley o por una reglamentación equivalente, adoptada de conformidad con el sistema

jurídico nacional, en que se definan expresamente los límites y se establezcan las garantías apropiadas.

Las excepciones al principio 5, relativo a la prohibición de discriminación, deberían estar sujetas a las mismas garantías que las previstas para las excepciones a los principios 1 a 4 y sólo podrían autorizarse dentro de los límites previstos por la Carta Internacional de Derechos Humanos y demás instrumentos pertinentes en materia de protección de los derechos y de lucha contra la discriminación.

7. *Principio de seguridad*

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

8. *Control y sanciones*

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

9. *Flujo de datos a través de las fronteras*

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

10. *Campo de aplicación*

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

El 8 de marzo de 1995, la Comisión de Derechos Humanos, refiriéndose a los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales, que se aprobaron por la Asamblea General en su resolución 45/95, de 14 de diciembre de 1990, decidió lo siguiente:

a) Pedir a los Estados y a las organizaciones intergubernamentales, regionales y no gubernamentales que cooperen plenamente con el Secretario General proporcionándole todas las informaciones pertinentes relativas a la aplicación de los principios rectores;

b) Pedir al Secretario General que continúe velando por la aplicación de los principios rectores en el seno del sistema de las Naciones Unidas;

c) Pedir al Secretario General que informe a la Comisión en su 53º período de sesiones acerca de:

i) La aplicación de los principios rectores en el seno del sistema de las Naciones Unidas;

ii) Las informaciones recibidas de los Estados y de las organizaciones intergubernamentales, regionales y no gubernamentales acerca de la aplicación de los principios rectores en los planos nacional y regional.

Con arreglo a esa decisión, el 6 de junio de 1996 el Secretario General transmitió solicitudes a los órganos, organismos, comisiones regionales, organismos especializados y organizaciones afines de las Naciones Unidas para que facilitasen información sobre la aplicación de los principios rectores dentro de las secciones correspondientes del sistema de las Naciones Unidas. Igual requerimiento se realizó a cada uno de los Estados y organizaciones intergubernamentales y no gubernamentales.

314.3. En Europa, el 28 de Enero de 1981 los Estados miembros del Consejo de Europa, suscriben *el Convenio 108*, considerando deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, y concretamente, el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados.

El convenio resuelve calificar como "datos de carácter personal", a cualquier información relativa a una persona física identificada o identificable (persona concernida). Interpreta como "fichero automatizado", el conjunto de informaciones que sea objeto de un tratamiento automatizado; y por éste entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: *a)* registro de datos, *b)* aplicación a esos datos de operaciones lógicas aritméticas, y *c)* su modificación, borrado, extracción o difusión.

También califica como autoridad "controladora del fichero" a la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.

314.4. El Convenio comenzó a aplicarse y la presión de los organismos internacionales dieron lugar a requerimientos de la ONU que permitieron obtener un cuadro de situación internacional sobre la materia. Al 10 de diciembre de 1996, se habían recibido respuestas de los siguientes órganos, organismos y organismos especializados de las Naciones Unidas: División de Prevención del Delito y Justicia Penal, Departamento de Asuntos Humanitarios, Comisión Económica para Europa, Comisión Económica para América Latina y el Caribe, Programa de las Naciones Unidas para

el Medio Ambiente, Fondo de Población de las Naciones Unidas, Programa Mundial de Alimentos, Organismo Internacional de Energía Atómica, Organización Internacional del Trabajo, Fondo Monetario Internacional, Unión Internacional de Telecomunicaciones y Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

También habían presentado información los gobiernos de los siguientes países: Alemania, Argentina, Austria, Croacia, Estonia, Filipinas, Jamahiriya Arabe Libia, Luxemburgo, Mauricio, México, Reino Unido de Gran Bretaña e Irlanda del Norte, San Marino, Suecia y Uruguay.

> De los 33 órganos, organismos, comisiones regionales, organismos especializados y organizaciones conexas de las Naciones Unidas a las que se dirigió la solicitud, sólo han respondido 12. El Departamento de Asuntos Humanitarios, la Comisión Económica para América Latina y el Caribe y la Unión Internacional de Telecomunicaciones afirmaron que no tenían información pertinente que transmitir ni observaciones que formular en relación con la cuestión.
>
> La Comisión Económica para Europa afirmó que en ella no había actividad alguna a la que pudieran aplicarse las decisiones de la Comisión de Derechos Humanos en esta esfera, pues los archivos estadísticos de la Comisión eran anónimos o constaban de datos agregados.
>
> El Programa de las Naciones Unidas para el Medio Ambiente indicó que su práctica era conforme a las disposiciones contenidas en los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales.
>
> El Organismo Internacional de Energía Atómica afirmó que las disposiciones contenidas en la sección 8 de su Manual Administrativo que trata de la protección de la información confidencial sobre el personal, se ajustaban a los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales aprobados por la Asamblea General. El Fondo Monetario Internacional (FMI) indicó también que los procedimientos relativos al acceso a los ficheros de datos personales en el FMI parecían ajustarse a los principios rectores. La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura confirmó que estaba aplicando los principios rectores en el mantenimiento de ficheros de datos personales.

314.5. El informe de Argentina, efectuado en el año 1996, sostuvo que

> […] a partir de la reforma constitucional que tuvo lugar en agosto de 1994, la Carta Magna incluye, en su artículo 43, párrafo 3º, la acción de amparo en relación con la toma de conocimiento por parte de cualquier persona, sobre datos referidos a ella, que consten en registros o bancos de datos públicos o privados, destinados a proveer informes, y en caso de falsedad de los mismos o cualquier forma de discriminación que de ellos se desprenda, para exigir su supresión, rectificación, confidencialidad o actualización, así como también para conocer la finalidad para la cual han sido recabados.
>
> La norma constitucional mencionada responde en forma positiva a los principios rectores aprobados por la Asamblea General de las Naciones Unidas en su resolución 45/95 del 14 de diciembre de 1990 y a la decisión 1995/114 aprobada por la Comisión de Derechos Humanos el 8 de marzo de 1995. Entre los principios tomados como base para la norma constitucional, es importante destacar el de finalidad (expresado en el

párrafo 3º); el de acceso de la persona interesada (4º); el de no discriminación (5º); el de establecimiento de controles (8º); y el referido al campo de aplicación en registros públicos y privados (10º).

En lo que respecta a la actividad legislativa en esta materia, se han presentado al Congreso Nacional 18 proyectos de ley, de los cuales, a la fecha, sólo uno ha recibido media sanción, por la Cámara de Diputados del Congreso de la Nación en la sesión del 5 de junio de 1996. Dicho proyecto recoge los principios rectores de manera total, estableciendo excepciones a su aplicación de conformidad con las directrices fijadas en su párrafo 6º. Por otra parte, establece de manera clara las definiciones a los conceptos tratados, para evitar discrepancias conceptuales que perjudiquen su plena aplicación y efectividad.

En cuanto a la autoridad de aplicación, el artículo 5 del proyecto crea, en el ámbito del Congreso Nacional, una Comisión Bicameral de Seguimiento de Protección de Datos, a los fines de posibilitar la salvaguarda y protección de los derechos tutelados por dicha ley.

Merece comentario el artículo 11 del proyecto de que se trata, que establece que determinados datos personales deberán estar especialmente protegidos: i) ideología, raza, religión, hábitos personales y comportamiento sexual; ii) estado de salud (a este respecto, el artículo 12 establece la excepción tendiente a suministrar la información pertinente a centros sanitarios y profesionales sobre personas que a ellos consulten o reciban tratamientos), situación patrimonial y obligaciones tributarias, salvo razones de interés general y por disposición legal o consentimiento del interesado; iii) datos relativos a procesos penales o infracciones administrativas, los cuales sólo podrán ser incluidos en registros o bancos de datos pertenecientes a las administraciones públicas competentes, siempre a través de sus respectivas normas reguladoras.

El proyecto dispone que los datos de carácter personal sólo podrán ser cedidos con el previo consentimiento por escrito del interesado —que podrá ser siempre revocado—, estableciendo a su vez, la sanción de nulidad de la cesión si no se desprende de ella con claridad la finalidad de la misma, (art. 15). El consentimiento del interesado no será requerido en los casos específicamente previstos por el proyecto y que atienden a razones de interés público como la eficaz administración de justicia y la salud pública general.

La transmisión de datos al extranjero, organismos internacionales o supranacionales, deberá gozar de la misma protección que los datos de carácter personal en el ámbito de la República. Los titulares de la información que se encuentran en los ficheros gozan de los siguientes derechos:

i) Impugnar los actos administrativos o decisiones privadas que tengan por único fundamento la valoración que de su persona se haga a partir del tratamiento de datos de carácter personal;

ii) Conocer la existencia de los registros o bancos de datos, su finalidad e identidad del responsable;

iii) Solicitar y obtener la información personal que figura en dichos registros o bancos de datos sin la exigencia de contraprestación alguna;

iv) Rectificar, eliminar y conservar los datos de carácter personal.

En relación con la tutela de los derechos, el proyecto prevé acción sumaria para establecer responsabilidad por daños o lesiones a los bienes o derechos del interesado causados como consecuencia de la información archivada y que deberá establecer una reparación bajo la forma de indemnización. La acción prevista se efectuará bajo el pro-

cedimiento sumario y no obstará a la interposición de la acción de amparo, prevista constitucionalmente y en consonancia con la Ley 16.986 (Ley de amparo federal), para la aplicación de la cual el Código Civil y Procesal de la Nación prevé en su artículo 321 la vía sumarísima para su tramitación.

Por su parte, el proyecto establece, para las personas responsables de los registros o bancos de datos —sin perjuicio de las responsabilidades emergentes de los daños y perjuicios ocasionados al afectado y de las sanciones penales a que hubieran dado lugar los delitos cometidos— las sanciones de apercibimiento, suspensión, multa, eliminación o clausura de los registros o bancos de datos, por parte del Defensor del Pueblo, quien, de acuerdo con la reglamentación a dictar por la Comisión Bicameral creada por la propia ley, será el órgano de aplicación.

De acuerdo al último artículo del proyecto que se comenta, se invita a las provincias a crear sus registros de bancos de datos provinciales y a establecer sus órganos de aplicación; sin perjuicio de ello, el proyecto dispone que la ausencia de reglamentación procesal en la materia no obstará a la tramitación de la acción sumarísima prevista en el artículo 43 de la Constitución Nacional.[4]

314.6. Europa tiene en cuenta el reclamo proveniente del organismo mundial y después de muchos avatares y resistencias, consigue sancionar por el Parlamento Europeo, la *Directiva 95/46* del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

CAPÍTULO I
Disposiciones generales

Artículo 1. *Objeto de la Directiva*

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.

Artículo 2. *Definiciones*

A efectos de la presente Directiva, se entenderá por:

a) "datos personales": toda información sobre una persona física idientificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda

[4] La información proporcionada corresponde al proyecto de Ley Nº 24.745 del año 1996 aprobado por ambas Cámaras, que fuera posteriormente vetado en forma total por el Poder Ejecutivo Nacional entonces a cargo del Dr. Carlos Saúl Menem, mediante el decreto 1616/96 del 23 de diciembre de ese año. En el mes de noviembre de 1998 el Honorable Senado de la Nación aprobó, con algunas modificaciones, un Proyecto de Ley similar a la otrora vetada ley 24.745. Girado a la Honorable Cámara de Diputados, el proyecto sufrió varios cambios aunque la mayoría de ellos no fueron aceptados por el Senado que, a excepción de una modificación incluida en el inciso 4 del artículo 6 y algunas reformas menores, insistiendo con su proyecto original, lo aprobó bajo el número 25.326 el 4 de octubre de 2000.

determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

b) "tratamiento de datos personales" ("tratamiento"): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

c) "fichero de datos personales" ("fichero"): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

d) "responsable del tratamiento": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;

e) "encargado del tratamiento": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;

f) "tercero": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;

g) "destinatario": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios;

h) "consentimiento del interesado": toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

Artículo 3. *Ámbito de aplicación*

1. Las disposiciones de la presente Directiva se aplicarán al tratamineto total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:

- efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;
- efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Artículo 4. *Derecho nacional aplicable*

1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;

c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

CAPÍTULO II
Condiciones generales para la licitud del tratamiento de datos personales

Artículo 5

Los Estados miembros precisarán, dentro de los límites de las disposiciones del presente capítulo, las condiciones en que son lícitos los tratamientos de datos personales.

SECCIÓN I
Principios relativos a la calidad de los datos

Artículo 6

1. Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;

b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas;

c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;

d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;

e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apro-

piadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.

SECCIÓN II

Principios relativos a la legitimación del tratamiento de datos

Artículo 7

Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca, o

b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o

c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

d) es necesario para proteger el interés vital del interesado, o

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

SECCIÓN III

Categorías especiales de tratamientos

Artículo 8. *Tratamiento de categorías especiales de datos*

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

2. Lo dispuesto en el apartado 1 no se aplicará cuando:

a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o

b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o

c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o

d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con

la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o

e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente público o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.

4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.

5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.

Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.

6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.

7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Artículo 9 Tratamiento de datos personales y libertad de expresión

En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.

SECCIÓN IV
Información del interesado

Artículo 10. *Información en caso de obtención de datos recabados del propio interesado*

Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

a) la identidad del responsable del tratamiento y, en su caso, de su representante;

b) los fines del tratamiento de que van a ser objeto los datos;

c) cualquier otra información tal como:

- los destinatarios o las categorías de destinatarios de los datos,
- el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,
- la existencia de derechos de acceso y rectificación de los datos que la conciernen,
- en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Artículo 11. *Información cuando los datos no han sido recabados del propio interesado*

1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello:

a) la identidad del responsable del tratamiento y, en su caso, de su representante;

b) los fines del tratamiento de que van a ser objeto los datos;

c) cualquier otra información tal como:

- las categorías de los datos de que se trate,
- los destinatarios o las categorías de destinatarios de los datos,
- la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas.

SECCIÓN V

Derecho de acceso del interesado a los datos

Artículo 12. *Derecho de acceso*

Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:

- la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;
- la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;
- el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;

b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra *b)*, si no resulta imposible o supone un esfuerzo desproporcionado.

SECCIÓN VI
Excepciones y limitaciones

Artículo 13. *Excepciones y limitaciones*

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras *c)*, *d)* y *e)*;

g) la protección del interesado o de los derechos y libertades de otras personas.

2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas.

SECCIÓN VII
Derecho de oposición del interesado

Artículo 14. *Derecho de oposición del interesado*

Los Estados miembros reconocerán al interesado el derecho a:

a) oponerse, al menos en los casos contemplados en las letras *e)* y *f)* del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento

destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra *b)*.

Artículo 15. *Decisiones individuales automatizadas*

1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o

b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

SECCIÓN VIII

Confidencialidad y seguridad del tratamiento

Artículo 16. *Confidencialidad del tratamiento*

Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal.

Artículo 17. *Seguridad del tratamiento*

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;
- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente.

SECCIÓN IX
Notificación

Artículo 18. *Obligación de notificación a la autoridad de control*

1. Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos.

2. Los Estados miembros podrán disponer la simplificación o la omisión de la notificación, sólo en los siguientes casos y con las siguientes condiciones:

- cuando, para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos y/o
- cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de los datos personales que tenga por cometido, en particular:
- hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,
- llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21, garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.

3. Los Estados miembros podrán disponer que no se aplique el apartado 1 a aquellos tratamientos cuya única finalidad sea la de llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté destinado a facilitar información al público y estén abiertos a la consulta por el público en general o por toda persona que pueda demostrar un interés legítimo.

4. Los Estados miembros podrán eximir de la obligación de notificación o disponer una simplificación de la misma respecto de los tratamientos a que se refiere la letra *d)* del apartado 2 del artículo 8.

5. Los Estados miembros podrán disponer que los tratamientos no automatizados de datos de carácter personal o algunos de ellos sean notificados eventualmente de una forma simplificada.

Artículo 19. *Contenido de la notificación*

1. Los Estados miembros determinarán la información que debe figurar en la notificación, que será como mínimo:

a) el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante;

b) el o los objetivos del tratamiento;

c) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento;

d) los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos;

e) las transferencias de datos previstas a países terceros;

f) una descripción general que permita evaluar de modo preliminar si las medidas adoptadas en aplicación del artículo 17 resultan adecuadas para garantizar la seguridad del tratamiento.

2. Los Estados miembros precisarán los procedimientos por los que se notificarán a la autoridad de control las modificaciones que afecten a la información contemplada en el apartado 1.

Artículo 20. *Controles previos*

1. Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes del comienzo del tratamiento.

2. Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá consultar a la autoridad de control.

3. Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías.

Artículo 21. *Publicidad de los tratamientos*

1. Los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos.

2. Los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18.

En el registro se harán constar, como mínimo, las informaciones a las que se refieren las letras *a)* a *e)* del apartado 1 del artículo 19.

El registro podrá ser consultado por cualquier persona.

3. Los Estados miembros dispondrán, en lo que respecta a los tratamientos no sometidos a notificación, que los responsables del tratamiento u otro órgano designado por los Estados miembros comuniquen, en la forma adecuada, a toda persona que lo solicite, al menos las informaciones a que se refieren las letras *a)* a *e)* del apartado 1 del artículo 19.

Los Estados miembros podrán establecer que esta disposición no se aplique a los tratamientos cuyo fin único sea llevar un registro, que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo.

CAPÍTULO III
Recursos judiciales, responsabilidad y sanciones

Artículo 22. *Recursos*

Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.

Artículo 23. *Responsabilidad*

1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.

2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Artículo 24. *Sanciones*

Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva.

CAPÍTULO IV
Transferencia de datos personales a países terceros

Artículo 25. *Principios*

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.

4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las

medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Artículo 26. *Excepciones*

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaren su oposición y la justificaren debidamente por motivos derivados de la protección de la vida privada y de los

derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

CAPÍTULO V
Códigos de conducta

Artículo 27

1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva.

2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales.

Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.

3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo.

CAPÍTULO VI
Autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales

Artículo 28. *Autoridad de control*

1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.

Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.

2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.

3. La autoridad de control dispondrá, en particular, de:

- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;
- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;
- capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.

5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.

6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.

Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil.

7. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso.

Artículo 29. *Grupo de protección de las personas en lo que respecta al tratamiento de datos personales*

1. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado "Grupo".

Dicho Grupo tendrá carácter consultivo e independiente.

2. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o

autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión.

Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente. Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios.

3. El Grupo tomará sus decisiones por mayoría simple de los representantes de las autoridades de control.

4. El Grupo elegirá a su presidente. El mandato del presidente tendrá una duración de dos años. El mandato será renovable.

5. La Comisión desempeñará las funciones de secretaría del Grupo.

6. El Grupo aprobará su reglamento interno.

7. El Grupo examinará los asuntos incluidos en el orden del día por su presidente, bien por iniciativa de éste, bien previa solicitud de un representante de las autoridades de control, bien a solicitud de la Comisión.

Artículo 30

1. El Grupo tendrá por cometido:

a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;

b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;

c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;

d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

2. Si el Grupo comprobare la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión.

3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad.

4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión y al Comité contemplado en el artículo 31.

5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado.

6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado.

CAPÍTULO VII
Medidas de ejecución comunitarias

Artículo 31. *El Comité*

1. La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

2. El representante de la Comisión presentará al Comité un proyecto de las medidas que se hayan de adoptar. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate.

El dictamen se emitirá según la mayoría prevista en el apartado 2 del artículo 148 del Tratado. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán del modo establecido en el artículo anteriormente citado. El presidente no tomará parte en la votación.

La Comisión adoptará las medidas que serán de aplicación inmediata. Sin embargo, si dichas medidas no fueren conformes al dictamen del Comité, habrán de ser comunicadas sin demora por la Comisión al Consejo. En este caso:

- la Comisión aplazará la aplicación de las medidas que ha decidido por un período de tres meses a partir de la fecha de dicha comunicación;
- el Consejo, actuando por mayoría cualificada, podrá adoptar una decisión diferente dentro del plazo de tiempo mencionado en el primer guión.

DISPOSICIONES FINALES

Artículo 32

1. Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, a más tardar al final de un período de tres años a partir de su adopción.

Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros velarán por que todo tratamiento ya iniciado en la fecha de entrada en vigor de las disposiciones de Derecho nacional adoptadas en virtud de la presente Directiva se ajuste a dichas disposiciones dentro de un plazo de tres años a partir de dicha fecha.

No obstante lo dispuesto en el párrafo primero, los Estados miembros podrán establecer que el tratamiento de datos que ya se encuentren incluidos en ficheros manuales en la fecha de entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva, deba ajustarse a lo dispuesto en los artículos 6, 7 y 8 en un plazo de doce años a partir de la adopción de la misma. No obstante, los Estados miembros otorgarán al interesado, previa solicitud y, en particular, en el ejercicio de su derecho de acceso, el derecho a que se rectifiquen, supriman o bloqueen los datos incompletos, inexactos o que hayan sido conservados de forma incompatible con los fines legítimos perseguidos por el responsable del tratamiento.

3. No obstante lo dispuesto en el apartado 2, los Estados miembros podrán disponer, con sujeción a las garantías adecuadas, que los datos conservados únicamente a efectos de investigación histórica no deban ajustarse a lo dispuesto en los artículos 6, 7 y 8 de la presente Directiva.

4. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 33

La Comisión presentará al Consejo y al Parlamento Europeo periódicamente y por primera vez en un plazo de tres años a partir de la fecha mencionada en el apartado 1 del artículo 32 un informe sobre la aplicación de la presente Directiva, acompañado, en su caso, de las oportunas propuestas de modificación. Dicho informe será publicado.

La Comisión estudiará, en particular, la aplicación de la presente Directiva al tratamiento de datos que consistan en sonidos e imágenes relativos a personas físicas y presentará las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información.

Artículo 34

Los destinatarios de la presente Directiva serán los Estados miembros.

314.7. La Directiva 95/46/CE establece condiciones generales de licitud en el tratamiento de los datos, en que amplia y detalla en diversos aspectos las previsiones del Convenio 108, dejando a los Estados miembros un margen de maniobra de que podrán servirse para precisar en el derecho interno tales condiciones. Al efecto, la Directiva impone plazo a los Estados miembros para la transposición de sus previsiones en el derecho interno.

La instrucción se circunscribe al tratamiento de datos personales correspondientes a personas naturales, excluyendo explícitamente de sus previsiones a las personas jurídicas, extiende sus prescripciones al tratamiento verificado por el sector público y privado, tanto por medios automáticos como manuales. A diferencia del Convenio 108, la Directiva amplia su protección a cualquier operación o conjunto de operaciones aplicadas a datos personales, desde el instante mismo de su recogida. Asimismo, la Directiva innova introduciendo normas para dirimir los conflictos de legislación originados en la materia, haciendo prevalecer la ley del Estado en que se sitúa el establecimiento del responsable de tratamiento y, en su defecto, aquél en que se ubiquen los medios empleados.

Respecto de las condiciones generales de tratamiento, la Directiva insiste en la aplicación de principios relativos a la calidad de los datos, esta vez, a diferencia de cuanto acontecía con el Convenio 108, imponiendo a los responsables de tratamiento la obligación de cumplir con ellos; persiste en que la legitimidad del tratamiento de datos descansa en el consentimiento del interesado, aún cuando admite una extensa gama de excepciones a tal regla; tal cual el Convenio 108, contempla categorías especiales de tratamiento (datos sensibles), respecto de los cuales en principio aboga por su prohibición, si bien establece un sistema reglado de excepciones. En general, la Directiva, sin desconocer el principio del consentimiento, a juzgar por el número de sus excepciones, parece hacer descansar la rigurosidad del tratamiento en el respeto al principio de la finalidad, al cual acude con miras a circunscribir la legitimidad de las operaciones que recaen sobre los datos.

En cuanto a los derechos del interesado, regla el derecho a información, sea que los datos se recaben de él o de terceros, fijando el contenido mínimo de tal comunicación; reconoce el derecho de acceso al interesado, el que proyecta inclusive al conocimiento de la lógica que subyace al tratamiento automatizado de los datos que conciernen, resguardando el menoscabo al secreto de los negocios, la propiedad intelectual y los derechos de autor; de igual forma, reconoce los derechos de rectificación y cancelación, e incorpora los derechos de bloqueo y notificación a terceros a quienes se haya comunicado los datos ante la rectificación, supresión o bloqueo de los mismos; con todo, admite ciertas excepciones y limitaciones a los derechos de acceso e información, así como a determinadas obligaciones del responsable del tratamiento, si bien estableciendo cortapisas para las mismas.

Del mismo modo, reconoce el derecho del interesado a oponerse a ciertos tratamientos de datos que le conciernen y adiciona, al catálogo de derechos del interesado, la prohibición de que éste sea sometido a decisiones con efectos jurídicos fundadas únicamente en un tratamiento automatizado de sus datos, aún cuando con ciertos matices.

Con el propósito de asegurar la publicidad de los fines del tratamiento y de sus principales características, así como para efectos de fiscalización, establece procedimientos de notificación a la autoridad de control por el responsable de tratamiento, sin perjuicio de ciertas exenciones y simplificaciones, a la par de ciertos casos que hacen necesario un examen previo de la autoridad de control o del encargado de protección de los datos en cooperación con aquélla. Tales antecedentes, al igual que los códigos de conducta que se adopten, deben ser publicitados por la autoridad de control mediante un registro público de los tratamientos.

La Directiva impone a los Estados miembros la obligación de velar por el respeto de las medidas técnicas y de organización apropiadas para garantizar un nivel de seguridad adecuado de tratamiento, fijando pautas para su determinación. Asimismo, exige la adopción de un recurso judicial por las legislaciones nacionales, para hacer se respeten los derechos de los interesados conculcados por el responsable de tratamiento, sin perjuicio del recurso administrativo que pueda interponerse ante la autoridad de control.

Una de las preocupaciones centrales fue hacer frente a los riesgos aparejados al flujo transfronterizo de datos personales, admitiendo que tal transferencia se verifique con terceros países que garanticen un nivel de "protección adecuado", para lo cual había necesidad de apreciar todas las circunstancias relacionadas con la transmisión o la categoría de transmisiones. En caso contrario, esto es, tratándose de terceros países que no ofrezcan tal nivel de protección, se prohíbe la transferencia, salvo excepciones, entre las que contempla el ofrecimiento de garantías adecuadas por el responsable del tratamiento, para lo cual obliga a la adopción de procedimientos de negociación entre la Comunidad y los terceros países de que se trate.

Respecto de la autoridad de control, a diferencia de cuanto preveía el Convenio 108, la Directiva califica su creación en cada uno de los Estados miembros como elemento esencial en la protección de las personas frente al tratamiento de los datos

nominativos; exige que ella ejerza sus funciones con plena independencia; le atribuye facultades de investigación, intervención y capacidad procesal, cualquiera sean las disposiciones de derecho nacional aplicables. Con todo, admite el control judicial de sus actos y le impone la obligación de publicar sus informes periódicamente. Asimismo, insiste en la necesidad de que las autoridades de control de los Estados miembros se brinden ayuda mutua en el ejercicio de sus funciones.

Finalmente, la Directiva contempla la creación del Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, órgano comunitario de carácter consultivo e independiente, integrado por las autoridades de control nacionales, que asesorará a la Comisión y contribuirá a la aplicación uniforme de las normas nacionales adoptadas en aplicación de la Directiva.[5]

314.8. Casi en forma inmediata, la legislación europea se fue adaptando a estas nuevas reglas (Suecia, 1998; Inglaterra, 1999; España, 1999, entre otros). La evolución fue magnífica, al punto que el 28 de Enero del 2009, muchos países de Europa resolvieron celebrar *el día internacional de la protección de datos personales*.

En efecto, el Consejo de Europa, con el apoyo de la Comisión Europea crearon esta importante fecha hace tres años en homenaje al Convenio 108 del Consejo de Europa. El día también fue creado para concientizar a los ciudadanos "*de los riesgos inherentes y asociados con el manejo ilegal de nuestros datos personales*".

315. La evolución en Latinoamérica

315.1. La *Declaración Universal de los Derechos del Hombr*e de 1948 es la piedra fundamental para el seguimiento que hace Latinoamérica en su desarrollo legal y, esencialmente, constitucional.

"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (art. 12).

También la *Convención Americana sobre Derechos Humanos* de 1969, estableció en el art. 11 que:

> 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

El *Pacto Internacional de Derechos Civiles y Políticos* tuvo igual redacción en el artículo 17.

---

[5] CERDA SILVA, Alberto, "Autodeterminación informativa y leyes sobre protección de datos", *Revista Chilena de Derecho Informático*, nº 3, diciembre de 2003, pp. 26 y ss.

Desde estos preceptos se ha considerado que la protección dispensada asienta en el derecho a la intimidad y la vida privada, tomando a los datos personales como una faceta de ambos.

Por eso, en las reformas constitucionales habidas fueron suscitándose versiones de la acción de *habeas data* que fue adoptado como proceso constitucional específicamente previsto para la protección de los datos personales.

315.2 *Argentina*, por ejemplo, en la reforma de 1994 incorpora dentro del amparo (como derecho o garantía), el art. 43 cuyo párrafo tercero dice:

> Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística.

Varios años después se sancionó la ley 25.326 que trataremos oportunamente.

315.3. En *Bolivia* la Constitución de 1995 introdujo el recurso de *habeas data* (art. 23), después modificado por la ley 2410 del año 2002.

El esquema reglamentario dice:

> I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de *habeas data* ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.
>
> II. Si el tribunal o juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado.
>
> III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo.
>
> IV. El recurso de *habeas data* no procederá para levantar el secreto en materia de prensa.
>
> V. El recurso de *Habeas Data* se tramitará conforme al procedimiento establecido para el recurso de Amparo Constitucional previsto en el artículo 19º de esta Constitución.

315.4. *Brasil* en la Constitución de 1988 establece, en el artículo 5, incisos primero, tercero, cuarto (LXXII) y quinto (LXXVII), la "garantía" constitucional del *habeas data*, del siguiente modo:

> Todos son iguales ante la ley, sin distinción de cualquier naturaleza. Se garantiza a los brasileños y a los extranjeros residentes en el país a la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad, en los términos siguientes:
>
> XXXIII. Todos tendrán derecho a recibir de los órganos públicos informaciones de interés particular, o de interés colectivo o general, que serán entregadas en los términos

que establezca la ley, bajo pena de responsabilidad, excepto aquellas cuyo secreto fuere imprescindible para la seguridad de la sociedad y del Estado [...].

LXXII. Se concederá *habeas data*: *a)* para asegurar el conocimiento de informaciones relativas a la persona del impetrante, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; *b)* para rectificar datos, cuando no se prefiriera hacerlo por procedimiento secreto, judicial o administrativo.

LXXVII: 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. 1. 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 de Brasil sea parte".

315.5. En la Constitución de *Colombia* de 1991 el artículo 15 reglamenta como proceso constitucional al *habeas data*, aunque no lo denomina así, lo que denota una diferencia que consideramos en el capítulo siguiente respecto a cierta distancia entre la protección jurisdiccional y la defensa orgánica de los datos personales.

Dice la norma que "todas las personas [...] tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución".

Este precepto divide las aguas entre el derecho a la intimidad, y el derecho de las personas a estructurar bases de datos, pues no sólo prevé precisamente que el *habeas data* es un mecanismo para rectificar el contenido de dichas bases, sino que además esa disposición establece literalmente que *en la recolección, tratamiento y circulación* .

El *habeas data*, como tal, se incluye en el capítulo 1 del título II de la Constitución Política, en el que se enuncian los derechos fundamentales. Ubicación que le valió cierta crítica de la doctrina.

La Corte Constitucional se ha limitado a conferir a la ubicación de los derechos bajo el mencionado capítulo y epígrafe, un valor meramente ilustrativo o indicativo de la naturaleza de un determinado derecho —no enteramente conclusivo—, no se ha puesto jamás en duda que el *habeas data* ostente la condición de derecho fundamental. De otro lado, no deja de tener alguna significación que el artículo 15 de la CP, en el que se regula el *Habeas data*, se ocupe básicamente del derecho a la intimidad personal y familiar y de la inviolabilidad de la correspondencia, además de establecer una excepción a la reserva de documentos privados. De hecho, la Corte Constitucional, en un primer momento, no dudó en acomodar conceptualmente el *Habeas data* dentro del ámbito del derecho a la intimidad. En esa oportunidad se precisó que la intimidad se proyectaba en dos dimensiones: como secreto de la vida privada (sentido estricto) y como libertad (sentido amplio). La primera dimensión ofrecería la visión tradicional de la intimidad marcadamente individualista y portadora de facultades de exclusión de signo negativo. La segunda, conferiría a la intimidad el carácter de libertad pública y la habilitaría para enfrentar las amenazas que en el mundo moderno se ciernen sobre ella. Concluye la Corte: "[...] en las nuevas

condiciones creadas por la emergencia de sofisticadas tecnologías, la intimidad adquiere más y más objetiva naturaleza política como que apunta a lograr un justo equilibrio en la distribución del poder de la información y no exclusivamente, como en el pasado, a garantizar los apetitos de soledad de una persona".[6]

Pero en la sentencia de unificación jurisprudencial SU-082 del 1 de marzo de 1995, la Corte Constitucional le reconocerá autonomía como proceso, estableciendo que el ámbito de protección a dispensar se funda en el derecho a la "autodeterminación informática", 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.

En el año 2008 se dicta la Ley Estatutaria nº 1266 que singulariza la protección constitucional y la desarrolla, teniendo especialmente en cuenta, las bases financieras, crediticias, comerciales, de servicios y las provenientes de otros países.

La norma define claramente su objeto: desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales así como el derecho a la información establecido constitucionalmente, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

315.6. En *Ecuador* la protección de datos personales aparece por primera vez en la Constitución Política del año 1996, para posteriormente pasar a ser regulada por la Ley del Control Constitucional de 1997 y, tras las reformas constitucionales, se incorporó en la Carta Constitucional de 1998.[7]

Ésta, en el artículo 94 trata, al igual que en Colombia, dentro de un mismo precepto dos derechos similares: el de acceso a la información pública y privada y la garantía constitucional de *habeas data*.

Dice la norma:

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.

---

[6] CIFUENTES MUÑOZ, Eduardo, "El *habeas data* en Colombia", *Revista Ius et praxis*, nº 1, año 3, Talca, 1997, pp. 81/106.

[7] ALVEAR, Caros Salmón, "Régimen procesal del *habeas data* en Ecuador", R*evista Jurídica de Jurisprudencia, Ciencias Sociales y Políticas*, Universidad Católica de Santiago de Guayaquil, versión online.

No obstante, entre el derecho de acceso a la información, y la tutela que proporciona el *habeas data* hay diferencias fundamentales que anidan en la materia que se persigue o busca obtener; la relación entre el actor y la información que se solicita; la finalidad que se busca; las pretensiones posteriores al acceso que se podrían esgrimir; y, el requerimiento previo exigido como condición de admisibilidad.

> Así, respecto de la materia, el *habeas data* siempre buscará el acceso a la información privada o propia del accionante; mientras que el recurso de acceso a la información pública pretenderá aquella información que es de todos los ciudadanos y que se almacena principalmente en las instituciones públicas. Consecuencia de lo anterior es que en el *habeas data* hay una relación directa entre el actor y la información que se requiere; mientras que, en el recurso de acceso a la información pública aquella relación no es directa o propia, ya que no es una información personal la que se busca, sino del Estado, del municipio, de la localidad a la que uno pertenece. Sobre la finalidad perseguida, el recurso de acceso a la información pública pretende ejercitar una suerte de fiscalización a la actuación pública, logrando conocer en forma clara y transparente la gestión de las instituciones y sus autoridades, las cuales están sometidas al principio de publicidad y transparencia. En cambio, el *habeas data* no pretende fiscalizar dicha gestión pública, sino controlar que los datos personales que se tengan registrados respecto del proponente de la demanda sean correctos, actualizados y no le causen discriminación alguna. Así mismo, en el *habeas data*, tras la recepción de la información solicitada, el actor puede solicitar la actualización, la rectificación, la anulación y hasta la reserva de la información personal; mientras que en el recurso de acceso a la información pública aquellas pretensiones no pueden ser esgrimidas, puesto que el recurso se limita y agota simplemente con la entrega de la información pública al peticionario de la misma.[8]

En el año 2009 se publica en el Registro Oficial nº 52 la *Ley Orgánica de Garantías Jurisdiccionales y Control constitucional,* dándole autonomía a la acción de *habeas data* (Capítulo VI), para disponer:

> ART. 49. *Objeto.*—La acción de *habeas data* tiene por objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos.
>
> El titular de los datos podrá solicitar al responsable del archivo o banco de datos, el acceso sin costo a la información antes referida, así como la actualización de los datos, su rectificación, eliminación o anulación. No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos.
>
> Las personas responsables de los bancos o archivos de datos personales únicamente podrán difundir la información archivada con autorización del titular o de la ley.

---

[8] ALVEAR, Caros Salmón, "Régimen procesal del *habeas data* en Ecuador", R*evista Jurídica de Jurisprudencia, Ciencias Sociales y Políticas*, Universidad Católica de Santiago de Guayaquil, versión online.

Las presentes disposiciones son aplicables a los casos de rectificación a que están obligados los medios de comunicación, de conformidad con la Constitución.

El concepto de reparación integral incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación".

ART. 50. *Ámbito de protección*.—Se podrá interponer la acción de *habeas data* en los siguientes casos:

1. Cuando se niega el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o estén en poder de personas naturales o jurídicas privadas.

2. Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos.

3. Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente.

ART. 51. *Legitimación activa*.—Toda persona, natural o jurídica, por sus propios derechos o como representante legitimado para el efecto, podrá interponer una acción de *habeas data*.

315.7. Siguiendo en América del Sur, *Paraguay* tiene en la Constitución de 1992, reglamentado como "garantía constitucional" el derecho de acceso y tratamiento a la información pública y privada en el artículo 135, de la siguiente forma:

Toda persona puede acceder a la información y a los datos que sobre si misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

La disposición es, básicamente, una modalidad dentro del amparo constitucional, e históricamente sirvió para poder acceder a documentos públicos y privados de la época de la dictadura militar.

La novedad principal de la norma paraguaya radica en que no solo comprende dentro de la protección de este instituto los consabidos derechos personales como privacidad, no discriminación, reserva sobre convicciones políticas o religiosas; sino también derechos personales de índole patrimonial, referidos a información o datos sobre bienes.

Después se han sancionado leyes especiales, como la nº 1682 que reglamenta la información de carácter privado, otorgando el derecho a toda persona a recolectar, almacenar y procesar datos personales para uso estrictamente privado. Asimismo considera que las fuentes públicas de información son libres para todos (acceso a la información).

315.8. En *Perú* la Constitución de 1993 establece en el artículo 200 numeral 3º como garantía especial

[…] la acción de *habeas data*, diciendo que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2º sus incisos reglamentan que toda persona tiene derecho a: […]

5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

El secreto bancario y la reserva tributaria pueden levantarse a pedido del Juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado.

6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

7. Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley.

Del precepto constitucional se desprende un radio de acción bastante amplio, que alcanza una vasta comprensión de materias que van desde el derecho informático a la intimidad y vida privada de las personas.

No obstante, como en paralelo se reconoce el derecho de acceso a la información pública, se han impuesto limitaciones para resguardar la intimidad personal y la seguridad nacional.

Asimismo, el derecho al secreto bancario y a la reserva tributaria se reconoce implícitamente, aunque se mantienen impedimentos cuando es necesario preservar una investigación de interés público.

Cabe recordar que la garantía constitucional dispuesta en el art. 200, inc. 3 citado, fue puesta a referéndum en octubre de 1993, en razón de la disputa eventual que sufría con el derecho a la comunicación y la libertad de expresión.

Además, no es posible soslayar el impacto del *Código Procesal Constitucional (*ley nº 27237) que regula los procesos constitucionales de *habeas corpus*, amparo, *habeas data*, cumplimiento, inconstitucionalidad, acción popular y los conflictos de competencia, para los que se dan principios generales.

El proceso constitucional de *Habeas data*, está normado en los artículos 61º al 65º del referido ordenamiento.

315.9. En *Uruguay* y solo como dato referencial, el *habeas data* es un proceso nuevo que nace con el impulso de la legislación. Ella se regla en la ley 18.331, que en su art. 48, derogó la anterior nº 17.838 de 24 de setiembre de 2004.

En el año 2009 se reglamenta la ley del año anterior, y queda articulado un conjunto de derechos y obligaciones vinculados a la recolección y tratamiento, automatizados o manuales, de los datos de las personas físicas y jurídicas, cuya ordenación se armoniza con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos personales.

315.10. La Constitución de la República Bolivariana de *Venezuela* de 1999, en el artículo 28 reconoce el derecho fundamental de acceso a la información pública y privada, como la acción de *habeas data*, en los siguientes términos:

> Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley.

El derecho público venezolano, siguiendo la ola latinoamericana de constitucionalización de la garantía de *Habeas Data*, tal como lo había hecho previamente Colombia, Perú, Paraguay, Ecuador y Argentina, regula dicha garantía constitucional a través del derecho de acceso a la información y los datos que tiene una persona concernida sobre sí misma como sobre su información patrimonial o de "sus bienes" (tal como lo hace la Constitución de Honduras, Ecuador y Paraguay). Igualmente, a "conocer el uso que se haga de" la información o datos personales que le conciernen e incluso cuáles son los fines que mueven o generan esos usos; así como, toda persona concernida, tiene derecho a aquellas facultades del *habeas data* elevadas a rango constitucional de "actualización, rectificación o la destrucción de" los datos o informaciones concernidas, cuando aquellos "fuesen erróneos o" afecten "ilegítimamente sus derechos".[9]

315.11. Dejamos *ex professo* al final a Chile (solo para centrar en Sudamérica la evolución habida) con el fin de señalar con él cada una de las modalidades que tuvo el tratamiento de datos personales y la protección procesal que ofrece el *habeas data*.

En este país, no existe un derecho particular que atiende el impacto de la informática en la vida de las personas, aunque la ley 19.223 (1993) trató los delitos informáticos, pero dejó sin atender la invasión a la intimidad mediante el uso inadecuado de datos personales.

El 27 de octubre de 1999 entró en vigor la ley 19.628 sobre "Protección de la Vida Privada", que regula el tratamiento que los organismos públicos y los particulares efectúen de los datos de carácter personal que se encuentren almacenados en registros o bancos de datos, sean estos de carácter automatizado o no.

Se entiende por datos personales a "*los relativos a cualquier información concerniente a personas naturales, identificadas o identificables*", provocando cierta duda en orden a las evaluaciones o informes que se proporcionan por entidades destinadas a dar información.

El paso del tiempo y la aplicación concreta de la ley ha llevado a decir que:

> […] lamentablemente, demostrando una notable falta de sensibilidad con la tutela de los datos personales, afanando el transparentar por la obligación de resguardar la privacidad y olvidando hacer cumplir la ley 19.628 -lo que expresamente puso de su cargo el artículo 33 letra *m* de la ley 20.285-, el Consejo de Transparencia ha deslindado proteger la privacidad y ha obligado en sus Dictámenes (i) a entregar —pudiendo haberse negado—

---

[9] Riascos Gómez, Libardo Orlando, "La visión constitucional del *habeas data*", *Revista Informática Jurídica*, nº año 2009 (segundo semestre), versión online.

tanto los millones de antecedentes personales y sensibles registrados por el SERVEL como las calificaciones de cientos de funcionarios públicos ante un requerimiento presentado al MINVU y a FONASA, y (ii) a que los servicios públicos se transformen en productores de bases de datos personales para que los ciudadanos asuman tareas con fines de lucro —como es el caso de agentes inmobiliarios que deseaban conocer todos los datos de los propietarios de bienes raíces en una región—. En paralelo y sin una Política Pública clara debatida, el gobierno anterior, apremiado con las exigencias para cumplir con los requisitos de incorporación a la OECD, el año 2009 mediante un proyecto de ley propuso desnaturalizar al Consejo de Transparencia y asignarle una nueva competencia, a saber, trasladarlo ahora al Sector Privado de la sociedad y ser el garante de que se respete la privacidad de las personas cuando los datos personales se procesan —por ejemplo— en la banca, en las ISAPRE, en las compañías de seguros, en las AFP, en el retail o en las empresas de marketing.

315.12. El derecho expuesto en su transcurso histórico muestra las tres líneas como se desenvuelve el derecho de protección de los datos personales.

Una primera lo traza en el camino de la *intimidad*, pero considerado fuera de un problema de derecho material o personalísimo, para ubicarlo como un derecho humano propio de la garantía que interpreta los derechos *pro homine*. En este sendero prevalece la legislación común (si bien de carácter constitucional).

Otros prefieren anticipar el derecho para ubicarlo como una *garantía constitucional*. Toda persona (se debate si ello comprende a las personas ideales, aunque predomina su incorporación) tiene derecho a la protección de sus datos personales (haya o no un fin discriminatorio en la aplicación de lo informado) y, en su caso, a tener acceso a las bases de datos para requerir acciones de control. Este es el campo de las Constituciones.

La mayoría de las Constituciones de Latinoamérica estipulan que el *habeas data* es un mecanismo jurídico constitucional que protege los datos o las informaciones de las personas que hayan sido recabadas o recolectadas por medios tecnológicos, informáticos o telemáticos y dejan implícito que también pudieran haberlo sido, por medios mecánicos, escriturarios o documentales, o medios tradicionales de archivo documental; otros pocas Constituciones, no sólo constitucionalizan la etapa de la recogida de la información (por medios informáticos y manuales), sino que avanzan a constitucionalizar, las etapas o fases del proceso informático que para algunos identifica y caracteriza al *habeas data*, tales como la de almacenamiento y procesamiento propiamente dicho (que abarca el uso y finalidad de la información), la actualización y la rectificación de la información; y tan solo la Constitución colombiana, constitucionaliza, la fase o etapa de comunicación de los datos o informaciones personales, que algunos llaman "cesión", "transmisión" y "circulación" de datos. Etapa, que hoy por hoy, es la que más produce quebrantamiento de derechos fundamentales y por la cual, los estados europeos y los de ámbito anglosajón también se oponen a los demás Estados para realizar transferencia o flujo de datos a Estados, que no tienen legislaciones homologadas a las que ellos manejan en la UE, ni tecnologías que utilizan los TIC, conforme a los actuales requerimientos de la informática, telemática o electrónica.[10]

[10] CERDA SILVA, *Autodeterminación informativa y leyes sobre protección de datos,* cit., pp. 26 y ss.

El tercer espacio (línea conductiva) se libera al proceso constitucional. Aquí. En lugar de especificar el alcance y naturaleza del derecho a la "autodeterminación informativa" o como quiera llamarse (ver capítulo siguiente), se opta por regular el trámite mediante el procedimiento de *habeas data*.

En esta sección el conflicto emerge del mecanismo sustitutivo de otras vías concurrentes (*v. gr.:* amparo, tutela, protección, acceso a la información, etc.), o de la posibilidad de alternar entre una y otra; o de permitir el acceso directo al proceso sin necesidad de agotar una instancia previa administrativa o privada (reclamo ante el archivo, base o banco de datos).

> En los Estados latinoamericanos, como hemos visto, que han preferido regular por separado los derechos de acceso y conocimiento de la información en general o en particular (*v. gr.:* en Colombia la Ley Estadística, No. 79 de 1993) de las que regulan el derecho a conocer el uso y la finalidad que se da a la información o datos de la persona o de sus bienes; y por su puesto, una y otra diferentes a las normas jurídicas especiales que regulan La Protección de datos personales o el "*habeas data*" (*v. gr.:* En Argentina o en España), la aplicabilidad de las normas sigue el principio universalmente conocido de que la norma especial se aplica de preferencia a la general, así como el principio de la subsidiariedad de la norma en aquellos aspectos no previstos en la norma especial, siempre que coexistan normas generales con la especial, pues en Estados como el Colombiano y el venezolano que todavía aún no tienen normatividad específica sobre protección de datos o *habeas data*, siguen aplicándose las normas.[11]

316. La situación de los datos personales en Estados Unidos

316.1. A pesar de tener un sistema legal similar al de Inglaterra que ha creado un organismo especial destinado a la protección de los datos: *el Information Commissioner's Office* (ICO), que se origina a instancias de la *Data Protection Act* de 1998; en Estados Unidos hay cierta orfandad en la materia.

> En Inglaterra existen las siguientes leyes: 1) *Data Protection Act* de 1998, transposición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo. 2) *Consumer Protection (Distance Selling) Regulations* de 2000 es la transposición de la Directiva europea 1997/7/EC y en ella se especifican, entre otros, los siguientes parámetros: la información necesaria para formalizar un contrato, los servicios que se han de prestar, el derecho a cancelar una petición o el pago por tarjeta de crédito. 3) *Freedom of Information Act* de 2000, que otorga a los ciudadanos a y a las organizaciones el derecho a solicitar información sobre los datos que poseen instituciones públicas de Inglaterra, Gales e Irlanda del Norte y de instituciones privadas de Escocia. 4) *Electronic Signature Regulations* de 2002, transposición de la Directiva 1999/93/EC del Parlamento Europeo y en la que el art. 5 se centra exclusivamente en la protección de datos, si bien no constituye el tema central de dicha regulación. 5) *Privacy and Electronic Communications (EC Directive) Regulations* de 2003, que constituye la transposición de la Directiva 2002/58/CE. 6) *Environmental Information Regulation* de 2004, transposición de la Directiva 2003/4/EC, y similar en esencia a la

[11] CERDA SILVA, *Autodeterminación informativa y leyes sobre protección de datos,* cit., pp. 26 y ss.

Freedom of Information Act, sólo que atañe únicamente a datos relativos a información medioambiental.

En general, ellos no siguieron ninguna normativa europea, ni respetaron las líneas trazadas por los "*Principios rectores sobre la utilización de ficheros computarizados de datos personales"* antes mencionados.

Se prefieren leyes puntuales y específicas, reglamentos sectoriales y políticas de poca generalización, de forma que los casos se resuelven sin parámetros y con una gran confianza en el sistema jurisdiccional.

Forman parte de estos mecanismos las leyes siguientes: *Cable Communications Policy Act* de 1984, *Driver s Privacy Protection Act, Electronic Communications Privacy Act* de 1986, *Electronic Funds Transfer Act, Telecommunications Act* de 1996, *Fair Credit Reporting* de 1970 y *Consumer Credit Reporting Reform Act* de 1996, *Right to Financial Privacy Act, Telephone Consumer Protection Act, Video Privacy Protection Act,* y *Aviation and Transportation Security Act* de 2001, entre otras disposiciones federales y estatales.

La legislación estadounidense se caracteriza además por su adscripción a un *laisez faire* del viejo cuño, en que los propios interesados deben velar por el cumplimiento de la normativa relativa al tratamiento de los datos personales que les conciernen ya sea a través del ejercicio de los derechos que se reconocen al titular de los datos, o bien mediante la formulación de códigos deontológicos y adopción de disposiciones reglamentarias por los órganos responsables de sistemas de registro y el Estado asegura su posición de gendarme mediante el establecimiento de excepciones fundadas en necesidades de orden público, prescindiendo de la consagración de una autoridad de control pública que vele por el cabal cumplimiento de la legislación.[12]

316.2. El problema que genera la antinomia con Europa se provoca con la política aquí generada de la *protección equivalente*, lo cual ha obligado a negociar los llamados "Acuerdos de Puerto Seguro" (*Safe Harbor Agreement*), que persiguen conciliar las diferencias legislativas.

Se llaman principios de "Puerto Seguro", a las disposiciones que deben respetar las entidades estadounidenses para obtener el visto bueno de la Unión Europea, cuando se genera el uso de información de personas a quienes se les debe asegurar una política de protección de datos adecuada, donde la privacidad y la confidencia de los datos que son transfronterizos (es decir que van de un continente a otro merced a un negocio, por ejemplo) deben recibir el mismo estándar de protección que tienen en Europa.[13]

De este modo, por su adhesión a *Safe Harbor* los organismos y entidades asumen ciertos principios rectores del tratamiento de datos, a saber: *a)* notificación e información a las personas, previas a la recogida de datos que les conciernen; *b)* derecho de opción para divulgación a terceros o usos incompatibles con el objeto inicial de

---

[12] CERDA SILVA, *Mecanismos de control en la protección de datos en Europa*, cit., p. 228.

[13] MOLINA QUIROGA, ob. cit., Capítulo IV de la tesis (inédita).

la recogida, ya sea en listas de exclusión o aceptación, según la naturaleza de los datos; *c)* se condiciona la transferencia ulterior de datos a terceros a la adopción de los principios y se impone a las entidades tratantes de datos la obligación de implementar medidas de seguridad; *d)* obligación de velar por la calidad de los datos; *e)* reconocimiento de los derechos de acceso y rectificación a las personas concernidas; y, se establece la necesidad de que las entidades tratantes adopten mecanismos que brinden garantías para la aplicación de los principios, tales como recursos independientes, procedimientos de seguimiento y medios para subsanar infracciones y sancionarles, en su caso.

> Sin embargo, *Safe Harbor* no es obligatorio *per se* para las empresas o entidades de Estados Unidos, ya que previamente deben aceptar voluntariamente la aplicación del Acuerdo, mediante autocertificación de su compromiso, la que debe ser notificada al Departamento de Comercio. Dicha notificación debe renovarse anualmente e incluye información básica relativa a la entidad u organización adherente, el tratamiento de datos personales provenientes de Europa que efectúa y una descripción de las políticas de protección a la vida privada a que somete el procesamiento de aquellos. La verificación de las prácticas de protección de la vida privada, así como su conformidad con los principios de *Safe Harbor* puede ser efectuada por terceros o por la propia entidad. Huelga decir que los compromisos asumidos por las entidades adscritas no son extensivos al tratamiento de toda la información personal, sino sólo a aquellos datos transmitidos desde la Unión Europea a partir del momento en que se adhiere al Acuerdo.[14]

El control de aplicación queda en manos del Departamento de Comercio de los Estados Unidos a través de la *Federal Trade Commission* (Comisión Federal de Comercio), que goza de amplias facultades para regular y fiscalizar cuanta relación comercial se entable.

Más adelante veremos en particular alguna de las leyes dictadas, en especial, la relativa con informes comerciales y sobre el derecho a la privacidad.

317. La Convención Americana sobre protección de datos personales

Por encargo de la Organización de Estados Americanos, el Comité Jurídico Interamericano elaboró un "*Anteproyecto de Convención Americana sobre Autodeterminación Informativa*", el cual dice:

> PREÁMBULO
>
> Los Estados americanos signatarios de la presente Convención,
>
> Considerando:
>
> 1) Que en la Declaración Americana de los Derechos y Deberes del Hombre, de 1948, se reconoce a la persona entre otros derechos, el de ser protegida contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar; que en la Convención Americana sobre Derechos Humanos, de 1969, se reconocen y amplían tales derechos

[14] CERDA SILVA, *Autodeterminación informativa y leyes sobre protección de datos,* cit., pp. 26 y ss.

al establecerse que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad, que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; y que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

2) Que lo anterior es congruente con lo normado en el ámbito internacional tanto en el contenido de las Declaraciones como en el de las Convenciones, pues desde la Declaración Universal de los Derechos del Hombre, de 1948, se reconoció, por primera vez, de manera expresa e un instrumento internacional, el derecho a la vida privada. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honor o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. Que el Pacto Internacional de Derechos Civiles y Políticos, de 1966, mantiene el mismo criterio.

3) Que no obstante lo anterior, el peligro en contra de a vida privada y el pleno ejercicio de otros derechos se ha acrecentado por el aparecimiento de nuevos medios técnicos de injerencia y control sobre los derechos y libertades, particularmente por el tratamiento automatizado de datos de carácter personal, que permiten el conocimiento general de la historia de cada ser humano, creándose la posibilidad de que por medio de los ficheros, registros o de los bancos de datos no sólo se conozca lo más privado de las personas y se les controle y dirija atentándose así contra su dignidad, libertad e igualdad y contra la estructura misma del sistema democrático, situación que vuelve necesario dar a las personas una ulterior protección a la ya prevista en el derecho interno, en las Declaraciones y Convenciones Internacionales citadas.

4) Que la normativa adicional que se dé para limitar la informática debe tender a lograr un justo equilibrio y armonía entre la protección a los derechos y libertades de las personas, con los derechos que emanan del poder informático especialmente, con la libre circulación de la información entre los pueblos y la necesidad del progreso y desarrollo nacional en una economía post-industrial globalizada e informatizada.

5) Que siendo los derechos a proteger, los conflictos a resolver y los intereses a armonizar, similares en los Estados Americanos como en el resto del mundo pues las nuevas tecnologías de la informática traspasan las fronteras, las soluciones jurídicas sean nacionales, regionales o universales no pueden ser muy diferentes sobre todo en materia de derechos humanos cuya tendencia lógica es hacia su total internacionalización, lo que conlleva que una Convención Americana respecto a la protección de las personas con respecto al tratamiento automatizado o manual de sus datos personales, trasciende su ámbito geográfico por lo que las soluciones que se adopten deben de conformarse en lo posible en las de otras regiones.

Han convenido en lo siguiente:

CAPÍTULO I
Disposiciones generales

ART. 1.—*Objeto y fin*

El fin de la presente Convención es garantizar, en el territorio de cada Estado Parte a cualquier persona física o jurídica sean cuales fueren su nacionalidad, residencia o domicilio, el respeto de sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa con relación a su vida privada y demás derechos de la

personalidad; asimismo, la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

ART. 2.—*Definiciones*

A los efectos de la presente Convención:

a) "Datos de carácter personal" significa cualquier información relativa a una persona física o jurídica identificada o identificable;

b) "Fichero automatizado" significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado;

c) Por "tratamiento automatizado" se entiende las operaciones que a continuación se indican, efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registros de datos, aplicación a esos datos de operaciones lógica aritméticas, su modificación, borrado, extracción o difusión;

d) Autoridad "controladora de fichero" significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la Ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán;

e) Afectado" persona física o jurídica, titular de los datos que sean objeto del tratamiento automatizado o manual.

ART. 3.—*Campo de aplicación*

1. La presente Convención será de aplicación a los datos de las personas naturales o jurídicas o a sus bienes que figuren en registro, ficheros o bancos de datos de los sectores público y privado, sean éstos automatizados o manuales.

Las restricciones permitidas a la aplicación de la presente Convención, sólo serán las aceptadas en la misma y no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas.

2. Cualquier Estado podrá en el momento de la firma o al depositar su instrumento de ratificación o adhesión de esta Convención, o en cualquier momento posterior hacer saber mediante declaración dirigida y depositada en la Secretaría General de la Organización de los Estados Americanos, la que transcribirá copias de los mismos a los Estados miembros de dicha Organización, que:

a) No aplicará la presente Convención a determinadas categorías de ficheros automáticos o manuales de carácter personal, una lista de los cuales quedará depositada. No podrán incluirse en esa lista categorías de ficheros sometidos conforme a su derecho interno a normas de protección de datos, ni los datos considerados sensibles conforme a esta Convención. Deberá por tanto, modificar dicha lista mediante una nueva declaración cuando estén sometidos a su régimen de protección de datos, categorías suplementarias de ficheros automatizados o manuales de carácter personal.

No aplicará la presente Convención a las personas jurídicas y a los registros o ficheros manuales.

3. Cualquier Estado que haya ampliado el campo de aplicación de la presente Convención mediante una de las declaraciones a que se refieren los apartados 2, *b)* o *c)*, que anteceden, podrá en dicha declaración, indicar que las ampliaciones solamente se aplicarán a determinadas categorías de ficheros de carácter personal mediante la declaración prevista en el apartado 2, *a)* anterior y no podrá pretender que una Parte que no los haya excluido aplique la presente Convención a dichas categorías.

4. Una Parte que haya procedido a una u otra de las limitaciones previstas en el párrafo 2, *b)*, del presente artículo no podrá pretender que se aplique la Convención en esas partes con respecto a una Parte que no haya procedido a esas limitaciones.

5. Las declaraciones previstas en el párrafo 2 del presente artículo tendrán efecto en el momento de la entrada en vigor de la Convención con respecto al Estado que las haya formulado, si dicho Estado las ha hecho en el momento de la firma o del depósito de su instrumento de ratificación o adhesión, o tres meses después de su recepción y depósito en la Secretaría General de los Estados Americanos si se han formulado en su momento ulterior. Dichas declaraciones podrán retirarse en su totalidad o en parte mediante el mismo procedimiento ante la Secretaría General de la Organización de los Estados Americanos. La retirada producirá efectos tres meses después de su recepción y depósito.

CAPÍTULO II
Principios básicos para la protección de datos

ART. 4.—*Compromisos de las Partes*

1. Los Estados Parte en la presente Convención se comprometen a respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio de toda persona natural o jurídica sujeta a su jurisdicción, con igualdad y sin discriminación alguna.

Cada Parte tomará en su derecho interno, las medidas legislativas o de otro carácter que sean necesarios para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

2. Dichas leyes deberán dictarse a la brevedad posible y las medidas de otro carácter a más tardar en el momento de su entrada en vigor de la presente Convención.

ART. 5.—*Derecho de información en la recogida de datos*

1. Los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco directamente o por su apoderado con poder o cláusula especial; las personas jurídicas por medio de su representante legal o apoderado con poder o cláusula especial;

a) De la existencia de un fichero automatizado o manual de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información;

b) Del carácter obligatorio o facultativo de sus respuestas a las preguntas que se les formulen;.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrados;

d) De la posibilidad de ejercer los derechos de acceso, rectificación, actualización, cancelación y confidencialidad;

e) De la identidad y dirección del responsable del fichero.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refiere el apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de la circunstancia en que se recaban.

ART. 6.—*Consentimiento del afectado*

1. El titular de los datos deberá dar por sí o por su representante legal o apoderado el consentimiento, salvo que la ley disponga otra cosa dentro de límites razonables, o que estuviere expresamente autorizada su recogida en esta Convención.

Dicha racionabilidad deberá ser considerada por el Juez si se le planteare en caso de controversia lo anterior vale tanto para los ficheros de titularidad pública o privada.

2. El consentimiento podrá ser revocado pero la revocatoria no producirá efectos retroactivos.

ART. 7.—*Calidad de los datos*

1. Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado o manual, así como someterlos a dicho tratamiento. Cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimos para que se han obtenido.

2. Los datos de carácter personal objeto de tratamiento automatizado o manual no podrán utilizarse para finalidades distintas de aquellas para que los datos hubieren sido recogidos.

3. Dichos datos serán exactos y puestos al día, de forma que respondan con veracidad a la situación real del afectado.

4. Si los datos de carácter personal registrados resultaren ser inexactos en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados, actualizados o complementados. Igualmente serán cancelados si no mediare un consentimiento legal y legítimo o estuviere prohibida su recolección.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser pertinentes o necesarios para la finalidad para la cual hubieren sido recibidos y registrados.

No serán conservados en forma que permita la identificación del interesado en un período que sea superior al necesario para los fines en base a los cuales hubieren sido recabados o registrados.

6. Serán almacenados de forma que permita el derecho de acceso por el afectado.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

8. Se prohíbe memorizar, registrar o archivar juicios de valor.

9. Se prohíbe tener sobre una persona más datos que los necesarios a los fines del fichero, por consiguiente la ley establecerá límites al número, clase y calidad de datos que puedan estar en un mismo fichero o en ficheros distintos de la misma entidad pública o particular.

10. El derecho interno de los Estados Parte, determinará el tratamiento para los ficheros que ya estén en funcionamiento a la fecha de la entrada en vigencia de esta Convención o a la fecha de la entrada en vigor de la ley respectiva. En todo caso, la regla básica es el consentimiento del afectado de tal manera que sea efectiva su autodeterminación sobre la información que le concierne.

ART. 8.—*Categorías particulares de datos*

Los datos de carácter personal de las personal físicas que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud y a la vida sexual, no podrán tratarse automática ni manualmente en registros o ficheros accesibles al público, a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales.

ART. 9.—*Seguridad de los datos*

1. El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten

su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía de ley o reglamentaria con respecto a su seguridad e integridad y a los de los centros de tratamientos, escalas, equipos, sistemas y programas.

3. Por ley o por reglamento, se establecerán los requisitos y condiciones que deban reunir los ficheros automatizados y los manuales y las personas que intervengan en el tratamiento automatizado o no de los datos .

4. El responsable del fichero y quienes intervengan en cualquier fase del proceso de recolección y tratamiento de los datos de carácter personal están obligados al secreto profesional.

ART. 10.—*Cesión de datos*

Los datos de carácter personal objeto de tratamiento automatizado o manual, sólo podrán ser cedidos de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

Dicho consentimiento no será necesario cuando así lo disponga la ley expresamente dentro de los límites razonables o si estuviera expresamente autorizado en esta Convención.

Dicha racionalidad deberá ser calificada por el Juez cuando se le planteare un caso concreto si se suscitare controversia.

Lo anterior es aplicable a cualquier fichero independientemente de su titularidad pública o privada.

El consentimiento para la cesión podrá ser revocado pero la revocatoria no tendrá efectos retroactivos.

ART. 11.—*Derechos y garantías de las personas*

Cualquier persona deberá poder:

a) Conocer la existencia de un fichero automatizado o manual de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;

b) Obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no del fichero automatizado de los datos de carácter personal que conciernen a dicha persona, así como la comunicación de dichos datos en forma inteligible;

c) Obtener, llegado el caso, la rectificación de dichos datos y su actualización o el borrado de los mismos cuando se hayan tratado con infracción a las disposiciones de esta Convención o del derecho interno, así mismo el cumplimiento de la garantía de confidencialidad;

d) La autoridad o el responsable del fichero deben cumplir con lo pedido gratuitamente y resolver en el sentido que corresponda en el plazo que se señale la ley;

e) Disponer de un recurso en su caso.

ART. 12.—*Garantías judiciales*

1. Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que los ampare contra actos que violen

sus derechos fundamentales reconocidos por esta Convención, la Constitución de los Estado Parte o la ley.

2. Toda persona tiene derecho a controlar sus datos personales existentes en los ficheros públicos o particulares, la garantía y el procedimiento judicial para ejercer tal control es el *habeas data*.

3. El derecho interno de los Estados Parte regulará la naturaleza constitucional o común de tal recurso, pero en todo caso este debe ser su medio de amparar en forma expedita, rápida y eficaz los derechos de la persona ante los excesos informáticos automatizados o manuales.

ART. 13.—*Del habeas data*

Se concederá *habeas data*:

a) Para acceder directamente o conocer las informaciones y datos relativos a la persona del impetrante sea esta persona natural o jurídica;

b) Para conocer la finalidad de los datos a ellos referidos y al uso que se haya hecho de los mismos;

c) Para solicitar y obtener la rectificación, actualización, cancelación o borrado y el cumplimiento de la garantía de confidencia respecto a los datos personales del impetrante;

d) Para obtener en su caso la correspondiente indemnización, daños y perjuicios.

Mientras esté pendiente el *habeas data* el responsable del fichero debe suspender todo uso de los mismos, salvo autorización judicial o consentimiento expreso del impetrante para una finalidad concreta.

ART. 14.—*Excepciones y restricciones*

Sólo por ley se podrán establecer excepciones y restricciones en los principios, derechos y garantías en esta Convención enunciados y siempre que éstas sean justas y razonables en una sociedad democrática:

a) Para la protección de la seguridad del Estado de la seguridad pública, para los intereses monetarios del Estado o para la represión de las infracciones penales;

b) Para la protección de las personas concernidas y de los derechos y libertades de otras personas;

c) Para el funcionamiento de ficheros de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existe riesgo de que las personas sean identificadas. Siempre existirá recurso para que la autoridad judicial decida si en un caso concreto estamos ante una excepción o restricción razonable.

ART. 15.—*Sanciones y recursos*

Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

ART. 16.—*Protección más amplia*

Ninguna de las disposiciones del presente capítulo se interpretará en el sentido que limite la facultad, o afecte de alguna otra forma la facultad de cada Parte, de conceder a las personas concernidas una protección más amplia que la prevista en la presente Convención.

CAPÍTULO III
Movimiento internacional de datos

ART. 17.—*Movimiento internacional de datos de carácter personal y el derecho interno*

1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuese de datos de carácter personal, que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.

2. Una Parte no podrá, como el único fin de proteger la vida privada prohibir o someter a una autoridad especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra parte.

3. Sin embargo, cualquier parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2:

a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal, o de ficheros automatizados de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente.

b) Cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no Contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo de este párrafo.

CAPÍTULO IV
Ayuda mutua

ART. 18.—*Cooperación entre las Partes*

Las partes se obligan a concederse mutuamente asistencia para el cumplimiento de la presente Convención.

El derecho interno de cada Estado Parte determinarán a la autoridad que cumplirá esta función hacia los otros Estados miembros y en relación con las personas naturales o jurídicas a fin de que cuenten con la asesoría y ayuda debida en la protección de sus datos personales.

CAPÍTULO V
Agencia de protección de datos

ART. 19.—*Naturaleza y régimen jurídico*

Los Estados Partes podrán crear Agencia encargada de la protección de datos personales, como Entes de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúen con plena independencia de las administraciones públicas en el ejercicio de sus funciones. Tendrán funciones administrativas, de recomendación, supervisión y control sobre los ficheros, registros y bancos de datos personales, podrán establecer sanciones sobre los mismos y sus resoluciones serán recurribles por la vía contencioso administrativa. La ley determinará las infracciones y sus sanciones, sin perjuicio de la responsabilidad penal que corresponda en caso de delito.

CAPÍTULO VI

ART. 20.—*El registro general de protección de datos*

1. Los Estados Parte crearán por ley un Registro General de Protección de Datos Personales.

2. Serán objeto de inscripción en dicho Registro:

a) Los ficheros automáticos o manuales de que sean titulares la administración pública o de titularidad privada;

b) Los datos que sean necesarios para el ejercicio de los derechos de acceso, rectificación, actualización, cancelación y confidencialidad de los datos personales;

c) Las autorizaciones para operar en su caso y otras obligaciones de los responsables del fichero que consten en la ley y los reglamentos;

d) Un índice o listado de las personas de que constan datos personales y el fichero en el que se encuentran sin que aparezca que clase de datos. Para tal efecto, los responsables del fichero enviarán al Jefe del Registro en el plazo que determine la ley los nombres y domicilios de las personas sobre la cual tienen datos personales para el solo efecto de facilitar el que el interesado pueda saber con facilidad si se encuentran datos suyos en algún fichero y en cuál.

CAPÍTULO VII
Enmiendas y cláusulas finales

ART. 21.—*Enmiendas previstas a futuro...*

Sección 2ª Intimidad y datos personales

318. Relaciones entre intimidad y datos personales

318.1. Las relaciones entre intimidad y datos personales parecen obvias, pero a los fines de la protección procesal es necesario descubrir que el tratamiento de información personal necesita salir del marco tuitivo que tienen las normas sustanciales, básicamente, el Código Civil y el Penal, para encontrar el fundamento constitucional que permite deducir el proceso constitucional de *habeas data*.

318.2. En efecto, observemos como punto de partida el objeto de esta garantía procesal o los contenidos de este nuevo derecho, según la tutela que se pretenda abordar, y de inmediato aparecen sucesivas alternativas. El *habeas data*, dicen algunos, protege el derecho a la intimidad; pero al mismo tiempo, se afirma que la defensa es de la privacidad, o de la dignidad humana, o el derecho a la información, o bien, la tutela del honor, o de la propia imagen o perfil personal, o el derecho a la identidad, o simplemente acotado a la autodeterminación informativa. Como se ve, son multifacéticas y distintas las proyecciones en cada caso. De allí lo necesario de efectuar algunas consideraciones previas, antes de entrar a analizar puntualmente el texto legal sancionado.

318.3. El derecho a la intimidad es amplio y omnicomprensivo. Ocupa sencillas manifestaciones del derecho a la soledad y a no ser perturbado en la vida privada, como también otras situaciones, por ejemplo, la reserva y confidencialidad de ciertos actos, la intimidad familiar, la defensa del honor, el derecho a la propia imagen, o la protección de la identidad. Inclusive, la categoría principal no se precisa, de forma que para algunos es la dignidad humana y para otros el derecho a la privacidad; pero si únicamente se focaliza el tema procesal, la mayoría sostiene que se trata de un límite al derecho a la información, o bien, un derecho a la autodeterminación informativa.

Evidentemente, tamaña extensión y perfiles impide sostener que el *habeas data* sea el proceso de defensa para todos ellos, y por eso, pareciera más importante, antes que definir la vía procesal, establecer el alcance del derecho fundamental.

> En el artículo de Warren y Brandeis encontramos —dice García San Miguel— una definición ya clásica que hizo fortuna: la intimidad es *the right to be alone*, el derecho a estar solo, el derecho a la soledad. Sin embargo, esta definición no parece cubrir todo lo que actualmente consideramos incluido en el ámbito de aquél derecho. Pensamos que nuestra intimidad viene agredida por escuchas telefónicas, fotos tomadas a distancia con teleob-

> jetivo y uso indebido de datos informáticos, pese a que nada de ello comporta la presencia física de otras personas. Es decir que, aunque en muchos casos estemos literalmente solos, nuestra intimidad puede resultar dañada por manejos que se emprenden a distancia y, a menudo, sin que el interesado se entere de los mismos.
>
> Por ello, algunos autores propusieron definiciones diferentes. Fried, en un trabajo de 1979 que lleva por título *An anatomy of values* define la intimidad como "control sobre la información que nos concierne", y Parker, en otro trabajo de 1974, con el título *A definition of privacy*, la define como "control sobre cuándo y quién puede percibir diferentes aspectos de nuestra persona" [...].[15]

La intimidad es, por tanto, el derecho a no ser conocidos, a mantenerse reservados, como una suerte de derecho al secreto, a que los demás no sepan lo que somos o lo que hacemos.

En la legislación argentina, la intimidad se encuentra en el artículo 19 de la Constitución Nacional: "Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe".

También, los artículos 31 y correlativos de la ley 11.723 (Propiedad Intelectual) y el artículo 21 de la ley 18.248 (Ley del nombre) refieren a ella. Específicamente, la intimidad se incorpora al Código Civil, con la sanción de la ley 21.173. El artículo 1071 *bis* dice:

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

Este conjunto normativo no se vincula en caso alguno al impacto informático, por ello recién con la reforma constitucional argentina de 1994 comienza alguna cobertura específica.

318.4. La perturbación que menciona el código de fondo se refiere a la publicación de retratos (derecho a la imagen); difusión de correspondencia (derecho al secreto; confidencialidad y reserva); mortificación de costumbres o sentimientos (posible vulneración de datos sensibles); o cualquier otro modo de disturbio que afecta la vida privada (dar a publicidad situaciones de crisis conyugal; cesaciones de pago; publicar una declaración elogiando un producto o suscribiendo una petición política que nunca firmó; revelar arbitrariamente el carácter adoptivo o matrimonial

---

[15] GARCÍA SAN MIGUEL, Luis, *Estudios sobre el derecho a la intimidad,* Tecnos-Universidad de Alcalá de Henares, Madrid, 1992, p. 13.

de un hijo sin el consentimiento de los padres; no entregar el cadáver de un niño nacido muerto a sus padres dándole horrible destino, etcétera). En cada supuesto el actor puede reclamar: *a)* el cese o la suspensión de la perturbación; *b)* una indemnización reparatoria.

En el primer caso, la acción de abstención que se propone puede ser adecuada si con ello se consigue paralizar los efectos perniciosos de la invasión a la intimidad; pero no resulta efectiva para resolver la afectación de otros supuestos como la lesión a la imagen, la difusión de un secreto, la exposición pública de costumbres o comportamientos que inciden en la personalidad del damnificado. Para estos supuestos, se puede escoger entre la acción indemnizatoria, o la acción penal correspondiente (si ella está prevista), o ambas simultáneamente.

318.5. Ahora bien, ¿dónde coincide la tutela civil de la intimidad con la previsión constitucional o legal de protección a los datos personales?

Si tomamos como fuente el derecho argentino, obsérvese que el artículo 1071 *bis* del Código Civil establece como presupuestos del acto lesivo los siguientes:

- *Entrometimiento arbitrario,* que supone sancionar a quien sin derecho viola la esfera de intimidad personal, afectando con ello, la vida privada. Es una acción positiva, que se manifiesta en el hacer.

  Aquí hay coincidencia con el *habeas data*.
- *Perturbación de cualquier modo,* siempre que no constituya un delito penal.

  También tiene su correlato con el *habeas data*.
- *Publicación de retratos sin consentimiento, difusión de correspondencia, mortificación en costumbres o sentimientos*, conceptuando las modalidades de lesión al derecho de las personas.

  Sin coincidencia con el *habeas data*.

El paralelo pretende significar que los derechos proyectados desde la tutela de la intimidad en el campo sustantivo, difiere del amparo constitucional previsto, debiendo el juez en cada supuesto establecer el tipo de procedimiento adecuado a la pretensión que se promueva.

318.6. Asimismo, en el terreno de la intimidad anidan otras cuestiones que se vinculan como derechos personalísimos, tales como el honor, la imagen, la dignidad, el perfil frente al público o la opinión personal que de uno se tiene, etc., los que por su variedad llevan a trazar un conjunto de situaciones que merecen tanto respeto como los ya observados. Y, en consecuencia, ¿cuál es la respuesta procesal para ellos? ¿Es el *habeas data*?

> Se ha simplificado el problema de limitar los derechos que ocupan el espacio de la intimidad con el fin de precisar las vías procesales específicas. En este sentido Herrán Ortiz sostiene que resulta un claro desacierto considerar que cuanto menos se conozca de la vida de las personas se goza de mayor intimidad, ya que ésta no consiste simplemente en la ausencia de información personal. En efecto, la intimidad se refiere a una esfera tan interior del individuo que en principio solo él puede revelar. Así, el carácter confiden-

cial de los datos no es, a diferencia del derecho a la intimidad, un instrumento cuya utilización dependerá de los fines y del modo en que se haga uso de la misma.

En definitiva, si "íntimo" es lo que cada persona reserva para sí y a los demás no es lícito invadir, confidencial es aquello que se revela a alguien con la intención o ánimo de que no sea revelado a los demás sin el consentimiento del interesado. De igual manera, no puede desconocerse que si bien en un primer acercamiento al derecho a la intimidad éste se puede relacionar estrechamente al "secreto", debe admitirse que la intimidad no implica exclusivamente la ausencia de información sobre la vida de la persona; representa, por el contrario, una necesidad de "vida interior", o relación intra-personal, de reflexión de los propios sentimientos y pensamientos.[16]

318.7. Para lograr una aproximación más o menos certera al objetivo que persigue el proceso constitucional de *habeas data*, es necesario tomar desde el comienzo una posición específica: o centramos la tutela en la protección de los datos, o expandimos los derechos defendidos hacia todo el universo que supone el derecho a la intimidad.

La relación entre derecho a la intimidad y el derecho a la protección de los datos personales o a la autodeterminación informativa ha sido analizada de forma diferente por la doctrina. Algunos sostienen que los términos "protección de datos" y "protección de la intimidad" son dos nociones distintas, ya que el interés de proteger la veracidad de los datos y el uso que de ellos se hace no está relacionado necesariamente con la protección de la libertad individual. En Estados Unidos, la distinción se traza más que en el significado en los sistemas legales, apuntando que, los países de tradición legal de *common law* utilizan más frecuentemente la expresión "protección de la intimidad", mientras que los países de *civil law* prefieren la expresión "protección de datos".

Es verdad que la revolución informática del siglo XX ha obligado a encontrar formas procesales que respondan a esa novedosa invasión a la esfera de intimidad de las personas.

En este terreno afinca el *habeas data* como garantía jurisdiccional; pero no es menos cierto que los derechos interesados en esta dimensión no pueden ser, únicamente, individuales y abonarlos en el campo de la intimidad. La sociedad, todos, tienen un interés especial que trasciende el reducto de lo propio en esta cuestión. Así como es necesario, también, advertir que el fenómeno de la recolección y archivo de datos provoca un negocio que no siempre es ilícito como parece resultar del mensaje.

318.8. La búsqueda del dato posee finalidades de organización y conocimiento, de seguridad y certidumbre para la toma de decisiones, y por ello, es el Estado mismo quien debe garantir el derecho y poner límites a la expansión.

Tanto como existe un derecho a no ser perturbado en la vida privada; también existe el derecho de las empresas a comercializar la información que obtiene cuando ello no tiene fines ilícitos.

---

[16] HERRÁN ORTIZ, Ana Isabel, *La violación de la intimidad en la protección de datos personales,* Dykinson, Madrid, 1999, pp. 37 y ss.

Lo que tratamos de manifestar es que aquella concepción tradicional sobre el derecho a la intimidad que nos llega del "derecho a ser dejado a solas", se ha ido transformando en el contexto de la sociedad informatizada.

Tal como afirma Estadella Yuste,

> existen varios aspectos que hacen evidente esta evolución: 1) Aunque la información personal puede tener un valor económico, no deja, por ello, de tener un valor personal. La información personal forma parte de la intimidad individual y está relacionada con el concepto de autonomía individual para decidir, hasta cierto límite, cuándo y de qué información puede ser objeto de tratamiento automatizado; 2) La protección del derecho a la intimidad contra el uso de un tratamiento automatizado de datos personales no se plantea exclusivamente a consecuencia de problemas individuales, sino que también expresa conflictos que incluyen a todos los individuos de la comunidad internacional. La idea de que la persona titular de los datos —el afectado— tiene interés, como parte de un grupo, es controlar el tratamiento automatizado de datos es reciente, ya que no aparece así en la "primera generación" de las leyes protectoras de datos, orientadas exclusivamente a la protección de la persona como entidad individual; 3) En algunos casos el tratamiento de datos automatizado se ha llegado a convertir en un arma estratégica de manipulación de conductas individuales; 4) La aplicación de avanzados métodos telemáticos a información de carácter personal ha dejado de ser la excepción para convertirse en una rutina diaria; en consecuencia, hay que tratar el tema como una realidad y no como un problema hipotético.[17]

318.9. Por ello, cuando se trata de establecer límites al sistema de circulación y registro de datos de las personas, se ha pensado que el mentado derecho a la intimidad no puede resultar afectado, al menos, en cuatro aspectos esenciales: vida privada, vida familiar, domicilio y correspondencia.

El artículo 12 de la Declaración Universal de Derechos Humanos establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación". Prácticamente igual es el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

A su vez, la faz comercial o empresarial, que tiene el tratamiento de datos, obliga a considerar el desarrollo de las telecomunicaciones, o de tecnologías de la información, o la vigía permanente por satélites de teletransmisión que, en cada caso, provocan una suerte de libertad vigilada que afecta el derecho a la intimidad, pero que resultan inevitablemente necesarios para asegurar aspectos tales como la seguridad del Estado, o el derecho a la información.

El Convenio 108 de la Unión Europea establece un límite a los derechos de la autodeterminación informativa cuando ellos constituyen una medida necesaria en una sociedad democrática para la protección de la seguridad del Estado: seguridad pública, intereses monetarios, o imposición de infracciones penales, y cuando estén dirigidas a la protección de la persona concernida y de los derechos y libertades de

---

[17] ESTADELLA YUSTE, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales,* Tecnos, Madrid, 1995, p. 14.

terceras personas. Aparte de estas restricciones se admiten otras respecto a aquellos ficheros automatizados de carácter personal utilizados con fines estadísticos o de investigación científica, siempre y cuando no existan manifiestamente riesgos de atentado a la vida privada de los afectados.

318.10. Importante resulta advertir que la lesión al derecho de intimidad no se da en un acto único que caracterice la afectación, es decir, no se puede encontrar una libertad de intimidad única, sino referida a un valor agredido. Por eso, el bien jurídico "intimidad" no se autoprotege ni defiende por sí mismo, sino que requiere la presencia de algún otro interés vulnerado, como pueden ser, la imagen, el honor, la reputación personal, etc.

En definitiva, precisar el contenido de qué se puede demandar desde el *habeas data*, es decir, saber para qué sirve y qué derechos tutela, es significativo y altamente complejo. No obstante, como punto de partida puede resultar útil el célebre informe "*Data och integritet*" de la Comisión Sueca sobre publicidad y secreto de documentos oficiales que en 1972 sostuvo que:

- No se podía pretender que el derecho a la intimidad fuera considerado un derecho absoluto; el primer límite al mismo se encuentra en el derecho que ostenta la sociedad a exigir a sus miembros las contribuciones necesarias para la realización de los fines comunes y, que…
- Tanto los entes públicos como los privados se encuentran en la necesidad de recoger numerosa información referente a los individuos para cumplir con los diversos fines que les son propios; por ello, toda información relativa a la condición de los individuos puede tener relación con el derecho a la intimidad

318.11. En la legislación comparada la inclusión de la intimidad en el reducto del *habeas data* tiene interpretaciones disímiles.

Colombia, en la Ley Estatutaria 1266 (art. 4°) inciso e) dispone como "Principio de interpretación integral de derechos constitucionales", que:

> La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el *habeas data*, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables.

De este modo, le asigna autonomía al *habeas data* respecto a la intimidad, aunque el proyecto del gobierno después convalidado por la Corte Constitucional, sostuvo que se pretendía proteger la intimidad de las personas asediadas por la creciente utilización de información personal por parte de la administración pública, de entidades financieras, educativas, profesionales u otras organizaciones privadas. Si esta información se da a conocer sin ningún tipo de restricciones, se estaría usurpando la prerrogativa personal de determinar cómo se quiere aparecer, ante quien y en qué

momento. La amenaza principal que se pretende evitar con la reforma sería la de que el individuo pierda el control sobre la propia información y no sepa quién puede hacer uso de ella.[18]

Bolivia, en cambio, al reformar la Constitución con la ley 2061, dice en el art. 23 (actual 21.2 de la Carta Fundamental) que:

> I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de *habeas data* ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.

Aquí la comunión es evidente. Intimidad y datos personales que afecten el derecho de la persona concernida, dejando la acción en manos del afectado, así como la prueba de dicha invasión ilegítima.

El Tribunal Constitucional de Bolivia en la sentencia 0127/2010 dijo al respecto:

> [...] La Constitución Política del Estado vigente cambia el *nomen juris* del *habeas data* a Acción de Protección de Privacidad, pero no así su esencia tutelar, empero contempla algunos cambios específicos en cuanto a su redacción, en especial el art. 130.I, en el que se refiere a los casos de legitimación activa que si bien es muy similar al texto del art. 23.I de CPEabrg, tiene una diferencia notoria cuando afirma; "...Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad" (las cursivas son nuestras). Observamos en primer lugar que se añaden a las personas colectivas como posibles legitimados activos, o futuros accionantes, concibiendo que las personas colectivas también tienen acceso a los derechos reconocidos por el art. 21.2 de la CPE, los cuales son: derecho a la intimidad, a la privacidad, honra, propia imagen y dignidad. Se entiende que el texto del art. 130.I al reconocer como posibles accionantes a personas colectivas, se refiere a aquellas de orden público como privado, pero con algunas diferencias en cuanto a los derechos tutelados para estas, es decir, que las personas colectivas no podrán aducir la vulneración de su derecho a la intimidad personal y familiar, que son derechos fundamentales de índole personal, pero si podrían denunciar la vulneración de sus derechos a la imagen; y reputación.

En *Brasil* la introducción constitucional nunca fue reglamentada, de manera que la figura tomó el curso del *habeas corpus* en la atención procesal, consiguiendo así una suprema restricción en orden al carácter de los derechos que podían entrar en la tutela constitucional.

---

[18] CIFUENTES MUÑOZ, *El habeas data en Colombia,* ob. cit., p. 83.

La intimidad fue dejada de lado, por considerar que el *habeas data* era un derecho personalísimo acotado al titular de la información. Por eso, se vinculó más con la vida privada, y solamente cuando los datos eran inexactos o desactualizados se interpretó que ellos podían alterar la imagen antes que la intimidad individual.

En *Chile*, ha expuesto Nogueira Alcalá, que el tema se ha tomado desde la perspectiva del derecho a la vida privada o de la intimidad afectada por el registro de informaciones en archivos manuales o informáticos que, al permitir socializar, develan ámbitos de la privacidad de las personas.

> […] El respeto a la vida privada e intimidad de las personas adopta un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona; un derecho a la autodeterminación informativa, lo que requiere que las personas puedan conocer la existencia de los ficheros o archivos de registro de información, públicos o privados, sus finalidades y los responsables de ellos, de manera que las personas concernidas puedan conocer los datos contenidos en dichos archivos o ficheros sobre su propia persona, teniendo el derecho de autorizar su recolección, conservación, uso y circulación, como asimismo, el derecho a actualizarla, rectificarla o cancelarla.[19]

En *Ecuador*, antes de la actual ley de jurisdicción y control constitucional, el Tribunal Constitucional sostuvo que toda persona, según el Art. 94 de la Constitución Política de la República, tenía el derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, constaren en entidades públicas o privadas, así como conocer el uso que se haga de ellos y su propósito.

Teniendo como base este derecho consagrado en la Constitución, puede solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación, anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.

En este marco sostuvo que:

> […] el *habeas data* protege el buen nombre, honor, dignidad, buena fama de la persona, y de sus bienes. Concede el derecho a conocer los documentos, bancos de datos o informes que existan sobre su persona o bienes. Y concede finalmente el derecho a solicitar al funcionario correspondiente, la actualización, rectificación, eliminación o anulación si fueren erróneos o cuando afectaren ilegítimamente sus derechos. Mas no puede servir como diligencia preparatoria para la iniciación de un proceso, o para la anulación o eliminación de una obligación, o para afectar el sigilo profesional, o para obstruir la acción de la justicia, o para conocer documentos que sean catalogados como de seguridad nacional, o para eliminar datos o informes que deben mantenerse en archivos públicos o privados.

Tampoco en la legislación actual se menciona a la intimidad como derecho a resguardar, lo que no impide considerar que el derecho a la autodeterminación informativa sea el marco propicio para adecuar la interpretación.

---

[19] NOGUEIRA ALCALÁ, Humberto, *Autodeterminación informativa y habeas data en Chile e información comparativa,* Anuario de Derecho Constitucional Latinoamericano, 2005, pp.460 y ss.

En *Paraguay* la ley de privacidad del año 2000 reglamenta la información de carácter privado" (ley nº 1682). Se refiere solamente a los bancos de datos privados, sin reglamentar los de carácter público, y considera aspectos de la intimidad muy puntuales, como son la intimidad sexual y la doméstica (vida privada)

En *Perú* la acción de *habeas data* tiene sustento constitucional y legal por vía reglamentaria. La intimidad se vincula más con el derecho a la reserva y secreto, con la idea de preservar la confidencialidad de informaciones que puedan afectar a la persoa concernida a su familia

En *Venezuela* se divide el acceso a la información de los derechos que se preservan con el *habeas data*. La distancia de las garantías del artículo 143 de la Constitución que tienen todos los ciudadanos a ser informados oportuna y verazmente por la Administración Pública, sobre el estado de las actuaciones en que estén directamente interesados, y a conocer las resoluciones definitivas que se adopten sobre el particular; es un derecho que si bien consagra la posibilidad de tener acceso a los archivos y registros administrativos, lo es sin perjuicio de los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto. La norma prohíbe, en todo caso, la censura a los funcionarios públicos en relación a lo que informen sobre asuntos bajo su responsabilidad.

> En cuanto al derecho de *habeas data* que consagra el artículo 28 de la Constitución, la Sala Constitucional del Tribunal Supremo de Justicia en su sentencia Nº 1050 del 23 de agosto de 2000 (caso: *Ruth Capriles y otros*), determinó que se trata de un "derecho de las personas a conocer la información que sobre ellas, hayan sido compiladas por otras" consecuencia del hecho de que "tanto el Estado, como los particulares, mediante diversas formas de compilación de datos: manuales, computarizados, etc., registran y almacenan datos e informaciones sobre las personas o sobre sus bienes, y en vista que tal recopilación puede afectar la vida privada, la intimidad, el honor, la reputación, la vida económica y otros valores constitucionales de las personas naturales o jurídicas, la Constitución, para controlar tales registros, otorga varios derechos a la ciudadanía que aparecen recogidos en el artículo".

En *México*, la actual ley federal de "Protección de datos personales en posesión de los particulares", dispone como objeto puntual garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Los sujetos regulados por esta ley, son los particulares, sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de: *a)* Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y, *b)* las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Como se observa, no hay referencia alguna en parte de la ley a la protección de la intimidad, mostrando la suma de legislaciones resumidas, la necesidad de interpretar si a los fines de comprender en la protección de datos personales, la intimidad

es comprendida con amplitud o tiene apego solo a aspectos de ella, como son los derechos que se explanan seguidamente.

318.12. La dispersión legal y la imprecisión de la jurisprudencia, pone de relieve dos tendencias en el plano de la intimidad y los datos personales. Una que asienta el contenido como un bien personal, un derecho subjetivo individual que no se transfiere ni negocia, y que por esa calidad de "derecho personalísimo" obtiene, respecto al tema que nos ocupa, una característica determinante: el ser posesión exclusiva y excluyente de la persona humana. Y otra que se atiende en relación a la intimidad afectada cuando son otros los que proyectan dicha afectación.

En la primera línea, solo el individuo puede resolver, sin interferencias ni perturbaciones, qué aspectos de su vida admite compartir y que pensamientos, sentimientos o hechos de su vida interior pretende que otros conozcan.

Para Herrán Ortiz:

> estas características facultan a que el derecho a la intimidad pueda ser un bien un derecho libremente determinado por la persona, permitiendo que ésta resuelva cuándo y hasta qué medida quiere exteriorizar su vida y ponerse en contacto con la sociedad. Como complemento de la existencia del ser humano debe ser protegido, en tanto que ha de considerarse esencial que cada individuo conserve una esfera de libertad y autonomía que pueda defender frente a intromisiones externas. Las manifestaciones concretas del derecho a la intimidad pueden transformarse con el transcurso del tiempo y a buen seguro que en el futuro se defenderá una idea diferente de la que actualmente se sustenta de este derecho.[20]

La intimidad es entonces el género desde el cual se pueden bajar otras manifestaciones como la vida privada, familiar, el derecho al secreto, al honor, a la imagen, etc. Es algo propio que se dispone con libertad; pero al mismo tiempo, es una obligación de los demás hacia ese derecho, y por tanto, se configura como un derecho de defensa y garantía esencial para la condición humana.

> Los derechos fundamentales deben considerarse garantías de la autonomía individual, derechos de defensa frente a las injerencias de los poderes públicos en la esfera privada de cada persona. Además, constituyen garantías jurídicas esenciales para el mantenimiento del orden y la paz económico-social. Si bien entre ellos se pueden observar notas comunes —afirma Herrán Ortiz— cada derecho representa una categoría independiente y, consecuentemente, debe ser interpretado y aplicado en forma autónoma. La esencia y naturaleza del derecho a la intimidad permiten su consideración como un derecho de defensa; se trata de una defensa en principio ilimitada y frente a toda injerencia en la esfera de la persona que debe permanecer reservada en su interior.[21]

Tanto se permite reclamar por la defensa de la intimidad violada o amenazada; cuanto se puede exigir del Estado que prevenga eventuales intromisiones que lesionen ese derecho personalísimo.

---

[20] HERRÁN ORTÍZ, ob.cit., p. 155.

[21] HERRÁN ORTIZ, ob. cit., p. 156.

318.13. En este sentido, el *habeas data* puede ser la garantía procesal adecuada para ciertos aspectos del derecho a la intimidad; pero el proceso es un remedio *ex post facto* que ofrece soluciones a situaciones ya padecidas; lo importante será actuar en la etapa previa, formando y concientizando para que los derechos se promuevan y ejecuten conforme sus premisas e ideales lo contemplan.

Sostiene el Tribunal Constitucional español que:

> los derechos fundamentales no incluyen solamente derechos subjetivos frente al Estado, y garantías institucionales, sino también deberes positivos de parte de éste. Pero, además, los derechos fundamentales son los componentes estructurales básicos, tanto del conjunto del orden jurídico objetivo como de cada una de las ramas que lo integran, en razón de que son la expresión jurídica de un sistema de valores que, por decisión del constituyente, ha de informar el conjunto de la organización jurídica y política [...]. La garantía de su vigencia no puede limitarse a la posibilidad del ejercicio de pretensiones por parte de los individuos, sino que debe ser asumida también por el Estado. Por consiguiente de la obligación de sometimiento de todos los poderes a la Constitución no solamente se deduce la obligación negativa del Estado de no lesionar la esfera individual o institucional protegida por los derechos fundamentales, sino también la obligación positiva de contribuir a la efectividad de tales derechos, y de los valores que representan, aun cuando no exista una pretensión subjetiva por parte del ciudadano (STC, 53/85, sentencia del 11 de abril de 1985).

318.14. En suma, asentar el piso de marcha del proceso de *habeas data*, a partir de la tutela de la intimidad, supone privilegiar la libertad de las personas para resolver qué aspectos de su vida permite se hagan públicos a través de la información compilada o la difusión consecuente.

A estos fines, la sola invasión en la vida privada o en la esfera de la intimidad permite considerar afectado el derecho a la intimidad, sin que resulte necesario buscar donde se encuentra la lesión individual.

Esta sustentación reconoce la exigencia constitucional para que el Estado garantice dicha libertad; y como acción frente a otro, a quien se reclama para que revele el conocimiento de los datos archivados y, en su caso, para que los conserve actualizados, los reserve en el marco de la confidencialidad o los suprima como un derecho derivado de la potestad de autodeterminación informativa.

318.15. La segunda línea que se contrapone a la anterior, atiende a la intimidad como un derecho personalísimo proyectado "hacia otros". La base que razona este derecho no supone caracterizarlo, estrictamente, como un derecho subjetivo. Vale decir, como una potestad exclusiva y excluyente de la actividad de otros; ni exigir de ello la mentada relación entre daño directo y efectivamente sufrido que admite la intervención jurisdiccional.

Si fuera mantenida la condición para el ejercicio del derecho, evidentemente, poco se habría avanzado porqué la lesión a la intimidad, muchas veces, es ocasional o circunstancial y hasta puede no existir, toda vez que se trata de una estimación puramente subjetiva.

La defensa que promete el *habeas data* no está circunscripta al daño, ni siquiera lo exige, como tampoco se requiere ilegalidad o arbitrariedad para los actos que recopilan la información individual. En los hechos, si la garantía pervive en la libertad de decidir sin interferencias sobre nuestra vida privada o familiar —entro otros— es evidente que el derecho se proyecta también a determinados aspectos de otras personas con las que se mantiene una estrecha vinculación, sea familiar o de amistad, y que como tales, inciden en la esfera de la personalidad.

> Resulta significativo -informa Herrán Ortiz- que el Tribunal Constitucional en su sentencia del 15 de noviembre de 1991 considere el derecho a la intimidad no como algo privativo de la vida de cada individuo, sino que también reconozca la existencia de circunstancias que sin afectar directamente al individuo son susceptibles de ser protegidas acudiendo al derecho a la intimidad que todo individuo ostenta. Sin embargo —agrega— el derecho a la intimidad no constituye, en modo alguno, un derecho absoluto, antes bien, se encuentra limitado, además de por el necesario respeto al derecho de los demás, por la necesidad de preservar otros bienes constitucionalmente protegidos que responden a una demanda de la sociedad cada vez más avanzada y en constante desarrollo.[22]

318.16. Ahora bien, este diseño obliga a investigar la naturaleza de la defensa que trae el *habeas data* y la legitimación procesal que admite y reconoce, porque si no es un derecho personal ni colectivo; tampoco difuso o de incidencia colectiva; aun cuando sea personalísimo con ampliaciones en la cobertura "hacia otros", es evidente que estamos ante un nuevo derecho, una novedosa garantía que no puede capturar su naturaleza jurídica tras la silueta del amparo tradicional.

Un ejemplo de las causas que obliga a sincerar la amplitud del *habeas data* se muestra con el fenómeno de las redes mundiales de comunicación y el ámbito del comercio electrónico que, por su propia globalización, necesitan una respuesta igualmente universal.

> Informa Ulf Brüehann (miembro de la Comisión Europea y Director de la Unidad "Libre flujo de la información y la protección de datos, incluyendo aspectos internacionales", que el trabajo de la World Wide Web Consortium se orienta hacia la elaboración de una tecnología de filtración (conocida como P3P), gracias a la que los usuarios de Internet podrían regular su propio acceso a páginas web en función de sus propias preferencias de intimidad. Los protocolos técnicos que se trabajan tienen un efecto directo en el nivel de intimidad del que disfrutarán los usuarios de la línea en años venideros.[23]

318.17. Lo mismo, aunque desde otra perspectiva, ocurre con los organismos que se ocupan de la defensa de los derechos humanos, sean organizaciones no gubernamentales o el propio Defensor del Pueblo (ombudsman), en la medida que tienen legitimación procesal suficiente basada en las actividades que celebran.

---

[22] HERRÁN ORTIZ, ob. cit., p. 158.

[23] BRÜEHANN, Ulf, *La escena internacional y la directiva comunitaria: 5 semanas antes de su entrada en vigor,* en XX Conferencia Internacional de autoridades de protección de datos (1998), Agencia de Protección de Datos, Madrid, 1999, p. 85..

Además, es obvio que la soledad intrínseca del derecho individual no puede ir contra los retos continuos de la acumulación de datos admitidos a sabiendas o sin ella, pues la utilización de tecnologías cada vez más avanzadas impone un tratamiento general que juzgue la pertinencia de esa actividad recolectora que invade permanentemente la intimidad de las personas.

El Parlamento Europeo ha manifestado, reiteradamente, que el tratamiento de datos no puede reducirse a una mera defensa de los derechos individuales ofreciendo al afectado la única posibilidad de accionar, pues esa actitud significaría dejarlo auténticamente solo, sin ninguna defensa comunitaria.

> Resumiendo —agrega Estadella Yuste— se puede decir que en un primer momento los instrumentos internacionales de derechos humanos no recogían expresamente el derecho a la protección de datos o autodeterminación informativa, sino tan sólo un derecho "a la vida privada" o a la intimidad personal. Posteriormente éste se ha ido desarrollando y paulatinamente se han adoptado otros instrumentos internacionales reconociendo el derecho a la protección de datos. Ello es importante porque, si la protección de datos sólo se hubiera plasmado en leyes de ámbito nacional, habría sido más difícil que la comunidad internacional lo considerara como un derecho individual.[24]

319. El derecho al honor

319.1. Reconoce una larga prosapia el derecho al honor. Aparece en las XII Tablas —*carmen famosum—,* se encuentra en el derecho romano, en la Grecia antigua y fue motivo central de buena parte de la historia del mundo, confiar en las personas honorables.

Honradez y dignidad personal son premisas del Fuero Juzgo, y las Leyes de Partidas las establecen como principios generales del derecho.

> En las grandes universidades del Renacimiento (París, Pavia, Salamanca, Coimbra) se comentaron las frases de la "Summa" de Santo Tomás sobre la vida, la integridad corporal, la tranquilidad espiritual, el honor y la fama. Las lecciones de Vitoria —dice Concepción Rodríguez—, llenas de vida y de sentimiento humano, despiertan el interés general. Soto expondrá con su habitual concisión y exactitud sistemática, la nueva doctrina de los bienes intrínsecos de la persona. Dice que el hombre tiene tres géneros de bienes: 1. La vida; 2. Honor y fama, y 3. Los bienes temporales.
>
> El hombre tiene el dominio de su honor y fama, pero no puede usarlos como el dinero, porque su valor es superior; aquellos bienes son más nuestros. Honor y fama a los que, por eso, colocará no en el orden de la vida, sino en el de los bienes externos.[25]

Tiempo después, los códigos civiles desatienden la esencia de este derecho personalísimo, quizás influidos por la condición de derecho fundamental que le otorgó la Declaración de los Derechos del Hombre.

En suma, podemos afirmar que las normas sustanciales no se han detenido cuidadosamente en la reglamentación de los derechos de la personalidad hasta

---

[24] ESTADELLA YUSTE, ob. cit., p. 23.

[25] CONCEPCIÓN RODRÍGUEZ, José Luis, *Honor, intimidad e imagen,* Bosch, Barcelona, 1996, p. 18.

bien avanzado el presente siglo, que coincide con su caracterización como derecho constitucional.

319.2. Ahora bien, ¿puede ampararse al honor desde el *habeas data*?

En principio la respuesta sería negativa, pero no absoluta. Por varios motivos. Uno de ellos proviene de la misma ley argentina (nº 25.326) cuyo artículo 1º establece que "*el habeas data garantiza el derecho al honor*", tomado de la legislación española con igual alcance; otra razón es la naturaleza del proceso que sólo se ocupa de la invasión a la persona que resulta arrebatada en sus datos que se recopilan y transfieren provocando una crisis en el derecho a la identidad. No obstante, la identidad es una parte del honor, pero no es el honor en sí mismo.

La identidad se distingue también de la intimidad: aquella asegura la fiel representación de la propia proyección social; ésta, la no representación al exterior de las propias vicisitudes personales, cuando un tercero no posee un interés socialmente apreciable, tal como lo sostiene Herrero Tejedor.[26]

Es verdad que definir al honor arrastra complejas disquisiciones y opiniones dispares. Por un lado, de manera general, se hallarían implicados valores como la intimidad, la buena fama, la reputación, el respeto propio y ajeno, la consideración familiar y social, y en definitiva, es propiamente un sentimiento propio sobre nuestra persona y una estima de los demás hacia nosotros.

Desde esta perspectiva, se trata de observar qué es lo intolerable cuando el honor se afecta, y qué puede admitirse aun existiendo un perjuicio contra el derecho de la personalidad.

> Este es el criterio predominante: la doble conceptuación que distingue el honor como resultado del juicio de valor que los demás hombres hacen de nuestras cualidades (honor objetivo), y como el sentimiento y la conciencia del propio honor: las representaciones que el sujeto tiene de sí mismo —conciencia del honor— y la voluntad de afirmar su propio valor —sentimiento del honor—.
>
> Resumiendo ambas nociones, De Cupis define el honor como el íntimo valor moral del hombre, la estima de los terceros, o bien la consideración social, el buen nombre o buena fama, así como el sentimiento y conciencia de la propia dignidad.[27]

319.3. Otra visión llega de su significado etimológico. La Real Academia dice que el honor es una *cualidad moral que nos lleva al más severo cumplimiento de nuestros deberes,* mientras que la honra se la define como la *estima y respeto de la propia dignidad.*

De esta lectura surge un honor *subjetivo*, propio, que se vincula con la autoestima o propia consideración (dignidad personal); y otro aspecto *objetivo* que es el respeto que de nosotros tienen los demás: la reputación, en definitiva.

> La concepción jurídica actual, de acuerdo con las enseñanzas cristianas —apunta Concepción Rodríguez—, considera que el honor es inherente al hombre; es un reflejo

---

[26] Herrero Tejedor, Fernando, *Honor, intimidad y propia imagen,* Colex, Madrid, 1990, p. 56.

[27] De Cupis, Adriano, *Il diritti Della personalità,* Giuffré, Milano, 1982, p. 166.

de la personalidad y uno de los derechos esenciales que le dan contenido. A toda persona corresponde un mínimo de responsabilidad y honorabilidad, que debe ser protegida por el orden jurídico.

Nadie, indica Alfredo Orgaz, está *a priori* excluido de esa tutela, ni siquiera las personas deshonestas o de mala reputación; también éstas pueden ser sujeto pasivo de un delito contra el honor, siempre que de acuerdo con las circunstancias, el ataque debe ser considerado como ilegítimo esto es, como no justificado por un interés superior. La inviolabilidad de la integridad moral, como la protección de los demás derechos naturales, no es absoluta e ilimitada.[28]

319.4. La defensa del honor esta mejor diseñada en el derecho penal. En este, el análisis recae sobre cuestiones fácticas que conducen a tipificar un delito preestablecido (*v. gr.:* calumnia, injuria). El derecho a ser respetado, se afinca asimismo en la Constitución, pero siempre calificando la ofensa como un hecho a comprobar, y al honor como un derecho subjetivo (individual).

Algunos autores —dice Cifuentes— han negado la existencia de un derecho subjetivo al honor. En particular aquellos que no reconocen los derechos personalísimos. Ennecerus, por ejemplo, dice que el honor es el reconocimiento del valor de una persona por sus contemporáneos, pero que ese concepto no pertenece al derecho y, en cambio, tiene una significación, moral y jurídica el honor civil, o grado de estimación y reconocimiento del valor que corresponde a todo hombre intachable.[29]

En cambio, no se repara la autoestima, es decir, la consideración que uno tiene sobre sí mismo y que entiende afectada por actos de otros.

La ley penal califica como "injuria", en la tipicidad requerida, la lesión al derecho subjetivo del honor; mientras que es "calumnia" la forma objetiva de agraviar la honra.

Las normas constitucionales no definen el derecho a defender el honor, sólo asignan una garantía procesal contra toda acción o amenaza que lesione la fama, el prestigio, la consideración, la dignidad, la reputación, el crédito, o el sentimiento de estima, por enumerar algunas de las probables alegaciones del interés dañado.

La norma constitucional argentina adopta una fórmula amplia, ya que no enuncia cuál es el bien jurídico protegido, tan sólo se limita a señalar que actúa frente a supuestos de "falsedad" o "discriminación", dejando abierta la posibilidad de inferirlo en cada caso concreto. Quizá por apresuramiento —dice Sagüés— el nuevo texto constitucional contempla el *habeas data* para supuestos de "falsedad" o "discriminación", en custodia de los valores verdad e igualdad; y no para otras hipótesis clásicas de esta figura como la protección del honor o privacidad.[30]

Como regla, la protección llega después de los hechos tornándose inevitablemente en un derecho indemnizatorio. A veces, la reparación se consigue con la

---

[28] CONCEPCIÓN RODRÍGUEZ, ob. cit., p. 23.

[29] CIFUENTES, Santos, *Derechos personalísimos,* Astrea, Buenos Aires, 1995, p. 76.

[30] SAGÜÉS, Néstor Pedro, *Subtipos de habeas data,* J.A., 20/12/95, p. 2

publicación de la sentencia que condena al difamador, pero es evidente que la tacha ya se produjo. En pocas palabras, no hay sentido preventivo en nuestra legislación positiva.

319.5. En la jurisprudencia generada desde el *habeas data*, a pesar de lo expresado, se ha hecho lugar a la defensa del honor aun cuando no se lo diga abiertamente.

En efecto, en la causa "*Gutiérrez, Héctor R. c/ Casino Militar del Personal Superior de la Base Naval Puerto Belgrano"*[31] se sostuvo que la acción no procedía si no estaba demostrado "*prima facie*" el motivo descalificante o discriminatorio que le impedía a un oficial de la Marina argentina ingresar al Casino Naval de su puerto de destino. Sin embargo, se advirtió que "la denegatoria de la admisión como socio en un club en el caso, Casino Militar no esta incluida dentro de los presupuestos de procedencia de la acción de *habeas data*, salvo que para tal negativa se haya tenido en cuenta algún dato descalificante o discriminatorio que conste en sus propios archivos, categoría que no alcanzan ni el listado de socios ni el registro de pago de cuotas".

En otra sentencia, se alegó que "la información que brinda la demandada (empresa de transmisión de datos con fines comerciales) no puede incursionar en el terreno del honor e intimidad de los actores y con ello resultar discriminatoria en su vida de relación por orientarse a actividades de índole estrictamente comercial y crediticia".[32] Con ello dio a entender que la simple información registrada y difundida a quien le adquiere el dato, si ella no es incorrecta ni desactualizada, no provoca discriminación ni afectación a las personas referidas, toda vez que la información transmitida es cierta.

La Corte Suprema de Justicia de la Nación sostiene que "artículo 43, párrafo tercero de la Constitución Nacional, ha incorporado un nuevo derecho a la protección de los datos personales frente a cualquier intromisión arbitraria o abusiva que pudiera implicar una violación a la intimidad y a los demás derechos constitucionales, hallándose en íntima relación con el derecho a la integridad, a la dignidad humana, a la identidad, al honor, a la propia imagen, a la seguridad, al de peticionar, a la igualdad, a la libertad de conciencia, a la libertad de expresión, a la libertad de reunión, de asociación, de comerciar y con cualquier otro que pudiera resultar afectado".[33]

Posteriormente, se dijo: "el *habeas data* —en tanto garantía de un derecho individual, personalísimo—, sólo puede ser ejercida por el titular del derecho a interponer la acción, en defensa de aspectos de su personalidad, vinculados con su intimidad, que no pueden encontrarse a disposición del público ni ser utilizados sin derecho".[34] También agregó que "la garantía del *habeas data* —dirigida a que el particular tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga—, forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad".

---

[31] Cámara Federal de apelaciones de Bahía Blanca, Sala 1, 1994/12/30.

[32] CNCiv., Sala A, 1997/09/07, "*Pochini, Oscar y otro c/ Organización Veraz S.A.*", La Ley Online.

[33] CS, 1998/8/13, voto del Dr. Boggiano, en "*Suárez Mason, Carlos G.*", La Ley Online.

[34] CS, 1998/12/15, voto del Dr. Fayt en la causa "*Urteaga, Facundo R. c/ Estado Mayor Conjunto de las Fuerzas Armadas*", La Ley Online.

La existencia y publicidad de datos desactualizados y erróneos relacionados con el actor deben haber repercutido en su espíritu, sentimientos o afecciones más íntimas, ya que implicaron un ataque a su honor, a su imagen y reputación; máxime si se tiene en cuenta la extensa labor profesional y académica del actor. Tales circunstancias, justifican sin hesitación la procedencia del daño moral. ("Ravina, Arturo Octavio c/ Organización Veraz S.A.". CNCiv., Sala F, 06/02/02 - ED, 197-265).

El Banco que por error comunicó al Banco Central la inhabilitación de una persona creyéndola cliente de la institución, se halla incurso en responsabilidad aquiliana, ya que no la une ninguna relación contractual con la damnificada y, en consecuencia, deberá reparar el daño causado por el ilícito (art. 1067 Cód. Civil). Esto es, haber quedado sindicado en el Banco Central y en las empresas que brindan informes como "deudor irrecuperable". Debe responder el responsable por el agravio moral causado en razón del descrédito en la solvencia moral y económica que a raíz de ello se sufrió (CNCom., Sala B, 12/03. "Pereyra, Héctor Alberto c/ Citibank NA s/ Sumario").

Es claro que la publicación de aquellos datos erróneos -atribuibles a la demandada- y, además, por tan prolongado tiempo tienen que haber repercutido en el espíritu y en los sentimientos o afecciones más íntimas del actor ya que implicaron un ataque a su honor, a su imagen y reputación. ("Fallone, Eugenio Donato c/ HSBC Banco Roberts S.A. s/ daños y perjuicios". CNCivil, Sala F, 06/11/03. Expte. Nº 368.998).

319.6. Observemos ahora como juega el conjunto normativo que tenemos. En primer lugar, el *Pacto de San José de Costa Rica* en su artículo 11 determina:

Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2) Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; 3) Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

De esta convención surge el derecho al honor como una expresión natural de los derechos humanos; pero de poco sirve si no cuenta con la herramienta precisa que le otorgue una particular fisonomía.

La Declaración Universal de Derechos Humanos establece: "Artículo 12: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Es similar la redacción del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

En conjunto, todas estas normas llevan a sostener que, sea considerado el derecho al honor y a la honra como un derecho del hombre o como un derecho subjetivo público, en ambos casos es un límite a la actuación de otros sobre nuestra persona y una obligación del Estado aportar la garantía procesal.

Cabe agregar que ni de los pactos ni de las convenciones incorporadas por los llamados bloques de constitucionalidad surge que sea el *habeas data* la vía reglamentaria que se espera para la tutela del honor.

319.7. En Argentina el Código Civil contiene varias disposiciones: Art. 1089: "Si el delito fuere de calumnia o de injuria de cualquier especie, el ofendido sólo tendrá derecho a exigir una indemnización pecuniaria, si probase que por la calumnia o injuria le resultó un daño efectivo o cesación de ganancia apreciable en dinero, siempre que el delincuente no probare la verdad de la imputación"

De esta amplia manifestación ("…*injuria de cualquier especie*…) se podría interpretar que anida allí el "*habeas data*". ¿Es ello correcto?

Pareciera que no. La previsión legal se sostiene en el delito (art. 1072) y una vez lograda la sentencia condenatoria, la obligación se desenvuelve como indemnización y no como un deber de realizar tal o cual acto, como correspondería al *habeas data*.

La *exceptio veritatis* le agrega un elemento más al fundamento, pues si la garantía procesal que se tiene para evitar la manipulación de nuestros datos lleva implícita la idea de proteger la intimidad personal, es probable que permitiendo que el delincuente (¿es delincuente quien registra datos o los transfiere aun a sabiendas del error informativo?) pruebe la verdad de sus dichos (o registros, por el caso), se deje expuesto al honor a una expoliación mayor.

Sostiene Cifuentes que:

> hay que defender hoy como nunca a la persona. Se extienden a diario, introduciéndose en el hogar mismo, los sistemas difusivos con nuevas formas de ataque, con una extraordinaria perfección en las comunicaciones, las noticias, los entretenimientos visuales y radiales. Se pretende, en no pocas ocasiones, halagar al público e interesarlo moviendo bajos instintos, haciendo fáciles y desdorosas apologías, destruyendo honras y respetabilidades, o sacando gavetas de la historia de anécdotas risueñas, trágicas y mortificantes. Bastaría probar la realidad celosamente guardada para conservar la impunidad. De ahí que al intérprete de una norma como el artículo 1089 le corresponda restringir el ámbito de la *exceptio veritatis*.[35]

El artículo 1090 agrega:

> Si el delito fuere de acusación calumniosa, el delincuente, además de la indemnización del artículo anterior, pagará al ofendido todo lo que hubiese gastado en su defensa, y todas las ganancias que dejó de tener por motivo de la acusación calumniosa, sin perjuicio de las multas o penas que el derecho criminal estableciere, tanto sobre el delito de este artículo como sobre los demás de este capítulo.

319.8. ¿Se aplica el precepto al *habeas data*? Una vez más el mismo interrogante. ¿Puede considerarse calumniosa la difusión de datos equivocados, parciales o desactualizados? En principio, parece que no, porque la norma refiere a la acción realizada a sabiendas y con intención de dañar, sin tener relación con la actitud imprudente, ligera o precipitada de quien transmite un dato sin haberlo confirmado. No obstante, esta actitud culpable podría repararse por el artículo 1109 del Código Civil argentino.

---

[35] CIFUENTES, ob. cit., p. 133.

Resulta así que la acción de *habeas data* se afinca en un preciso punto de referencia, que de por sí es acotado (conocer el dato, y requerir su actualidad, supresión o rectificación) y no podría transferirse hacia otros que cuentan ya con una vía procesal de protección.

De todos modos, el honor se puede afectar con la transmisión de datos sensibles o que impliquen alguna forma de discriminación (por ejemplo: la raza o el origen étnico), en cuyo caso la garantía constitucional es procedente para tutelar a la persona concernida; como también lo es el proceso civil reparatorio del perjuicio emergente. Serían las denominadas vías concurrentes que no pueden impedir el progreso del *habeas data*.

319.9. En suma, lo que queremos significar es que aun cuando la protección del honor y la reputación puedan tener respuestas en el ordenamiento positivo actual, es bien sabido que la actuación es posterior al hecho y obra como sanción al ofensor y como reparación para el ofendido.

En cambio el *habeas data* puede servir indirectamente para estos derechos personalísimos, en la medida que la afectación puede prevenirse desde los objetivos que tiene la garantía procesal.

Una vez más se advierte la omisión de la norma reglamentaria porque nada ha dicho al respecto, aunque al sostener que persigue el "*restablecimiento del pleno ejercicio de los derechos a que se refiere la presente ley*", puede colegirse alguna amplitud, teniendo en cuenta que, a diferencia de otras cartas constitucionales, la argentina no consagra explícitamente la defensa al honor, a la buena reputación, a la intimidad personal y familiar, a la propia imagen, al buen nombre, etc. que son cuestiones que, hipotéticamente, podrían argumentarse desde el *habeas data*.

Sostiene Bidart Campos:

> […] que el *habeas data* haya surgido y funcione habitual y normalmente como garantía para preservar la autodeterminación informativa y la privacidad de datos personales no alcanza para agotar su funcionamiento en esa dirección: toda garantía constitucional debe ser tan *elástica* cuanto la realidad de una situación determinada lo demande; y ello a efectos de que rinda su efecto tutelar respecto del derecho que a través de esa misma garantía se pretende. Como en tantas otras cosas, nada de rigideces, estrangulamientos, reduccionismos, ni cosa semejante. Las garantías deben holgarse y si, acaso, nunca antes nos imaginamos que íbamos a precisar alegar un "derecho" a la verdad y a los datos de víctimas desaparecidas, ahora que se hizo necesario hay que buscar con aperturismo y activismo procesal y judicial la mejor vía conducente —en cada caso— para que haya una —o más— garantías a disposición de quien invoca aquel derecho. Si las garantías no sirven para el fin por el cual existen, no sirven para nada. Y esto no es tolerable ni admisible.[36]

319.10. En Latinoamérica la ubicuidad del honor en la dimensión del *habeas data* tiene la misma contingencia que sufre la intimidad.

---

[36] BIDART CAMPOS, Germán J., *¿Habeas data o qué? ¿Derecho a la verdad o qué?,* La Ley, 1999-A, 212.

El Tribunal Constitucional de *Bolivia*, por ejemplo, dice que:

> […] si bien el derecho a la imagen, a la honra y a la reputación, parecieran estar dentro del mismo grupo de derechos tutelados por la acción de protección de privacidad, en el caso de las persona colectivas, sólo podrían denunciar la vulneración de los derechos a la imagen y la reputación, pero no así de la honra, debido a que el derecho a la honra es de índole estrictamente personal, es decir, entra dentro de la esfera de la personalidad y es concebido doctrinalmente como la pretensión de respeto que corresponde a cada persona como reconocimiento de su dignidad frente a la sociedad.[37]

De su lado, la Corte Constitucional de *Colombia* en su Sentencia T-412 al referirse al derecho a la honra estableció lo siguiente: "El concepto de honra se debe construir desde puntos de vista valorativos y, en consecuencia, con relación a la dignidad de la persona. Desde dicha perspectiva la honra es un derecho de la esfera personal y se expresa en la pretensión de respeto que corresponde a cada persona como consecuencia del reconocimiento de su dignidad".

Cuando las norma constitucional consagra específicamente la protección del derecho a la honra, entendiendo por ella, la estimación o deferencia con la que cada persona debe ser tenida por los demás miembros de la colectividad que le conocen y le tratan, en razón a su dignidad humana; tienen un derecho que debe ser protegido con el fin de no menoscabar el valor intrínseco de los individuos frente a la sociedad y frente a sí mismos, y garantizar la adecuada consideración y valoración de las personas dentro de la colectividad.

> Ahora bien, los derechos al buen nombre y a la honra son derechos que se ganan de acuerdo a las acciones realizadas por el individuo, sea que en virtud de ellas pueda gozar del respeto y admiración de la colectividad como consecuencia de su conducta intachable; criterio que es compartido por la jurisprudencia del Tribunal Constitucional de Bolivia, que en su SC 0686/2004-R de 6 de mayo establece que: "Según la doctrina del Derecho Constitucional el derecho a la honra, es la estimación o deferencia con la que cada persona debe ser tenida y tratada por los demás miembros de la colectividad que le conocen; es el derecho que tiene toda persona a que el Estado y las demás personas reconozcan y respeten la trascendencia social de su honor. Es un derecho que se gana de acuerdo a las acciones realizadas por cada persona, de manera que en virtud de ellas pueda gozar del respeto y admiración de la colectividad como consecuencia de su conducta correcta e intachable acorde con valores de la ética y la moral, o, por el contrario, carezca de tal imagen y prestigio, en razón a su indebido comportamiento social; cabe advertir que la honra, se constituye en una valoración externa de la manera como cada persona proyecta y presenta su imagen; de manera que las actuaciones buenas o malas, son el termómetro positivo o negativo que la persona irradia para que la comunidad se forme un criterio objetivo respecto de la honorabilidad de cada ser; pues las buenas acciones acrecientan la honra, las malas decrecen su valoración. En este último caso se entiende que no se puede considerar vulnerado el derecho a la honra de una persona, cuando es ella misma quien ha impuesto el desvalor a sus conductas y ha perturbado su imagen ante la colectividad".

---

[37] Tribunal Constitucional de Bolivia, sentencia 0127/2010.

En consecuencia cuando la honra no tiene inserción constitucional cuadra atender el bloque de constitucionalidad, porque el derecho sí lo está en los arts. 12 de la Declaración Universal de Derechos Humanos; 5 de la Declaración Americana de Derechos y Deberes del Hombre; 17 del Pacto Internacional de Derechos Civiles y Políticos; y 11 de la Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica.

En *Bolivia*, como se dijo, la diferencia entre una y otra acción deriva de la diversidad entre la acción de protección de privacidad y el *habeas data*, pero que puede empalmar dentro del nuevo marco constitucional.

> La Sentencia Constitucional 0965/2004-R de 23 de junio, con el objeto de lograr una cabal comprensión de la naturaleza jurídica del *habeas data* señaló entre sus aspectos más importantes, los siguientes: "[…] Siguiendo la doctrina del Dr. José Antonio Rivera Santivañez en su obra *Jurisdicción Constitucional*, se definió el *habeas data* "como el proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la 'autodeterminación informática'", explicando a continuación que, es una garantía constitucional que, sin desconocer el derecho a la información, al trabajo y al comercio de las entidades públicas o privadas que mantienen centrales de información o bancos de datos, reivindica el derecho que tiene toda persona a verificar qué información o datos fueron obtenidos y almacenados sobre ella, cuáles de ellos se difunden y con qué objeto, de manera que se corrijan o aclaren la información o datos inexactos, se impida su difusión y, en su caso, se eliminen si se tratan de datos o informaciones sensibles que lesionan su derecho a la vida privada o íntima en su núcleo esencial referido a la honra, buena imagen o el buen nombre".

320. El derecho a la propia imagen

320.1. Seguramente en los tiempos actuales la comprensión del concepto de "imagen" se encuentra afectada por la idea de apariencia sobre lo que uno es y representa ante los demás. Antes, la imagen era una pertenencia de la persona que se violaba cuando, sin consentimiento, se reproducían sus rasgos físicos en forma reconocible a través de un soporte material cualquiera. Hoy la reputación se forja también desde la apariencia transmitida.

Es decir, ambas facetas se ocupan de proyecciones distintas de un mismo derecho. Mientras la imagen es el derecho que uno conserva para mostrarse ante los demás, y como tal, es un derecho intrínseco de la intimidad; el otro es el poder estrictamente individual de impedir el uso de nuestra fisonomía a través de un medio de reproducción cualquiera.

> La invención de la fotografía y el grabado, así como el extraordinario desarrollo que en la vida moderna ha alcanzado la publicidad y la propaganda mercantil e industrial plantearon, a partir del siglo pasado, según dice Concepción Rodríguez —siguiendo a Castán Tobeñas— la cuestión del derecho a la imagen.[38]

---

[38] CONCEPCIÓN RODRÍGUEZ, ob. cit., p. 27.

320.2 Sin embargo, esta es una distinción no aceptada en legislaciones donde el "derecho a la propia imagen" se construye como límite específico de las libertades de expresión e información.

En España doctrina de las más calificadas sostiene que el derecho a la propia imagen:

> […] es un derecho innato de la persona, derecho que se concreta en la reproducción o representación de la figura de ésta, en forma visible y reconocible. Es un derecho subjetivo de carácter privado y absoluto. Es un derecho personalísimo, pero dotado de un contenido potencialmente patrimonial en cuanto que a través de su ejercicio pueden obtenerse bienes económicamente valorables, y además en cuanto a la posible indemnización pecuniaria en el caso de su violación. Es un derecho inalienable; como tal irrenunciable, y en general, inexpropiable. Es un derecho intransmisible *mortis causa*, bien que su tutela post mortem corresponda fundamentalmente a los más próximos parientes del difunto. Es, en fin, un derecho imprescriptible.[39]

En tal sentido, por constituir la exteriorización de la imagen una misteriosa impronta de la personalidad, nadie, sin estar debidamente autorizado, puede propagar mediante ilustraciones la efigie de una persona aunque ella se muestre en público y el público la conozca. Y este razonamiento no meramente especulativo, lleva a la conclusión de que no son los bienes jurídicos del honor ni del secreto personal el contenido propio y genuino del derecho a la propia imagen; porque la reproducción arbitraria de una figura humana puede no lesionar el honor de la persona reproducida, ni quebrantar el secreto de una vida privada cuando se trata de exhibición popular *ad incertas personas*, en ellos desaparece aquel secreto o derecho a la reserva de la figura humana.

El Tribunal Constitucional español ha dicho que:

> los derechos a la intimidad personal y a la propia imagen, garantizados por el artículo 18.1 de la Constitución, forman parte de los bienes de la personalidad que pertenecen al ámbito de la vida personal y familiar que queda sustraído a intromisiones extrañas. Y en este ámbito de la intimidad, reviste singular importancia la necesaria protección a la propia imagen frente al creciente desarrollo de los medios y procedimientos de captación, divulgación y difusión de la misma y de datos y circunstancias pertenecientes a la intimidad que garantiza este precepto.[40]

320.3 El derecho a difundir el nombre o la fotografía de una persona sin ocasionarle molestias o perjuicios depende en gran medida de la subjetividad que el individuo tenga respecto a su vida privada. Una persona cualquiera tiene derecho a que se la proteja en su vida y en su propiedad, y actualmente el primero ha llegado a significar el derecho a disfrutar de la vida, sin la publicidad o perturbación de una encuesta organizada sin autoridad. Los tribunales aseguran aquél derecho "a ser dejado en paz" que recuerda el derecho a estar a solas, propio de la privacidad.

---

[39] GITRAMA GONZÁLEZ, Manuel, *Derecho a la propia imagen*, SEIX XI, Madrid, 1962, p. 66.

[40] STC, 170/87.

Los derechos íntimos deben ser respetados al igual que los deseos y sensibilidades de la gente, los que pueden vulnerarse cuando se afecta la esfera inalienable de la imagen que ante los demás se tiene.

Ahora bien, la imagen se extiende a otras manifestaciones y perseguir una defensa particular en cada caso. En una primera etapa (1839/1900) el derecho se relaciona con la propiedad intelectual y artística. Después (1900/1919) comienza a considerarse como un derecho esencial de la persona: es un atributo de la personalidad

Sostiene Marcela Basterra, a quien seguimos en esta división de períodos para el reconocimiento del derecho a la imagen, que:

> en 1902, en el marco del XXVI Congreso de Juristas alemanes, celebrado en Berlín, queda abiertamente reconocido el derecho a la propia imagen como uno de los derechos inherentes a la personalidad. Por otro lado, hacia fines del siglo pasado en Estados Unidos se conocía el célebre artículo de Warren y Brandais "*The right of privacy"* de 1890, que se refiere al derecho a la imagen personal como la forma más simple del *right of privacy*, y cuyo antecedente más inmediato es la expresión acuñada por el juez Cooley en 1879 *the right to be let alone* (el derecho a ser dejado en paz). Estos autores plantean que si la *Common law* cada vez ampliaba más su protección a las personas y a sus bienes, dicha protección debía extenderse a los particulares en su vida privada y si se tenían en cuenta las nuevas circunstancias sociales, tecnología y desarrollo de la prensa, crecimiento del interés informativo, etc., sería conveniente considerar al *right of privacy* como reconocido por la cuarta enmienda de la Constitución Americana.[41]

Entre 1910 y 1948 se consolida la garantía con jurisprudencia que la interpreta desde el derecho a la privacidad.

> A partir de la Declaración Universal de los Derechos del Hombre —1948— (art. 12) se protege especialmente la vida privada y la honra, transmitiendo a las cartas constitucionales del mundo el derecho consagrado.

Vuelve a sostener Basterra que:

> en nuestra Ley Fundamental no hay artículo que se refiera al derecho a la imagen propia, o al propio perfil, pero está implícito a través de las normas supranacionales que quedaron incorporadas a nuestra Constitución después de la reforma de 1994, en el art. 75 inciso 22. Por su parte el art. 43 establece la garantía de *habeas data* como el acceso a los datos, y la finalidad que se dará a los mismos y la posibilidad según los casos de rectificación, supresión, confidencialidad y actualización de los mismos. Nada dice en relación a los derechos protegidos en doctrina, varios autores consideran entre los derechos tutelados por esta garantía, el derecho a la propia imagen.[42]

En cada etapa se observa el paso de la defensa patrimonial de lo que es intrínsecamente propio (el producto del intelecto) al campo de lo espiritual (la tranquilidad de conciencia) y terrenal (vivir una vida propia sin interferencias). Por ello está bien que la imagen se considere como un derecho de la personalidad, o como una barrera

---

[41] BASTERRA, Marcela I., *Habeas data: derechos tutelados,* Doctrina Judicial, 1993-3, pp. 77 y ss.

[42] BASTERRA, ob. cit., p. 78.

que evita perturbar la dignidad humana. Ello es consecuencia de la evolución legislativa, pero también lo es, de la propia estima que el hombre reconoce sobre su persona.

Dice Puig Brutau que:

> si se considera el derecho de la personalidad como una institución puesta al servicio de la persona para hacer valer su dignidad como tal, no cabe duda que la dignidad moral es un bien que merece ser protegido; por consiguiente, toda persona tiene derecho a recibir de los demás un trato acorde con la dignidad que el ordenamiento jurídico reconoce a todo sujeto de derecho, y en ese sentido cabe hablar de honor como una manifestación del derecho de la personalidad, que repercute además en la consideración que la propia persona tenga de sí misma.[43]

320.4. Ahora bien, la imagen en sí misma puede transmitirse en dos formas: a través de la reproducción por cualquier medio de una figura propia, que sería un supuesto objetivo, inmediatamente reconocible. O bien, como creencia que los demás tienen sobre nuestra persona a partir de la imagen pública que expresamos, caso éste que resulta esencialmente subjetivo.

Por ello, mientras es posible actuar prontamente para la defensa de la imagen cuando esta se afecta en la publicación de fotografías o retratos producidos sin autorización del titular; resulta más difícil encontrar la vía de respuesta a las agresiones contra la reputación cuando ella no alcanza para lesionar el honor de la persona. Adviértase que en éste, el comportamiento atacado es aquél que pretende afectar la consideración social del individuo.

En uno y otro caso, el *habeas data* no parece ser la herramienta más precisa, salvo claro está, que el camino aplicado para inferir el agravio sea un dato transmitido desde un archivo o base registral.

> Así pues —dice Herrán Ortiz— el derecho a la propia imagen debe identificarse con los derechos de libertad, de manera que al individuo le es garantizado el derecho a decidir libremente respecto a su imagen, adoptando en su caso las medidas que procedan para impedir la divulgación de imágenes o retratos de la persona, aunque la misma no dañe su honor, ni interfiera en su derecho a la intimidad. Claro que no se requiere la intención dañosa o injuriosa para que la libertad del sujeto, en cuanto a su imagen, se considere vulnerada, y constituye una realidad irrefutable que el simple hecho de divulgar, exhibir o publicar la imagen de la persona puede y debe ser cuestión que quede al exclusivo arbitrio de cada individuo.[44]

320.5. La especialidad del proceso constitucional evita confundir el derecho a la propia imagen con el derecho a la intimidad o el derecho al honor, aunque no es necesario establecer una diferencia manifiesta entre ellos, pues en definitiva el derecho personalísimo que se tiene apunta a proteger la identidad personal mediante

---

[43] PUIG BRUTAU, José, *Fundamentos de derecho civil*, Tomo I, Bosch, Barcelona, 1979, p. 46.

[44] HERRÁN ORTIZ, ob. cit., p. 177.

el *habeas data*; mientras que el honor y la intimidad se tutela con herramientas específicas sustantivas (civiles y penales).

De todos modos, al proteger a la persona de las invasiones ilegítimas (sea por reproducción gráfica o difusión escrita) contra esa parte de la vida que quiere mantener fuera del alcance de otros, evidentemente también se defiende la privacidad o el derecho a tener una vida privada.

321. La fama o reputación

321.1. La intimidad se podría representar, en forma figurada, cual si fuera una espiral cuyo núcleo contiene la más sagrada de las reservas que la persona quiere mantener. Aparece así una suerte de anillos donde el más expuesto hacia el exterior es el que los demás observan y conocen, y que puede asentar en la esfera de la fama o reputación.

> De manera similar, la doctrina alemana intenta profundizar el contenido de la intimidad distinguiendo en él tres esferas. Constituirían a modo de círculos concéntricos, representativos de una triple graduación de la vida privada, desde el más permisivo al más restringido. Novoa las explica diciendo que la más amplia, o *esfera privada*, comprende todos aquellos comportamientos, noticias y expresiones que el sujeto desea que no lleguen al conocimiento público. Se incluye aquí la imagen física de la persona y su comportamiento, aun fuera del domicilio, que no debe ser conocidos sino por quienes se encuentran en contacto con él. Le sigue la denominada *esfera confidencial*, que abarca lo que el sujeto participa a otra persona de confianza; de esta esfera quedan excluidos, aparte del público en general, aquellas personas que operan en la vida privada y familiar. Aquí se incluyen correspondencia, memorias, etc. Finalmente, como círculo concéntrico de menor radio, aparece la *esfera del secreto*, que corresponde a las noticias y hechos que por su carácter extremadamente reservado han de quedar inaccesibles a todos los demás.

321.2. En España, la originaria ley de Tratamiento de Datos (derogada a fines del año 1999), identifica la defensa de la fama cuando ella supone reputación profesional. En la exposición de motivos se lee: "[…] "el conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor".

Esta inclusión en el terreno que el honor abona nos llevaría a interrogar si los actos lesivos dirigidos contra la fama pueden ser resueltos por las acciones que sirven a la defensa de la honorabilidad, o en su caso, si la herramienta precisa es el *habeas data*.

Las posibilidades se alternan entre la visión patrimonialista que privilegia la atención sobre el daño provocado y, en consecuencia, la reparación a través de una indemnización por el perjuicio sufrido; o bien, la tutela del honor, ya sea en su aspecto interno afirmado en la autoestima, o en su faz externa integrado por el reconocimiento que los demás hacen de nuestra dignidad.

321.3. El Tribunal Constitucional español ha terminado por incluir la fama o prestigio profesional dentro del concepto constitucional de honor en sentido trascen-

dente, que no es otro que la opinión que la gente pueda tener de cómo trabaja cada cual y que respeto merece por ello.

No existen dudas respecto al derecho a la necesidad de protección jurídica que tienen ambas cuestiones, el punto a esclarecer es si el derecho se apoya en un derecho fundamental, o en su caso, en una solución material sostenida en la reparación de los perjuicios sufridos.

Cada profesión tiene códigos deontológicos que previenen las actitudes deshonrosas de los hombres que en el sector se desempeñan. Quienes no responden a esas normas de conducta moral o ética profesional, son sancionados. Una regla no escrita supone que a mayor responsabilidad, mayores son los deberes de conducta, y en consecuencia, más graves debieran ser las sanciones.

321.4. Ahora bien, afinando el concepto se advierte que cada vez más nos alejamos de la tutela prometida desde el *habeas data*, en cuyo caso, esta vía solamente sería útil cuando en un archivo o registro se encuentren datos que descalifiquen o menosprecien la calidad del profesional.

Sin embargo, también en este punto hay que tener cuidado, pues los datos sobre una persona pueden capturar opiniones que otros tienen de ella a través de las publicaciones que constituyen críticas u observaciones que definen la expresión del arte, oficio o profesión que tiene.

Bien apunta Cifuentes que:

> es necesario buscar un punto de equilibrio entre la libre crítica y la ofensa de la persona. Esto será, por fatalidad, cuando alguien se siente ofendido en su condición profesional, desempeño de su especialidad o creación literaria, científica, artística, cultural y pública supeditado a la decisión judicial. El magistrado, según las circunstancias, pruebas y elementos objetivos y subjetivos del caso, deberá graduar la fuerza del cuestionamiento, de la ironía acusadora, del juicio desfavorable y sus comentarios y manifestaciones, a fin de establecer si se ha sobrepasado el mero disentimiento, para desmerecer la persona con aguda saña o en aspectos privados y propios de la honorabilidad profesional.[45]

321.5. El acto de archivar, conservar y difundir datos que puedan lesionar la honorabilidad de una persona, o al menos, su reputación personal o profesional, se distingue de las vías positivas de defensa que el derecho tiene, pues el buen nombre vituperado solamente tiene indemnización económica, haciendo cierta la expresión que sostiene que, una vez que el dato se ha hecho público es inútil cualquier corrección, y lo único que queda, es la reparación patrimonial de un daño que, moralmente, no tiene sosiego.

Por ello, el *habeas data* puede actuar preventivamente para evitar la difusión de comentarios hirientes o mal intencionados que persigan agredir el respeto personal o la fama profesional que se tenga. Es evidente que, aun sin ley expresa o disposición constitucional que lo autorice, no se puede privar a la ley de su auténtica interpreta-

---

[45] CIFUENTES, ob. cit., p. 88.

ción axiológica, al ocuparse de la persona y sus datos personales como aspectos inherentes a su intimidad.

> Con el fin de apoyar este argumento, deberíamos considerar varios aspectos, algunos de los cuales son ampliamente aceptados, tales como la Directiva Europea relativa a la protección de datos y libre circulación de los mismos. De hecho, varios de los artículos de la Directiva se refieren explícitamente a la naturaleza pública de ciertos datos a la hora de concluir que los datos personales que se han hecho públicos no se pueden proteger de la misma manera que los datos personales. Al menos tres de estas disposiciones deberían examinarse con más profundidad, como son los artículos 8.2; 18.3 y 26.1.
>
> El artículo 8.2 de la Directiva relativo a las categorías especiales de datos (convicciones políticas, filosóficas o religiosas, datos personales que revelen el origen racial o étnico o la moral de cada persona) señala explícitamente que no se podrían tratar a menos que el interesado haya dado su consentimiento explícito.
>
> El artículo 18.3, exige que cualquier recopilación de datos debe ser anunciada a la autoridad encargada de la supervisión de los mismos. Este artículo presenta una exención para esta exigencia a las "recopilaciones destinadas a facilitar información al público y a la consulta abierta por parte del público".
>
> Para concluir, el artículo 26.1 admite una excepción a la exigencia de un nivel adecuado de protección para los datos objeto de comunicación transfronteriza, a saber: si los datos transferidos a un Estado que no proporciona dicho nivel de protección tienen su origen en "registros que están a disposición del público"

321.6. Desde otro punto de vista, también se puede enfocar el derecho que el individuo tiene para no descubrir facetas de su personalidad que le provocan deshonra o, al menos, son indecorosas para su imagen.

Surge así una suerte de relación confusa entre el engaño y la intimidad, una conducta que se puede ocultar y mantener al margen del conocimiento de otro porqué, de otro modo, caería el prestigio adquirido.

Sostiene Catalán González que:

> la relación entre engaño e intimidad es diacrónica: allí donde se dé un área de conducta que hoy tengo derecho a mantener al margen de la inspección de los otros, desde la correspondencia privada a la cuenta bancaria, desde el número de teléfono particular al seudónimo del concurso literario, desde el diario íntimo al secreto informático, allí se dio antes motivo para el engaño y el secreto. La intimidad así entendida, y con ella el engaño que la antecede, sólo podrían aprehenderse desde una perspectiva genética, atendiendo al precario equilibrio de fuerzas entre aquello que el grupo sabe del individuo y aquello que el individuo está dispuesto a reconocer ante el grupo; también, trasladando el ángulo de inspección, como un pacto entre ambas instancias donde cada una sacrifica algo para recibir algo a cambio, y, por último, como el reconocimiento simultáneo de que alguien no puede renunciar a ciertas actividades que le acarrearían consecuencias desagradables de ser conocidas.[46]

---

[46] CATALÁN GONZÁLEZ, Miguel, "Descrédito, intimidad y encubrimiento", en *Sobre la intimidad*, Fundación Universitaria San Pablo C.E.U., Valencia, 1996, p. 34.

321.7. Las inclinaciones sexuales, por ejemplo, son datos sensibles que tienen prohibida su difusión. Este sería un derecho al secreto que el *habeas data* puede amparar; en cambio, divulgar que la fama de un autor literario se debe a que contrata servicios de otros para sus ediciones, es un hecho inconveniente para esa notoriedad alcanzada; aquí, la revelación de los servicios prestados afectaría el crédito logrado, aun cuando lo fuese mediando un intelecto que no le es propio y se vale de esa ocultación. Aunque parezca incómodo decirlo, el hecho no es delictual (si bien pueda ser cuasidelictual), y recobra aquella máxima que ponía en práctica "Anibal" en su lucha contra los romanos: "Se debe luchar con la astucia cuando no se puede ser igual con las armas".

En términos similares se plantean otras diferencias sensibles que inciden en la reputación como "estigmas o descréditos", aunque de hecho no lo sean, y el individuo desea conservar en su más sagrada reserva; por ejemplo: los atributos físicos diferentes (*v. gr.:* enfermedades crónicas como la diabetes); las capacidades diferenciadas (*v. gr.:* sordera, tartamudez, etc.); las costumbres sociales o sexuales; el comportamiento doméstico, etc. En cada caso, existe una relación entre el encubrimiento y la intimidad.

321.8. La revelación se produce cuando la confidencia se hace pública; ese acto, además, agrede la fama o reputación.

> Las figuras de la "discreción" y la "ocultación éticamente justificada" del individuo ante el tanteo para saber más que ejercen los extraños o simples conocidos, son figuras morales que se remontan a fechas muy anteriores a la moderna eclosión de los valores de la vida íntima. Se pueden hallar en los textos de las grandes religiones y en los escritos morales de la antigüedad grecorromana. Nada tiene de extraña —agrega Catalán González— esta inveterada apreciación que constituye el bastidor invariable sobre el que se teje, como dijimos, el cambio social de valores; puesto que las relaciones sociales se asientan en el conocimiento que tengamos del otro, y ese conocimiento ha de ser mayor conforme aumente la mutua relación. El límite de los tanteos realizados para saber más de él, sin que ese tanteo pueda considerarse "indiscreto", no puede establecerse de una vez y para siempre, sino que varía conforme lo hacen las condiciones sociales.[47]

En el fondo, la intimidad mejor protegida es la que oculta la información agraviante, a pesar de confrontar con ello la simulación del "yo" y el disimulo de lo inconveniente a la imagen.

> Por mucho que pueda repugnarnos a primera vista —afirma Catalán González— la aspiración al secreto bancario y al derecho del aspirante a un empleo a no revelar al empleador su "biografía moral" sufren de la misma dualidad pragmática: por un lado, aceptan la importancia del descrédito sociogénico; por otro, hacen uso de la capacidad reconocida de reserva para encubrir características de su comportamiento que saben desacreditables.[48]

---

[47] González Catalán, ob. cit., p. 35.

[48] Catalán González, ob. cit., p. 36.

322. El derecho a la reserva y confidencialidad

322.1. Es común afirmar que la reserva y confidencialidad pertenecen y corresponden con los objetivos del derecho a la intimidad.

También se afirma que, entre los tipos de *habeas data*, aparece el *reservador* (que sólo puede transmitirse a quien se encuentra legalmente autorizado y en las circunstancias en que corresponde), el cual involucra la confidencialidad del dato (supuesto de datos sensibles que se excluyen en todo tipo de información).

Sin embargo, es preciso afinar los conceptos, porqué el punto de partida no es la intimidad en sí misma, sino otro u otros derechos, que por ahora dejamos planteados sin definirlos.

322.2. Un dato es una fuente de información. No se obtiene sino a través de la pesquisa o de la revelación que haga la persona. Cuando es ésta quien lo da a conocer, pone en exposición un pensamiento, una característica de su personalidad, un gusto, una idea, o cualquier manifestación que hace a su identidad. En ese momento el dato deja de pertenecerle porqué lo ha transferido a otros. Esta actitud puede representar una confidencia y la obligación del otro es conservar el secreto revelado como un derecho que aquél tiene a la reserva.

Se observa así, como la intimidad, atraviesa por el secreto absoluto (porque sólo el individuo sabe del dato que transfiere), para llegar al secreto compartido donde se puede hablar, con mayor precisión, del ámbito de la reserva y confidencialidad.

> En definitiva —afirma Herrán Ortiz— si íntimo es lo que cada persona se reserva para sí y a los demás no es lícito invadir, confidencial es aquello que se revela a alguien con la intención o ánimo de que no sea revelado a los demás sin el consentimiento del interesado. De igual manera, no puede desconocerse que si bien en un primer acercamiento al derecho a la intimidad éste se puede relacionar estrechamente con el "secreto", debe admitirse que la intimidad no implica exclusivamente la ausencia de información sobre la vida de la persona; representa, por el contrario, una necesidad de "vida interior", o relación intra-personal, de reflexión de los propios sentimientos y pensamientos.[49]

322.3. Cuando la información es producto de la investigación practicada sobre alguien, y éstas conciernen a la vida y personalidad, se puede presumir que esa búsqueda tiene alguna finalidad, más allá de la simple recopilación y almacenamiento. El individuo tiene desde el *habeas data* la posibilidad de saber el objetivo del archivo y solicitar la confidencialidad como un medio de autopreservar su derecho a la intimidad.

Por ello, la intimidad no es tanto una cuestión de ocultamiento o secreto, que corresponda a terceros en atención a las circunstancias que justificaron su revelación, sino de libertad del individuo, de posibilitar la plena disponibilidad sobre su vida y relaciones personales.

---

[49] HERRÁN ORTIZ, ob. cit., p. 179.

Por su parte la confidencia se resguarda en la confianza depositada en otro, quien se vale de su propia conducta para mantener el ocultamiento, y también, porque no, de cierto grado de complicidad con el dato revelado; el secreto pertenece a la intimidad, como la máxima expresión de la vida interior que no se transfiere. A su turno, la información pesquisada no pertenece al secreto (porque éste no se consigue sin la voluntad del individuo) sino a la intimidad, y el deber de quien obtiene datos que son expresiones de ese derecho, es conservar la confidencialidad como una obligación derivada.

> Por todo ello —concluye Herrán Ortiz— el deber de secreto constituye una de las manifestaciones del derecho a la intimidad, pero no se confunde con él. En ocasiones, el deber de ocultar se limitará a bienes de la personalidad, a la esfera interior de la persona, pero la más de las veces lo que se debe reservar del conocimiento ajeno serán informaciones no íntimas; sin embargo, también estas informaciones constituyen el deber de secreto. Así lo íntimo es lo más personal siendo, por tanto, todo lo íntimo secreto y reservado. Representa, por otro lado, una evidencia que cada persona puede develar, por decisión propia, parte de su intimidad a los demás, naciendo entonces un deber secreto en aquél a quien se ha confiado la intimidad. Por ello, determinados autores han querido ver en el derecho al secreto una especie del derecho a la intimidad.[50]

322.4. La interesante diferencia entre secreto y confidencialidad, desde esta perspectiva, sirve para tomar distancias respecto de la protección penal que, por lo general, se establece para la incolumidad de la correspondencia particular, que responde a un tiempo distinto.

Actualmente, cabe pensar que así como la justicia remoza los alcances de las normas penales, también la legislación ha evolucionado permitiendo extender la protección a los registros privados contenidos en computadoras o cualquier otro soporte, pues siempre existe en ellos un ámbito propio de la reserva de las personas.

323. El derecho al secreto

323.1. Esta es una de las cuestiones más difíciles de establecer en el alcance del *habeas data*. Se parece a la reserva personal sobre hechos y pasiones que la persona conserva para sí, pero excede la privacidad determinada por uno al ser un aspecto que, pudiendo ser conocido por otros, no se quiere transferir el dato, el pensamiento o la característica, o la cuestión que fuera motivo de expreso ocultamiento.

Para Santos Cifuentes:

> por secreto debe entenderse no lo reservado, la vida interior o en soledad, sino aquellas situaciones, pensamientos y datos en general que pertenecen a la persona y que, por su índole o porque así lo quiere aquélla, están destinados a no expandirse ni ser conocido por terceros. Es lo que se mantiene oculto, y si bien muchas veces el ocultamiento es diverso de lo puramente personal, no cabe duda que se refiere a un aspecto del derecho a la intimidad.[51]

---

[50] HERRÁN ORTIZ, ob. cit., p. 188.

[51] CIFUENTES, ob. cit., p. 143.

El secreto es un misterio individual; es algo que cuidadosamente se mantiene alejado de los demás. La similitud con el estudiado derecho a la reserva y confidencialidad es manifiesta, pero tiene algo más.

En primer lugar la relación entre intimidad y secreto no es permanente, aun cuando sea cierto que el fundamento de lo que se quiere preservar reposa, en última instancia, en una decisión individual que afinca en la parte más íntima de una persona.

No todo lo secreto será íntimo; aquello que es revelado en determinadas circunstancias o a determinadas personas aunque no se identifique con la interioridad del individuo, con su esencia personal, deberá ser ocultado por aquellos a quienes se comunicó, es decir, tienen el deber jurídico, además de moral, de no compartir la información recibida con terceros extraños.

323.2. Si la explicación la abordamos desde la protección a la correspondencia y papeles privados, la cuestión puede ser más clara.

En efecto, el artículo 18 de la Constitución argentina y distintas normas de los códigos civil y penal, garantizan la inviolabilidad de las cartas y otros papeles privados que contengan la expresión de un pensamiento aunque no esté destinada a ser comunicada a otro, siempre que estén dentro de la esfera de custodia de la persona.

Es decir, la garantía está en el secreto de lo que se dice o escribe, sin importar si las expresiones constituyen revelaciones de intimidades o son hechos intrascendentes. La idea es que la persona tenga libertad para expresar aquello que a otros comunica sin que nadie pueda interferir en forma directa o solapada. Por eso las intercepciones telefónicas son ilegítimas, como lo es también la apertura indebida de una carta, un pliego cerrado o un despacho telegráfico o de cualquier naturaleza.

323.3. La correspondencia particular y los papeles privados deben interpretarse con sentido amplio que admita el desarrollo tecnológico y evite la zona de grises que se encuentra aun sin definir.

En efecto, el caso de las cartas misivas debe capturar en su alcance los mensajes del correo electrónico, los informes del "pager" o "beeper" (pese a la intervención de un tercero que mediatiza el mensaje pero que participa de la confidencialidad), y todo tipo de mensajero que aplica esa función de correspondencia a particulares.

Lo mismo puede ser dicho respecto a los papeles privados, los cuales conservan el derecho al secreto y a su invulnerabilidad (por ejemplo: legajos personales, fichas de trabajo, historias clínicas, etc.). La extensión mentada se aplica a todo tipo de comunicaciones interpersonales, de forma tal que el medio utilizado no es trascendente como sí lo es la garantía que preserva la libertad de intimidad.

> Con la técnica moderna —agrega Bidart Campos— consideramos que la libertad de intimidad se extiende a otros ámbitos: comunicaciones que por cualquier medio no están destinadas a terceros, sea por teléfono, por radiotelegrafía, etc. Este último aspecto atañe simultáneamente a la libertad de expresión: la expresión que se transmite en uso de la libertad de intimidad no puede ser interferida o capturada arbitrariamente. La captación indebida tampoco puede, por ende, servir de medio probatorio. Sería extenso enumerar otros contenidos que quedan amparados en la intimidad, y sobre los cuales sólo puede

> avanzar una ley suficientemente razonable con un fin concreto de verdadero interés. Así, el secreto financiero y bancario, el retrato o la imagen, etc.[52]

323.4. La dimensión de los derechos tiene presente, en definitiva, la seguridad individual y no es otro el sentido que orientan las normas del Código Civil y en cuanto corresponde al Código Penal.

Apunta Oteiza siguiendo el criterio que se expone,

> que continúan en esta línea la ley 23.798 que se ocupa de distintos aspectos vinculados con el síndrome de inmunodeficiencia adquirida cuando impone la codificación de las fichas y los registros y la obligación de guardar reserva absoluta de los profesionales que intervengan en el tratamiento. La ley 11.723 que requiere el consentimiento de la persona fotografiada y que su difusión se vincule con fines científicos, didácticos o culturales. Las citadas disposiciones reciben en forma atenuada el derecho de evitar las invasiones sobre aquellos aspectos de la vida personal que no existe mérito para revelar, o que conocidos no deben ser dominados o empleados por terceros.[53]

323.5. Con mayor preocupación el Pacto de San José de Costa Rica (art. 11), y otros tratados y convenciones (*v. gr.:* art. 12 de la Declaración Universal de Derechos Humanos; art. 17 del Pacto Internacional de derechos civiles y políticos) prefieren evitar toda intromisión arbitraria en la vida privada, domicilio, vida familiar y correspondencia privada, que son los numerales que acepta el derecho a la intimidad en sentido lato.

Ahora bien, ¿cómo trabaja el *habeas data* en este campo de la correspondencia epistolar? En primer lugar debemos partir de la base de sostener que el concepto no está limitado a las cartas misivas, sino a todo tipo de comunicaciones que emitan información privada y que no importa que en el intercambio participen terceras personas. Esta actuación necesaria o contratada de otro individuo o de un medio técnico controlado por otro, no significa publicitar o dar sentido público al envío.

En segundo término, hay que resguardar y asegurar el derecho a mantener secreta cierta información que le concierne, de modo tal que no esté al alcance de persona alguna, a excepción de autorizaciones judiciales expresamente indicadas.

323.6. Un aspecto más se vincula con las nuevas modalidades de información que una persona investiga y que, sin saberlo ni quererlo, tiene "buscadores" que siguen sus preferencias para utilizar ese dato obtenido.

Existen cuatro acciones calificadas como muy graves en la utilización de la red Internet:

a) Seguimientos de qué sitios en la red visita cada persona y utilización indebida de esa información;

---

[52] BIDART CAMPOS, Germán J., *Tratado elemental de derecho constitucional argentino,* Tomo 1: *El derecho constitucional de la libertad*, Ediar, Buenos Aires, 1986, pp. 45 y ss.

[53] OTEIZA, Eduardo D., *Información privada y habeas data,* en *Estudios de Derecho Procesal en homenaje a Adolfo Gelsi Bidart,* Fundación de Cultura Universitaria, Montevideo, 1999.

b) introducción en Internet de información sobre personas presente en registros públicos que permite la identificación de las mismas;

c) lectura de mensajes de correo electrónico por personas a las que no van dirigidos;

d) sitios de la red que recopilan direcciones de correo electrónico de sus visitantes para obtener listas de comercialización sin consentimiento ni autorización alguna.

La suma de cuestiones previas abre esperanzas para que con el *habeas data* se pueda saber qué registros se tienen de alguien que comercializa vía Internet y qué otro destino puede tener ese archivo; qué sentido tiene la persecución completa de datos para registrarse en un hotel; impedir la agresiva venta telefónica que invade permanentemente la línea celular, satelital u ordinaria que se ha contratado, en fin, toda inmiscusión en la zona de reserva y confidencialidad propia de los papeles privados, constituye un campo propicio de ocupación por el proceso constitucional.

323.7. Sin embargo, la cuestión no podrá seguramente tener solución ni por la ley ni a través de su garantía. La novedosa injerencia y penetración en lo que es propio obligará a complementar las leyes con acciones precisas destinadas a la protección efectiva, antes que la invasión se produzca. De otro modo, cualquier proceso será meramente resarcitorio porqué el daño se habrá producido.

> La normativa, por sí misma, no será suficiente para proteger el derecho a la intimidad en el próximo siglo —asegura Ann Cavoukian—; será necesario emplear diversos instrumentos como complemento a la legislación y, en particular, herramientas de carácter tecnológico (herramientas de protección de la intimidad)…Puede adoptarse la legislación más estricta, como es el caso en la Unión Europea, pero si existe la posibilidad de eludirla mediante la aplicación de las diversas tecnologías, su valor disminuirá en gran medida. Además, en el mundo de Internet, en el que no se conocen fronteras políticas ni se observan leyes aplicables, no queda otra opción que recurrir a la tecnología… Quizás, las plataformas para las preferencias de intimidad (P3P) apoyen esta tecnología y pueden considerarse un paso adelante hacia la mejora en la protección de la intimidad.[54]

En relación con ello la Convención Europea para la protección de los derechos humanos resguarda la capacidad legal de mantener cierta información secreta o fuera del alcance de la autoridad estatal y de otras personas. El artículo 8º se preocupa e insiste sobre la inviolabilidad de la correspondencia, el domicilio y la vida privada y familiar, a excepción que una ley lo autorice expresamente y constituya una medida resuelta dentro de una sociedad democrática. Además, debe revestir el carácter de "necesaria" para sostener la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de las libertades y derechos de los demás.

---

[54] CAVOUKIAN, Ann, *Comercio electrónico: las personas necesitan protección, no perfección,* en XX Conferencia Internacional de autoridades de protección de datos (1998), Agencia de Protección de Datos, Madrid, 1999, p. 199.

> Informa Oteiza que la Corte de Estrasburgo interpreta con amplitud el texto de la Convención. En el caso Klass (sentencia del 6/9/78) se analizaba la legislación de la por entonces Alemania Federal que permitía un control genérico sobre la correspondencia, los envíos postales y las telecomunicaciones. Con respecto a las conversaciones telefónicas no mencionadas expresamente en el art. 8º el Tribunal estimó que ellas se encuentran comprendidas en las nociones de "vida privada" y de "correspondencia", agregando que el sistema de vigilancia previsto contiene diversas cláusulas destinadas a evitar a un mínimo indispensable el efecto de las medidas de control que limitan a la autoridad administrativa.[55]

323.8. Ahora bien, ¿cómo se elabora este principio aplicado al proceso constitucional de *habeas data*?

En primer lugar, dando por cierto que *secreto* es lo que cuidadosamente se tiene reservado y oculto, y por tanto que su alcance jurídico consiste en asumirlo como un hecho que se quiere mantener escondido por considerar que su conocimiento podría dañar a alguien. En ambos casos, el término dominante y coincidente es la ocultación.

En virtud de ello, el derecho a mantener oculto los datos obliga a pensar en un destinatario que está impedido de conocerlos, por eso, al *habeas data* no es posible estructurarlo como un derecho al secreto personal, es decir, con relación a uno mismo.

En segundo término, el derecho al secreto es una garantía para la confidencialidad de las comunicaciones de cualquier tipo, en cuyo caso, el *habeas data* queda fuera del mensaje, en razón de que si hubiera que reclamar por el incumplimiento o la violación del derecho, la vía judicial más idónea sería el amparo.

> Llegado a este punto habría que preguntarse con Velázquez Bautista, acerca de cuál es el contenido del derecho al secreto, y en particular, el "secreto de las comunicaciones". La idea sería que éste ampara tanto la "libertad de comunicación", como el mantenimiento en secreto de las mismas con independencia de cual es el contenido de los mensajes. Sin embargo, no se considerará violación de secreto cuando se autorice su intervención mediante mandato judicial o medie consentimiento.[56]

Por su parte, el artículo 8º de las Directivas de la Comunidad Europea sostienen:

> 1. El organismo de telecomunicaciones deberá garantizar una protección adecuada, utilizando las técnicas más avanzadas, de los datos personales contra posibles accesos y usos no autorizados; 2. En caso de que exista un riesgo especial de violación del sistema de seguridad de la red, como por ejemplo, en el ámbito de la radiotelefonía móvil, el organismo de telecomunicaciones deberá informar a los abonados de dicho riesgo y ofrecerles un servicio de cifrado de extremo a extremo.

---

[55] OTEIZA, Eduardo D., *Información privada y habeas data*, comunicación presentada en el XX Congreso Nacional de Derecho Procesal, San Martín de los Andes (Argentina), 1999.

[56] VELÁZQUEZ BAUTISTA, Rafael, *Protección jurídica de datos personales automatizados,* Colex, Madrid, 1993, p. 92.

324. El derecho a la información

324.1. El derecho a la información es producto de una sociedad democrática que reclama saber y conocer el complejo mundo que habita y las vicisitudes donde esta inserto.

Sostiene el Tribunal Constitucional español que:

> la libertad de información juega un papel esencial como garantía institucional del papel democrático que inspira nuestra Constitución, el cual presupone, el derecho de los ciudadanos a contar con una amplia y adecuada información respecto a los hechos que les permita formar sus convicciones y a participar en la discusión relativa a los asuntos públicos. Es este aspecto el que puede explicar que este tipo de comunicados haya aparecido en otros periódicos sin que ello haya motivado la intervención de la justicia penal, como se desprende de la documentación acompañada en autos.

El derecho a estar informado tiene una doble e interesantes facetas. Mientras por un lado privilegia el derecho de los medios de comunicación a publicar y difundir sin restricciones ni límites a la libertad de prensa (inclusive en el artículo 43 de la Constitución argentina se lee la previsión para que el *habeas data* no afecte las "*fuentes de información periodística*"); por otro se defiende el derecho individual de las personas para estar informado sobre datos que le conciernan y estén archivados o registrados en una base específica.

324.2. Además, puede ocurrir que una publicación ofenda o de una versión equívoca de los hechos, en cuyo caso, obrarán los derechos repulsivos consecuentes como la querella penal o el derecho de rectificación o respuesta, pero éstos no son temas de esta obra.

> El contenido de un derecho de la información —dice Gutiérrez Castro— no se agota con el contenido de un derecho a la información, sino que, "la información" es hoy objeto de un tratamiento especial por los juristas y el derecho a ser informado por la prensa es sólo uno de sus aspectos, ya que tiene características propias y opera tanto como derecho individual, político y social, amén de su enorme interés como garantía institucional de la democracia. Así, junto al derecho a la información (libertad de prensa en toda su gama de aspectos y medios), aparecen otros derechos subjetivos que tienen como objeto directo "la información", tal es el caso, del derecho de acceso a documentos, registros, archivos y papeles del gobierno (transparencia de la administración).[57]

324.3. Sí interesa observar cómo el derecho a la información puede aplicarse en el *habeas data* como derecho a la verdad de saber si está en un banco de datos (derecho de acceso) y, en su caso, cuál es el destino que se quiere aplicar a ellos (con el fin de resolver su derecho a rectificar, actualizar, cancelar o solicitar la confidencialidad de ellos).

La Corte Suprema de Justicia de la Nación Argentina ha desarrollado esta idea, interpretando con amplitud el sesgado artículo 43, luego esclarecido y reglamentado

---

[57] GUTIÉRREZ CASTRO, ob. cit., p. 84.

por la ley 25.326. El juez Petracchi en la causa "Urteaga" sostuvo que "proteger el derecho a conocer todo lo relativo a la muerte de un familiar cercano —ocurrido en luctuosas circunstancias que vivió el país— significa reconocer el derecho a la identidad y a reconstruir la propia historia, los cuales se encuentran estrechamente ligados a la dignidad del hombre".

Ni más ni menos que saber lo que ocurrió: es un derecho a la información, y el *habeas data* el camino apropiado.

324.4. Es igual la inteligencia que acuerdan otras constituciones, como Brasil (art. 5.XXXIII) cuando dispone que todos tienen derecho a recibir de los órganos públicos informaciones de su interés particular, o de interés colectivo o general, que serán facilitados en el plazo señalado en la ley, bajo pena de responsabilidad, salvo aquellas cuyo secreto sea imprescindible para la seguridad de la sociedad y del Estado.

324.5. La causa "*Ganora*" fallada por el Tribunal Superior de Justicia de la Nación Argentina el 16 de setiembre de 1999, insiste y concluye que:

> la obtención de información sobre datos personales obrantes en los organismos y fuerzas de seguridad halla adecuación legal en la acción de *habeas data*; ello sin perjuicio de que el suministro de esa información pueda, eventualmente, afectar la seguridad, la defensa nacional, las relaciones exteriores o una investigación criminal, cuestión que en cada caso deberá ser invocada por el titular de la respectiva institución.

Vamos entonces por un buen camino, logrando encausar los bienes jurídicos que el *habeas data* respalda. El derecho a la información, sin lugar a dudas, es un fundamento esencial.

324.6. De allí que corresponda advertir cuáles son los espacios de cobertura que se tienen desde esta perspectiva, que le permite al individuo exigir al banco de datos la información que tenga sobre su persona.

Este es un aspecto, quizás el más importante; pero hay además, un conjunto de posibilidades que encuadran como la libertad de expresión, la libertad de prensa y de imprenta, la libertad de opinión y otras que, confrontadas con las potencialidades que ofrece el *habeas data*, pueden ocasionar algunas reservas. Quizás, pensando en ellas, en muchas legislaciones se deja asentado que el *habeas data* no puede afectar el secreto de las fuentes periodísticas.

324.7. Ahora bien, como el derecho a la información resume en los hechos tres actividades: *a)* la libertad de investigar; *b)* la libertad de difundir y *c)* la libertad de recibir información y opiniones; cada una de ellas tiene el correlato de la responsabilidad, razón por la cual existe otro derecho personal a no recibir información distorsionada, y su reflejo en el derecho a no ser objeto de una información falsa o abusiva.

> El tema lo explica acertadamente Uicich al agregar que por libertad de investigar se entiende la posibilidad irrestricta de utilizar toda la información obtenida legalmente y todos los medios existentes en procura de información. La libertad de difundir es la consecuen-

> cia de la facultad de investigar. Toda esa información obtenida, en la medida que no perjudique el legítimo interés de los terceros, goza de la facultad de ser difundida por cualquiera de los medios de comunicación. La libertad de recibir información es la faceta pasiva de la ecuación. Así como el ser humano, por ser tal, goza de la libertad de investigar y de difundir, él mismo es titular del derecho a ser informado, a exigir que la información le sea brindada…El derecho a la información comprende pues la faceta de quien tiene la facultad de acceder a la información cuanto la del sujeto pasivo de esa información de que no sea distorsionada o no sea revelada en tanto afecte su intimidad y no exista cuestión de orden público o de seguridad del Estado que lo justifique.[58]

De esta manera el derecho afianza la potestad de control sobre el derecho a la verdad, tanto para el sujeto activo que está en el archivo o registro, como para quien recibe la información.

> El problema, a juicio de Gutierrez Castro, se plantea en un conflicto de intereses, es decir, no sólo de legalidad, sino que sobre todo de legitimidad, vale decir de justicia y racionalidad en el ejercicio de un derecho. Por decirlo de otro modo, ambos derechos valen, el de quien informa y el de quien se informa. Pero valen dentro de límites razonables de modo que cuando se abusa del derecho de informar este se ejercita ilegítimamente; o sea, no es que un derecho se imponga a otro por su mayor peso, es que no puede coexistir dos conductas lícitas y legítimas contrapuestas, una debe ceder en el caso concreto ante otro y cuando se cede o es porque no se tenía derecho (legalidad) o porque se llegó a su límite razonable (legitimidad).[59]

324.8. La primera puesta en escena se obtiene con el derecho de información a los sujetos que están en el archivo. Éstos deben proporcionar siempre información a la persona concernida en ellas.

Los bancos de datos registran información muy diversa que, por lo general, no es de conocimiento público y, menos aun, de la persona que en él se encuentra.

El acopio y obtención de datos es bastante simple si se quiere. Todo depende de la finalidad que el registro persiga (por ejemplo, lograr información respecto a litigios que tenga una persona, causa y estado de cada expediente se puede conseguir hasta desde un ordenador con su módem respectivo) y del destino que piensa asignar a esa información compilada. Precisamente por esta presunta facilidad en la recopilación, algunas legislaciones establecen que no se puede evitar el carácter público del dato destinado a facilitar información general que, para ello, está abierta al público.

> El crear una base de datos —afirma Marcel Pinet— a partir de datos personales que sean públicos, aunque sea sólo por un instante, llevaría a la modificación de la naturaleza de la información. Un ejemplo sirve para ilustrar este punto de manera más que suficiente: en cualquier democracia, la vista de un procedimiento penal en la que se dicta sentencia es pública, pero en todas y cada una de nuestras democracias los antecedentes penales,

---

[58] UICICH, Rodolfo Daniel, *Los bancos de datos y el derecho a la intimidad,* Ad Hoc, Buenos Aires, 1999, p. 36.

[59] GUTIÉRREZ CASTRO, ob. cit., p. 155.

que son los archivos de las condenas que se dictaron de manera pública, son uno de los archivos más protegidos y menos accesibles. Esto es un ejemplo de como cuando se recopila información, ésta toma un valor informativo específico.[60]

324.9. Por ello, es más importante trazar el límite de divulgación que tiene el registro, antes que determinar cuando un dato se puede o no hacer público de acuerdo a la instancia individual. En este sentido, el derecho de acceso a los archivos es una garantía derivada del derecho a la información.

En el ámbito de las telecomunicaciones es bien conocido el ejemplo de los directorios inversos: se crean con los mismos datos que se utilizan para los directorios públicos de los abonados telefónicos, pero se invierte el criterio de búsqueda: en vez de utilizar un nombre y una dirección conocidos para encontrar un número de teléfono, se usa un número de teléfono para averiguar el nombre y la dirección del abonado. El criterio que se use para acceder a los datos puede cambiar radicalmente el uso que se vaya a darles. En ambos casos (directorios normales e inversos) la información es la misma y, a no ser que el interesado se haya opuesto de manera explícita, está al alcance del público en general. Sin embargo buscar el nombre y dirección de una persona si sólo tiene su número de teléfono supone buscar información que, tal vez, esa persona no pensaba dar; supone descubrir información suya sin su consentimiento y saber más de lo que esa persona quería revelar.

Y ese acceso está especialmente previsto como un mecanismo de vigilancia sobre el dato y la difusión que del mismo se pretenda realizar.

324.10. Otro aspecto del derecho a la información es que las bases de datos tengan actualizados los archivos, lo que suele llamarse como *derecho a la información veraz*.

Con la misma preocupación con que se agiliza la defensa de la persona registrada, se debe proteger al usuario de ese banco de datos (principio de exactitud).

Veracidad de la información supone mantener actualizado el archivo y conservar la información oportunamente tomada de acuerdo con las reales circunstancias en que sucedieron (situación real del afectado).

La transportación del informe por la vía que sea, exige responsabilidad en el llamado "tratamiento del dato".

324.11. Dado que el responsable de la veracidad del informe no es el acreedor, pues no tiene competencia para modificar o cancelar los datos inexactos que se encuentran en el archivo, aquella recae exclusivamente sobre la persona que comunicó el dato, a quien podría llamarse "responsable de la anotación" para distinguirlo del responsable de la base de datos que es el titular de la responsabilidad global.

La inclusión de los datos en un fichero ajeno, supone un tratamiento automatizado de estos. Por ello, no han existido dudas en la interpretación de la ley española

---

[60] PINET, Marcel, *Datos públicos o datos a los que puede acceder el público y protección de datos personales,* en XX Conferencia Internacional de autoridades de protección de datos (1998), Agencia de Protección de Datos, Madrid, 1999, pp. 23 y ss.

acerca de que cualquier incumplimiento respecto de la calidad de los datos incluidos en el fichero, salvo que fuera imputable a la exclusiva responsabilidad del titular del registro, deba ser imputado a la persona que introdujo los datos, al responsable de la anotación como se dijo, quien deberá garantizar la calidad de los datos.

324.12. También el *derecho al olvido* es una parte, un extracto del derecho a la información exacta. En la especie se trata de preservar la intimidad de la persona en sus actuales circunstancias, procurando que los datos compilados en su vida no lo conviertan en un reflejo de lo que fue antes de lo que es.

Existe otra vertiente que no escala en esta cuestión, y proviene del artículo 14.1 de la Convención Americana de Derechos Humanos que establece, con carácter vinculante, que "toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley".

La facultad de requerir la cancelación o la corrección de los datos inexactos, otorga el denominado *derecho al olvido*, esto es, el principio a tenor del cual ciertas informaciones (*v. gr.:* antecedentes penales prescriptos) deben ser eliminadas de los archivos transcurrido un determinado tiempo desde el momento en que acaeció el hecho a que se refieren para evitar que el individuo quede prisionero de su pasado.

La corrección de los archivos puede efectuarse por el mismo sistema que los contiene, sea ya por la aclaración que se peticione, o por la información corroborada por la base de datos.

> En el mecanismo articulado por el Consejo de Europa, el Convenio 81 previene un "mínimo necesario" de exactitud en los registros, comprendiendo como tales, la pertinencia, la corrección y la conservación actualizada de los archivos. Estos organismos de registración, públicos o privados, generalmente pueden oponerse a las rectificaciones cuando ellas se promueven por quienes no son directamente interesados, excepción hecha de las pretensiones sostenidas por personas que invoquen un legítimo interés y la mantención de los datos les provocare riesgos o daños inminentes.

324.13. Por tanto, la subsistencia de un dato caduco en un archivo, registro o base de datos es ilícito, toda vez que no media correspondencia con la actualidad requerida y, además, no media consentimiento del interesado ni existe un interés público prevalente.

Dato caduco es el que por efecto del transcurso del tiempo ha perdido virtualidad y ha devenido intrascendente a los efectos de cualquier efecto jurídico relativo a la ejecutabilidad. El Código Penal argentino, por ejemplo, al referirse a los datos de reincidencia, dispone que "el registro de las sentencias condenatorias caducará a todos sus efectos, después de transcurridos cinco (5) años desde su extinción para las condenas a pena de multa o inhabilitación. En todos los casos se deberá brindar la información cuando mediare expreso consentimiento del interesado…"

De este modo queda emplazado en esta suerte de "derecho al olvido" un fundamento más para localizar los contenidos tutelares del *habeas data*.

Según Palazzi:

> el tema es complejo, pues plantea la posibilidad de aceptar en el proceso constitucional otros motivos distintos a la falsedad o discriminación, lo que ratifica como posible. De otro modo, la difusión de datos pasados puede lesionar el derecho a la privacidad.[61]

325. El derecho a la identidad

325.1. La consideración de los derechos personalísimos donde la intimidad aflora como esencial y contundente, aparece el derecho a la identidad que supone el ser en sí mismo, la persona con sus propios caracteres y acciones, constituyendo la misma verdad de la persona que, por tanto, no puede en sí y por sí, ser destruida: porque la verdad, por ser la verdad, no puede ser eliminada.[62]

Según Cifuentes, intimidad e identidad difieren:

> La diferencia está en que la primera no tutela las reservas personales y familiares como un ámbito que tiene el sujeto para desarrollarse, sino la verdad de su perfil sociocultural. Y este perfil socio cultural puede estar en el exterior, no ser privado ni íntimo, sino por el contrario dado al público. Se ataca la intimidad mostrándose la verdad de lo que no se desea difundir. Se ataca la identidad desfigurando la personalidad del sujeto y mostrándola distinta de lo que es. Esta consiste en un conjunto de actividades públicas caracterizantes de dicha personalidad, que puede ser inexactamente deformada. En general, en la intimidad esa actividad pública no existe. Pero es claro que aprovechando lo recoleto del individuo, puede a la vez falsearse su perfil espiritual, con lo que podría verse producido un doble ataque de su persona: lo reservado y la identidad dentro de lo reservado.[63]

325.2. La identidad tiene aspectos que no suponen, en principio, problemas que deban resolverse en la vía del *habeas data*, tales como los derechos derivados del nombre o la propiedad intelectual. Aunque la ley argentina 18.248 (ley del nombre) admita acciones para reclamar, contestar, suprimir u oponerse a decisiones vinculadas con la identificación personal, ellas no afectan derechos de naturaleza constitucional en la medida que se tratan de atributos jurídicos de la persona que tienen un reglamento especial para su tratamiento y consideración.

Lo mismo puede aplicarse a los derechos emergentes de la creación artística o literaria, los cuales a pesar de poderse registrar y archivar en un sistema informatizado, cuando son violados o amenazados encuentran un mecanismo particular para su defensa.

325.3. La identidad fundamental, como derecho personalísimo y englobado dentro de los derechos humanos, pretende amparar el perfil que hace a una personalidad. Es parte del derecho a la imagen, pero al mismo tiempo, lo comprende.

---

[61] PALAZZI, Pablo, *El habeas data en la Constitución Nacional (La protección de la privacidad en la "era de la información")*, en Jurisprudencia Argentina del 20 de diciembre de 1995.

[62] DE CUPIS, Adriano, *I diritti della personalità,*editorial Giuffrè, Milan, 1982, p. 23.

[63] CIFUENTES, ob. cit., p. 87.

> La identidad del ser humano, en tanto éste constituye una unidad, presupone un complejo de elementos, una multiplicidad de aspectos esencialmente vinculados entre sí, de los cuales unos son de carácter predominantemente espiritual, psicológico o somático, mientras que otros son de diversas índole, ya sea cultural, religiosa, ideológica o política. Estos múltiples elementos son los que en conjunto, globalmente, caracterizan y perfilan el ser "uno mismo", el ser diferente a los otros, no obstante ser todos iguales en cuanto pertenecen a una misma especie, entendiéndose en definitiva "como identidad personal el conjunto de atributos y características que permiten individualizar a la persona en sociedad. Identidad personal es todo aquello que hace que cada cual sea "uno mismo" y "no otro". Este plexo de características de la personalidad de "cada cual" se proyecta hacia el mundo exterior, se fenomenaliza y permite a los demás conocer a la persona, a cierta persona, en su "mismidad", en lo que ella es en cuanto específico "ser humano", para utilizar la expresión de Fernández Sessarego.[64]

325.4. Cualquier información sobre este perfil puede ser motivo de la acción constitucional, por ejemplo, cuando se registra la pertenencia o afiliación política; o las cirugías practicadas en su cuerpo; o la filiación que le pertenece, etc.

Agrega Cifuentes que:

> es cierto que el sexo, la filiación y la edad registrables identifican. Es cierto que forman parte de la unidad-hombre y están en su proyección existencial desde el origen. También la formación genética forma parte de la combinación biológica, pero, sobre todas estas manifestaciones de la persona, domina, es primero y más visible, la conformación orgánica y los derechos respectivos. Creo que, ante todo, la ligadura de estos derechos se enraíza con las expresiones corporales del ser, y que desde el punto de vista de la caracterización diferenciadora, juegan allí un papel principal, siendo según ese orden la identidad cultural subordinada, secundaria. De todas maneras, cualquiera sea la ubicación del analista, la de la integridad orgánica o la de la identidad personal, son especies de derechos personalísimos que merecen tutela semejante. También la imagen debe distinguirse. No sólo por su condición ajena a la fuerza del movimiento cultural propia de la identidad, aunque pueda modificarse con la cirugía plástica o por accidentes, lo que no significa que sea una manifestación dinámica, sino también porque la violación es el aprovechamiento veraz, y, en la identidad, se trata de evitar la falsedad y mantener la verdad.[65]

325.5. Observado atentamente, el derecho a la identidad puede ser atacado también desde la ofensa al honor. De este modo, si alguien expusiera un agravio contra la honorabilidad que identifica a la persona, evidentemente y más allá de las pretensiones penales que pudieran caber, el registro de esa expresión puede evitarse desde el *habeas data*, sea a través de la supresión o la corrección por el dato exacto.

Y aún más lejos se puede llegar, por cuanto desde este derecho a la identidad se puede exigir el "derecho a la verdad", y perseguir la revelación de datos que permitan conocer el origen familiar, como una legítima manifestación del derecho humano a saber la verdad de su historia.

---

[64] FERNÁNDEZ SESSAREGO, Carlos, *Derecho a la identidad personal*, Astrea, Buenos Aires, 1992, pp. 66 y ss.

[65] CIFUENTES, ob. cit., p. 77.

La jurisprudencia acompaña esta proyección de acceder a los datos personales, entre los que se halla la ascendencia biológica que permite desentrañar la propia identidad del sujeto. Sin embargo, el *habeas data* debe ser el punto de inflexión que permita el equilibrio prudente, en virtud de que un banco genético violaría el derecho a la identidad del niño.

325.6. El derecho a la identidad es otro de los más preciados fundamentos para la protección de los datos personales.

En efecto, la identidad constituye una suerte de carta de presentación personal. Es la radiografía de la vida, y en buena medida, el atributo central de la personalidad.

Teniendo en cuenta que los bancos de datos registran información, ha de aceptarse que la veracidad del archivo pueda ser controlada por el propio interesado que se ha visto registrado; y aun frente a la posibilidad de incertidumbre acerca de la existencia del registro, es posible ingresar al mismo persiguiendo conocer la verdad compilada.

Por tanto, el derecho a la identidad supone además de la acción para reclamar información que le concierne, la proyección de requerir al banco de datos toda información que se conserve sobre alguien que pertenece al ámbito de intimidad de la persona, con lo que se advierte la extensión del derecho hacia una legitimación procesal más amplia que la tradicional.

> La protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las administraciones públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una administración pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el artículo 18 de la Constitución española, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos…Al desconocer estas facultades, y no responder a las peticiones deducidas, la administración del Estado hizo impracticable el ejercicio de su derecho a la intimidad, dificultando su protección más allá de lo razonable, y por ende vulneró el art. 18 de la Constitución (TC, 254/93, sentencia del 20 de julio de 1993).

325.7. De esta manera, se comprende que la identidad colectada no resulta un derecho privativo de cada individuo, porque admite la existencia de circunstancias que, sin encontrar una afectación directa, es susceptible de ser protegido por otros acudiendo al derecho a la intimidad que toda persona ostenta.

Afirma Herrán Ortiz que:

> la jurisprudencia ha acogido como característica del derecho a la intimidad su eficacia general, unida a ello, su categoría como derecho absoluto, donde la lesión no se da, ni surge acción para su protección, en tanto se cumple el deber privado de respeto. No hay acción allí donde falta el interés nacido de la agresión. Surge el derecho a la intimidad como derecho general, con capacidad para proteger a la persona frente a cualquier intro-

misión o ataque a su vida privada. Ahora bien, impera una consideración dogmática general o comprensión preinformática de la intimidad, que permite dudar y recelar de la posibilidad de fundamentar sobre el derecho a la intimidad la totalidad del sistema de protección de los datos personales, lo que llevaría a admitir la necesidad de reconocer la existencia de un nuevo derecho fundamental sobre el que asentar la protección de los datos de carácter personal.[66]

La necesidad de ampliar los objetivos de tutela de la libertad de intimidad se motiva en la propia conversión del derecho tradicional. No se trata aún de la defensa de la persona en sus aspectos más recónditos, sino de comprender que existe un derecho al desarrollo de la personalidad y de todas las vicisitudes que ella abarca, donde anida, entre otros, el derecho a la verdad. Verdad a que se sepa quién es uno; verdad a saber nuestros orígenes y la de quienes nos rodean; verdades que se quieren ocultar a otros.

El caso Garkin resuelto por el Tribunal Europeo de Derechos Humanos versa sobre el principio de acceso individual a documentos e información sobre la infancia de un huérfano, recogida en el fichero de un orfanato. Las autoridades locales denegaron el acceso argumentando que sería contrario al interés público, puesto que si los datos fueran revelados violarían la confidencialidad con la que fueron creados por enfermeras, profesores, padres adoptivos, etc., perjudicando el sistema de ayuda y protección de los niños, ya que los profesionales se negarían a redactar de nuevo tales documentos. A la vista de lo importante que era la petición de acceso del Sr. Gaskin, la dirección del orfanato intentó ponerse en contacto con todas las personas que habían contribuido a la creación de aquellos documentos para solicitarles su consentimiento en la revelación de la información. El resultado fue que algunas personas no pudieron ser localizadas y otras se opusieron, aunque sin argumentos consistentes.

El Tribunal Europeo sostuvo que era necesario examinar y encontrar un equilibrio entre los intereses generales de la comunidad y los del individuo. Entendió que había existido una violación al artículo 8 porque tales datos concernían a la vida privada y familiar del reclamante, constituyendo un interés vital para el individuo, ya que de lo contrario sería incapaz de entender su infancia y adolescencia. Además el Tribunal añadió que una denegación de acceso a los ficheros basado en argumentos de que las personas que han intervenido en su creación no fueron localizadas o que se opusieron injustificadamente, exigía la existencia de una autoridad independiente que decidiera si procede el acceso o no. La ausencia de esta autoridad impidió que el demandante tuviera garantizado el respeto de su propia vida privada y familiar, por lo que se violó el art. 8 del Convenio Europeo de Derechos Humanos (Gaskin *vs*. Reino Unido, sentencia del 7 de Julio de 1989).

325.8. En Argentina, el caso resuelto por la Corte Suprema de Justicia de la Nación, caratulado:" *Urteaga, Facundo R. c/ Estado Mayor Conjunto de las Fuerzas Armadas" (Octubre 15/1998)* dejó establecido que el *habeas data* ampara la identidad personal y permite ampliar la cobertura sobre el sentido personalísimo de ese derecho.

---

[66] HERRÁN ORTIZ, ob. cit., p. 145.

En este sentido se afirmó que la protección garantizada facultaba al hermano de la víctima (desaparecida años atrás y de la cual no existían noticias ciertas) a esclarecer las circunstancias en que se produjo la muerte de su familiar, y en su caso, el destino dado al cadáver.

El voto unánime de la Corte fue sostener que:

> […] de acuerdo con lo expuesto, lo afirmado por la Alzada en cuanto a que la finalidad perseguida en la presente acción no se compadece con el texto constitucional, se aparta de las circunstancias de la causa. Ello es así en la medida en que la presentación inicial —entre otras peticiones— incluía la de obtener información existente en registros o bancos de datos públicos que permita al recurrente establecer el fallecimiento de la persona desaparecida y, en su caso, conocer el destino de sus restos, es decir, acceder a "datos" cuyo conocimiento hace al objeto de la garantía de que se trata.

325.9. Desde el derecho a la identidad se puede encontrar otra proyección interesante: el *derecho a la verdad*.

La extensión que promete la garantía protegida por el *habeas data* se fundamenta en el derecho que "toda persona" tiene para saber la verdad sobre los hechos que le conciernen, que se tornan ineludibles cuando está de por medio la libertad de intimidad.

La pauta constitucional (o legal) abarca manifestaciones distintas como son el derecho de amparo, la tutela de la supremacía de la ley fundamental, la exigencia de licitud, lealtad y exactitud en la información contenida en archivos o bancos de datos públicos y privados, la defensa de la libertad ambulatoria, entre otras garantías afincadas en el contexto.

Pero en esta dimensión, las normas parecen circunscribir el alcance, dejando el *habeas data* solo para quienes tienen una afectación directa y personal. Esta es la tendencia legislativa que reglamentan las constituciones de Portugal, de España, los Países Bajos, Hungría, Suecia y Perú, entre otros. Y es, por su parte, la opinión que en "*Urteaga*" domina el pensamiento del Ministro Fayt.

> Dice el Juez Superior en el Considerando 9 de su voto que el núcleo del tema es la libertad del individuo frente al procesamiento de datos, es decir, la protección del individuo contra la evolución técnica de la informática. En tal sentido, la Declaración de Derechos y Libertades Fundamentales de 1989, aprobada por el Parlamento Europeo, reconoce a las personas el derecho a la intimidad en su art. 6 y les confiere el derecho de acceso y de rectificación de los datos que les afecten en los documentos administrativos. En cuanto al control sobre los datos acumulados y procesados en registros o bancos de datos públicos y privados, se trata de un derecho individual reconocido únicamente al afectado…

325.10. Sin embargo, el derecho a la identidad se relaciona profundamente con el derecho a la intimidad, y como ya hemos dicho, ambos usan al *habeas data* como instrumento destinado a evitar injerencias extrañas en la vida privada, y en la medida de sus posibilidades, responde también para reparar el honor agraviado, la imagen perturbada o la identidad igualmente afectada.

La personalidad de un individuo está conformada por ese conjunto de atributos que lo destacan (nombre, imagen, reputación, etc.), de forma que ella se mantiene como un derecho inalienable a la identidad. Si esa malla de protección se penetra por actos abusivos, autorizados o no, y registran datos de esa persona ofreciendo un archivo documental sobre la misma, es justo y legítimo que la base mantenga una verdad refleja de la identidad.

La persona concernida tiene, efectivamente, un derecho a ser informado sobre las características del registro; la duda que cabe plantear es si es un derecho transmisible o, en su caso, si finaliza con la muerte del interesado.

325.11. En nuestro parecer, el problema no está en la prosecución del derecho por otros, sino en el mantenimiento del archivo que, por tanto, conserva datos que pueden ser importantes para situaciones distintas.

> La Corte Nacional completa la idea en el voto del Dr. Petracchi en la citada causa "Urteaga", por el cual se sostiene que la negativa del Estado a proporcionar la información que estuviera registrada acerca del destino de una persona posiblemente fallecida, afecta indudablemente la vida privada de su familia, en tanto ésta ve arbitrariamente restringida la posibilidad de ejercer derechos tan privados como el del duelo o el de enterrar a los propios muertos.

Agrega el citado ministro que:

> […] dado que el *habeas data* se orienta a la protección de la intimidad, el giro "datos a ella referidos" debe ser entendido como el reaseguro del derecho básico protegido por la norma, como medio de garantizar que sea el titular de los datos el que pueda obtener el desarme informativo del Estado, o de quien fuere, para poder decidir acerca del destino y contenido de dichos datos. Pero, además, en tanto el texto constitucional permite ejercer un control activo sobre los datos, a fin de supervisar no sólo el contenido de la información en sí, sino también aquello que atañe a su finalidad, es evidente que se trata, a la vez, de un instrumento de control. Por lo tanto, no es posible derivar de la citada expresión un permiso genérico para que el Estado se exima de su "deber de información", pues ello significaría revertir su sentido fundamental.

La identidad resulta así proyectada a un derecho justo como es reconstruir el pasado de alguien que pertenecía a nuestra intimidad y que desaparece sin causas, al menos, razonablemente lógicas. Saber la verdad es también aquí el derecho que se garantiza desde el *habeas data*.

> Insistimos con el carácter de leading case que tiene "Urteaga", y en lo profundo de sus votos. Por ejemplo, en párrafos finales, agrega Petracchi que …en la medida en que lo solicitado representa el ejercicio de un interés legítimo, y en tanto ello no vulnera en modo alguno la intimidad de terceros, no cabe restringir la legitimación activa del recurrente, con base en que no se trata de "datos referidos a su persona". Pues proteger el derecho a conocer todo lo relativo a la muerte de un familiar cercano ocurrida en las circunstancias referidas significa, en última instancia, reconocer el derecho a la identidad y a reconstruir la propia historia, los cuales se encuentran estrechamente ligados a la dignidad del hombre.

325.12. Es evidente, en consecuencia, que los vínculos jurídicos familiares, que determinan el estado de familia, integran la identidad de la persona y, en la perspectiva funcional y dinámica que alentamos para la garantía creada, puede obtener tutela el tercero que tiene el derecho a saber la verdad.

También la Corte Nacional argentina en el precedente "*Suarez Mason*" (agosto 13/1998), sostuvo en el voto del Dr. Boggiano que:

> [...] la actora tiene derecho a obtener la información que existiera en los organismos públicos requeridos pues, tal como ha sido expresado anteriormente, la Constitución ha consagrado el derecho a conocer los datos que el Estado pudiera tener de su persona que, en la causa, concierne a su hija... Pues tal como ha juzgado este tribunal, el derecho consagrado en el art. 19 de la Constitución Nacional protege jurídicamente un ámbito de autonomía individual constituido por los sentimientos y las relaciones familiares de proximidad existencial y, por lo tanto, el desconocimiento de la verdad acerca de las circunstancias de la desaparición de su hija y de dónde se hallan sus restos afecta gravemente su derecho a la identidad y a la intimidad, que en su fase positiva, habilita la presentación efectuada en autos.

En síntesis, el derecho a la identidad permite generalizar el objeto tutelado sin caer en el riesgo limitativo de las fórmulas constitucionales rígidas e inalterables, donde la precisión matemática no tiene cabida.

326. El derecho a la vida privada

326.1. Toda persona tiene derecho a vivir su propia vida; a desarrollarse conforme pueda y pretenda; a generar relaciones con otros o a mantenerse ajeno y en soledad. Los comportamientos del hombre serán externos cuando se proyecten hacia otros dando publicidad a esos actos; o serán internos e intransferibles cuando permanecen en el espacio interior de la persona. Este es el terreno de lo privado, lo propio, la esfera de máxima intimidad.

La vida privada es una parte esencial de la persona, que sin resultar secreta ni de carácter íntimo, merece el mayor de los respetos para garantizar el normal desarrollo de las libertades.

La doctrina suele distinguir entre "vida privada", haciendo referencia a una esfera de retiro y aislamiento donde los demás dejan en paz al sujeto; e "intimidad" por la cual el individuo tiene un mundo propio, fuera de los ojos de los demás. Mientras el *derecho a la intimidad* tutela la zona espiritual, reservada, de la persona que permanece en su interior, referida a la conciencia de sí mismo como ser humano libre en su ámbito moral e intelectual; el *derecho a la vida privada* se manifiesta a través de la realización de actividades y comportamientos en un ámbito estrictamente personal, de amistad o familiar en que el sujeto decide desarrollar su existir, preservando esa esfera de su existencia del conocimiento general.

326.2. Es verdad aquella reflexión de Sartre cuando dice que la mirada del otro nos esclaviza, pues trasciende la metáfora, porqué cuando alguien nos mira nos juzga y, cuando nos juzga, de algún modo, nos domina.

La opinión pública se forma, en buena medida, con este juego sutil de la observación penetrante; de otro lado, la soledad, parece emerger como remedio que relaja la tensión que produce la presencia de quienes nos miran para analizarnos.

La presencia informática en la vida de las personas es cotidiana; se manifiesta continuamente desde nuestros primeros pasos en el día y no deja de abandonarnos en la práctica frecuente. A veces, la voluntad implícita de la persona reporta una autorización no pensada para quien está observándonos y registrando esos actos y costumbres (*v. gr.:* encuestas; inscripciones en concursos; planillas que se completan a ciertos fines, etc.). Otras, la información se debe ofrecer como un requisito para "entrar" en un ámbito determinado (*v. gr.:* asociaciones, entidades financieras; bancos; hoteles, etc.); también el Estado almacena nuestros datos con finalidades diversas (censo poblacional; identidad de las personas; historias médicas; etc.) y así, sucesivamente, el hombre encuentra que su vida está archivada prolijamente en un banco de información.

326.3. Lo trascendente no es el carácter más o menos íntimo de los datos personales que se cedan, sino las posibilidades infinitas de la técnica informática para tratar esos datos (posiblemente irrelevantes cada uno de ellos para la intimidad de su titular) y extraer de ellos informaciones precisas.

Sostiene el Tribunal Constitucional español que:

> el incremento de los medios técnicos de tratamiento de la información puede propiciar la invasión de la esfera privada, haciéndose necesario la ampliación del ámbito de juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestos en práctica a través de cualquier instrumento que produzca tal efecto, y a incrementar las facultades de conocimiento y control que se otorguen al ciudadano para salvaguardar el núcleo esencial de su derecho […] Las normas autorizatorias de recogida de datos, incluso con fines legítimos y de contenido aparentemente neutro, deben incluir garantías adecuadas frente a su uso potencialmente invasor de la vida privada, por lo que si no lo hacen pueden y deben considerarse vulneradoras de la intimidad.[67]

Por tanto no hay datos que sean secretos absolutamente sino en la medida que se han conocido, a cuyo fin, regresamos al punto de la confidencia o al derecho a la reserva que antes mencionamos.

Es decir, la garantía constitucional del proceso de *habeas data* procura que la vida privada de los hombres no sea invadida ilegítimamente por el acopio o almacenamiento de datos personales, ni que ellos sean difundidos sin la expresa autorización del titular o de quien tenga derechos de representación.

De algún modo, esta línea de pensamiento se asocia a la diferencia que hacía Nino y que explica con suficiencia Eduardo Oteiza cuando expone que:

> la noción de privacidad pareciera abarcar dos conceptos independientes que garantizan ámbitos distintos. Por una parte, nos encontramos con las acciones privadas que no dañan a terceros y sólo afectan a la persona que las realiza. Ellas solamente entran en juego

[67] ESTADELLA YUSTE, ob. cit., p. 167.

> con la moral personal, al consistir en la elección de aquellos aspectos que conforman el plan de vida de cada individuo. En el plano normativo el artículo 19 de la Constitución Nacional acepta el principio liberal de la autodeterminación, que deja librada a la decisión individual las acciones privadas. Sin embargo, una lectura restrictiva, fundada en ideas perfeccionistas, que consideran el Estado puede interferir con conductas que no lesionan a terceros, bajo la pretendida defensa de sus propias convicciones y creencias sobre una proyección comunitaria, ha limitado el marco de libertad en áreas sensibles para la ética individual, apoyada en su propia apreciación de la moral pública.[68]

326.4. La diferencia entre moral pública y ética privada ha sido explicada a partir de la noción de privacidad, que se ha utilizado, también, para identificar a aquellas circunstancias que caen bajo el dominio exclusivo de una persona, por su voluntad de no dejarlas trascender a otros. Nino, siguiendo a Parent, vinculaba el concepto de privacidad con la posibilidad irrestricta de realizar acciones privadas que no son objeto de una moral pública, separándolo de la idea de intimidad. Asociaba a esta última con el derecho a que los demás carezcan de información sobre hechos personales, cuando el sujeto al que se encuentran asociados niegue su consentimiento. Consiste, entonces, —concluye Oteiza— en la exclusión de información documentada accesible al público, mediante la potestad de limitar el conocimiento sobre aspectos personales, cuando el mismo no se encuentre justificado por una razón que en la tensión entre la reserva y la publicidad ceda en favor de la primera.[69]

326.5. A pesar de ello, no es la propia determinación sobre la transmisión del dato lo que caracteriza el derecho a tener una vida privada, sino el derecho a mantenerse ajeno a las intromisiones ilegítimas o legítimas pero infundadas.

Asimismo, muchas veces el límite entre intimidad y privacidad es difuso y no se podría hallar un derecho preciso que alimente la fuente de protección respectiva; en definitiva, todo conduce a sostener que la limitación que se persigue pretende, como mínimo, que nadie se entrometa en la vida de otro sin tener consentimiento para ello, y que el individuo mantenga la libertad de resolver, en todo tiempo y espacio, que aspectos de su vida personal quiere ocultar o trascender.

En opinión de Bianchi:

> la distinción entre privacidad e intimidad es más aparente que real. Para ello se vale de algunos ejemplos: una reunión es íntima o privada cuando asisten a ella algunas pocas personas elegidas. La correspondencia que intercambian dos individuos es íntima o privada entre ellos y no debe ser conocida ni divulgada por otros. La relación carnal entre dos personas es íntima o privada entre ellos y no puede ser objeto de interferencia alguna. En todo caso —y con ánimo de formular alguna diferencia— podría decirse que íntimo, es más privado aun que lo privado. El fuero íntimo de una persona es lo que sólo le pertenece a ella y está exento de cualquier objetivación forzosa. Desde este punto de vista, afirma el prestigioso publicista argentino, el pensamiento es íntimo mientras no

---

[68] OTEIZA, Eduardo David, *Información privada y habeas data*, comunicación presentada en el XX Congreso Nacional de Derecho Procesal, San Martín de los Andes (Argentina), 1999.

[69] OTEIZA, ver nota anterior.

sea objeto de exteriorización y se transforma en privado cuando es divulgado en un pequeño o limitado círculo.[70]

326.6. Cuando se estudia el derecho a la vida privada, en realidad, no se demanda que sea éste el fundamento del *habeas data*, sino que es una parte de todo ese cuadro de derechos que mejoran el perfil del proceso constitucional creado.

Observado atentamente el fenómeno en el tiempo que transcurre, se puede advertir que la distancia está trazada entre la tutela que deriva del derecho a la intimidad y, en su caso, del carácter individual que tiene, y por ello, el signado de derecho personalísimo. Frente a la corriente que postula la relación con el "tratamiento de los datos", en cuyo supuesto la atención no se fija tanto en la persona como sí en el interés en preservar la veracidad de la información y el uso que de ella se hace.

Sostiene Garzón que:

> la categoría de "protección de datos" ha surgido para aplicarse a nuevas realidades jurídicas, que sólo parcialmente pueden ser descriptas o fundamentadas a través de la noción tradicional de "intimidad". El derecho a la protección de datos, según su propia expresión, pertenece al contexto de la era informática y ciertamente resulta atrevido afirmar que esta compleja disciplina legal estuviera ya implícita en las referencias generales al derecho a la intimidad inserta en cuerpos normativos de ámbito nacional o internacional de la era preinformática.[71]

326.7. La vida privada que atiende el *habeas data* se vincula con todas aquellas manifestaciones que se registran o archivan con alguna finalidad sin tener consentimiento expreso de la persona.

> Recordemos que el resonado caso argentino fallado por la Corte Suprema de Justicia de la Nación (CS, 11 de diciembre de 1984) en autos "*Ponzetti de Balbín c/ Editorial Atlántida s.a.*", sostuvo que el derecho a la privacidad e intimidad, en relación directa con la libertad individual protege un ámbito de autonomía individual constituida por sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significa un peligro real o potencial para la intimidad. En rigor, el derecho a la privacidad comprende no sólo la esfera doméstica, sino otros aspectos de la personalidad espiritual o física de las personas, tales como la integridad corporal, la imagen, y nadie puede inmiscuirse en la vida privada de una persona ni violar las áreas de su actividad no destinadas a ser difundidas, sin su consentimiento o el de sus familiares autorizados para ello, y sólo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de la libertad de otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen.

"Vida privada" hace referencia a una esfera de retiro y aislamiento, al ámbito donde los demás dejan en paz al sujeto, con tranquilidad para actuar y donde no

---

[70] BIANCHI, Alberto B., *Habeas data y derecho a la privacidad*, El Derecho, 161-866.

[71] G. GARZÓN CLARIANA, *El marco jurídico de los flujos internacionales de datos*, IBI, Doc. TDF 206, Roma, 1984, *passim*.

tienen derecho a inmiscuirse. En tanto que la intimidad se refiere al individuo, a un "mundo propio", fuera de los ojos de los demás, se trata de la esfera más sagrada de la persona.

Esta interpretación conlleva a fragmentar la defensa del *habeas data* si aplicamos la jurisprudencia tal como se expresa.

Es decir, la privacidad se recorta en dos vertientes: la vida personal y la vida familiar, y en la misma línea, la inviolabilidad del domicilio y de la correspondencia particular.

326.8. Por eso la vida privada excede a la intimidad, y por tanto comprende, además de los bienes que el fallo enumera, otros como la imagen y el honor. En consecuencia, también las personas jurídicas tienen vida privada, aunque no posean intimidad.

La distancia entre vida personal y derecho a la intimidad no supone que la primera necesite de una regulación legal expresa mientras la segunda cuente con respaldo constitucional, en razón de que en Argentina, de conformidad con el artículo 75 inciso 22 de la Ley Fundamental, reconoce varios tratados y convenciones donde se distingue la defensa que al domicilio, a la correspondencia, a la propia imagen y a la individualidad se dispensa.

De algún modo puede coincidir con esta idea la opinión de Martínez Sospedra cuando expresa que:

> …de este modo aquellas áreas de la vida privada que exceden del ámbito de la intimidad y no se hallan protegidas ni por el derecho fundamental a la misma ni por los otros derechos fundamentales con incidencia en aquella obtienen protección constitucional mediante la internalización de las disposiciones de los tratados que reconocen el derecho a la vida privada que provoca la ratificación de los mismos. En sentido estricto no hay, pues, en nuestro ordenamiento (España) un derecho propiamente constitucional a la vida privada, pero si existe, mediante la vía señalada, una suerte de derecho *paraconstitucional,* si bien el mismo sólo es protegible en amparo en aquellos supuestos en que se puede obtener la cobertura del artículo 18 de la Constitución española.[72]

326.9. En síntesis, el derecho a la vida privada contrae, al menos, las siguientes obligaciones:

- Recrear la doctrina del derecho a estar a solas, evitando que la persona humana sea invadida por intromisiones de cualquier naturaleza que afecten su vida íntima o privada.
- Auspiciar una defensa efectiva del individuo contra la publicidad de actos personales que se ponen a disposición del público interesado sin conocimiento ni permiso del afectado.
- Propiciar un régimen de control sobre el almacenamiento de datos personales y el destino que a ellos se asigne.

---

[72] Martínez Sospedra, Manuel, "Sobre la intimidad. Derecho a la intimidad, vida privada y privacy. El art. 18 CE in principio en la jurisprudencia del Tribunal Constitucional", en *Sobre la intimidad,* Fundación Universitaria San Pablo C.E.U., Valencia, 1996, p. 56.

- Formular un criterio economicista respecto a la vida privada, a cuyo fin se la puede analizar como resultado de la difusión y retención de la información en el contexto comercial y personal.
- Dar un sentido amplio al derecho a tener una vida privada, para evitar el egoísmo de considerar únicamente el problema del tratamiento de datos, sin relacionar otras situaciones tan o más importantes que ella, como son las intercepciones telefónicas, la penetración de los correos electrónicos, la invasión domiciliaria de publicidad, etc.

327. La vida familiar

327.1. El derecho de exclusión que pervive en la defensa de la vida privada, en cuanto evitar o prevenir las intromisiones en la dimensión de lo que resulta absolutamente reservado y secreto de las personas; se extiende a la vida familiar como una proyección del derecho a la privacidad.

En este aspecto, la tutela constituye un avance necesario en la forma de resolver la invasión o perturbación en el reducto de lo íntimo, si se tiene en cuenta que la protección estuvo dirigida a salvaguardar la familia de la indiscreción y las consecuencias que traía a ella ese conocimiento de hábitos o costumbres.

Sostiene Lyon que:

> constituye una realidad que, si bien en sus comienzos la protección de la vida personal se salvaguardaba frente a la indiscreción ajena que, con más curiosidad que malicia, interfería en la intimidad de quienes por su profesión, condición o deseo se consideraban personas públicas, hoy la protección de la intimidad o de la privacidad de las personas adopta una nueva dimensión, más social, menos individual y que se proyecta en las circunstancias más cotidianas e irrelevantes de la existencia humana. Negar que la protección de la persona en la era de las computadoras ha superado el estricto ámbito de la intimidad, representaría la negación de una realidad constatable pero, igualmente, podría calificarse de parcial un estudio de la protección de la persona en la que la intimidad, como aspecto de la personalidad individual, no sea reconocida en cuanto ámbito personal digno de tutela frente a las agresiones informáticas.[73]

327.2. La vida en familia representa un sin número de comportamientos que identifican el perfil del diario acontecer. Existen gustos, tolerancias, manifestaciones que identifican el carácter de los miembros, preferencias, etc. que, observadas y registradas, definen el ser cultural y económico del grupo. Cuando esa vigilancia es producto de intromisiones directas o indirectas, debe existir un control sobre ellas y una forma de prevenir el uso de ese archivo de costumbres.

A veces, la familia se encuentra invadida sin saberlo, aunque de hecho lo admite. El caso de medios electrónicos que conviven con ella es habitual. Por ejemplo, la televisión representa hábitos, promueve usos y costumbres. La utilización de la red Internet obliga a dejar datos y otros registros cuando se practica el comercio electró-

---

[73] LYON, David, *El ojo electrónico. El auge de la sociedad de la vigilancia,* Alianza, Madrid, 1995, p. 18.

nico; el uso del teléfono es también un medio indirecto de invasión a la intimidad (por eso, saber quién nos llama antes que un servicio es un derecho).

> Cierto que, en principio —afirma Herrán Ortiz— el conocimiento de los comercios donde una persona adquiere sus enseres o el vestuario parecen datos irrelevantes y sin trascendencia, no obstante, adviértase que el conocimiento de estos datos debidamente relacionados pueden ofrecer una imagen de la persona, de sus gustos, aficiones o puede revelar, por ejemplo, su desmesura en el gasto. Datos, todos ellos que pueden perjudicar a la persona, no por su falsedad o por el desmerecimiento de su reputación, sino por el solo hecho de que el individuo no ha consentido su almacenamiento y, menos aun su utilización por terceros.[74]

327.3. La utilidad para otros de estos hechos cotidianos seguramente es inasible o probablemente difuso. También es cierto que esa ausencia de daño, peligro o incertidumbre, no puede solaparse tras la defensa de la intimidad o la privacidad como derechos de contenido personal (subjetivos).

Lo que se procura mantener en la mira del *habeas data* es el control sobre los registros, antes que evitar la recopilación propiamente dicha. Toda información de la persona, familia y amistades, ese reducto o círculo de "los íntimos" no puede ser observado con desinterés y tolerancia, seguramente tiene un fin y un objetivo. En consecuencia, es una amenaza y necesita una herramienta de control.

328. Derecho a la privacidad

328.1. Todas las manifestaciones de la libertad de intimidad asumida como derecho fundamental de las personas, o bien, del derecho a la intimidad interpretada como derecho subjetivo, permiten desplazar cada uno de los enunciados hasta aquí presentados.

Es decir, desde la intimidad uno puede llegar al honor, a la propia imagen, a la fama o reputación, a la reserva y confidencialidad, al secreto, al derecho al olvido y a la verdad, etc. etc.; pero el marco donde ha de ubicarse el proceso de *habeas data* requiere, siempre, del tratamiento de datos de una persona que por esa causa tiene interés. Luego de observar el uso y destino de ese archivo sobre alguien, se podrá colegir si está afectado el honor, la fama, el secreto, o cualquiera de los derechos antes enumerados. Y, en todo caso, si la vía procesal que se implementa es, efectivamente, la garantía constitucional creada y en estudio, para recién allí determinar la condición del acto lesivo.

Sobre esta base la cuestión parece demasiada compleja, cuando en realidad no lo es. La defensa de la intimidad puede ser el género que amplía las fronteras del *habeas data*; pero el derecho a la privacidad resulta más adecuado para recibir los bienes a tutelar por el proceso.

328.2. En efecto, *privacy* tiene un sentido activo que tiende a concretar la protección de los particulares impidiendo que terceros se ocupen de la vida privada de

---

[74] HERRÁN ORTIZ, ob. cit., p. 135.

otros. Al mismo tiempo, implica que si el banco de datos es legal y permitido, sea también "privado", en el sentido de lograr confidencialidad y secreto, seguridad y privacidad en la transmisión que se efectúa.

No se tratan de bienes jurídicos diferentes, pues la privacidad que la persona prefiere, a veces no es posible, porque los registros se toman en diversas formas y manifestaciones (por ejemplo, ofrecer datos personales en un requerimiento de crédito o completar una planilla de inscripción para un sorteo ofrecido) y pocas veces puede conocer el uso posterior que se dará a esos datos.

328.3. Si interpretamos la privacidad en ambas dimensiones, los intereses se pueden conciliar. Tanto los del hombre y su derecho a la libertad de intimidad; como los de la empresa que en ejercicio de un comercio lícito debe resguardar la seguridad del sistema (privacidad en las comunicaciones).

De este modo, intimidad y privacidad no son realidades contrastables.

> Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservada de la vida de las personas —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo—, la privacidad constituye un conjunto, más amplio, más global, de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo" (párrafo de la Exposición de Motivos de la LORTAD* española).

328.4. Creemos que el ámbito natural del *habeas data* es el derecho a la privacidad, en dos sentidos: uno se dirige como mensaje impeditivo o barrera que se pone para evitar que la vida personal sea accesible a otros cuando el titular no lo admite; el restante, como acción positiva tendiente a obrar preventivamente frente a las agresiones provenientes de la informática.

La *privacy* se concibe por un sector doctrinal como una libertad positiva para ejercer un derecho de control sobre los datos referidos a la propia persona que, si bien han emergido al exterior, fuera de la esfera íntima de la persona, y se han incorporado a un archivo electrónico, nada impide que puedan continuar bajo control y salvaguarda de su titular. En definitiva, se identificaría con el mismo derecho a la autodeterminación informativa, porque ese es el significado y contenido de este derecho. Se confunde pues, el derecho en sí mismo como medio y respuesta jurídica de tutela de la persona, con el ámbito o bien jurídico tutelado, si la privacidad se identifica con los aspectos o ámbitos de la existencia personal que se preservan del tratamiento informatizado, no puede identificarse con el derecho que lo tutela.

328.5. Si en la defensa de la intimidad el fin fue evitar las intromisiones en la vida privada y espiritual de alguien; en la tutela que reserva el *habeas data* el derecho

se actúa, antes que previene. Es un ejercicio plenamente dispositivo de la libertad de control sobre los datos que le conciernen.

En definitiva no se trata de defender a la persona en su hábitat individual, en su soledad absoluta o en la confidencia más extrema; porqué el *habeas data* no es una cuestión de hermetismo o secreto, sino de otorgar un recurso a la privacidad, permitiendo con ello una vía de control a la esfera de reserva.

328.6. Sin embargo, no es bueno auspiciar que esta vía permita eludir todo tipo de registros o transmisión de datos que son necesarios para la vida social y para los intereses del Estado.

No es posible instaurar un recurso a la privacidad para ocultar datos de carácter económico, patrimonial o penal, impidiendo con ello aquellas formas de control social que tutelan los intereses de la comunidad.

Se trata, por tanto —dice Alpa— de la defensa de la persona frente a la intromisión, la recogida, difusión y utilización de aspectos de su vida pertenecientes a su privacidad, actos que hoy son frecuentes y ante los cuales no podía oponerse un conjunto de instrumentos jurídicos eficaces.[75]

328.7. Lo dicho en párrafos precedentes no debe conducir a la creencia de que el *habeas data* se aloja únicamente en la vida privada o personal, ni que el Estado —o los particulares que comercializan con bases de datos— cuenten con una herramienta útil para legitimar el uso que aplican a esos registros.

Los derechos de la privacidad, en realidad, constituyen una gama muy compleja de situaciones que fueron transformándose en la historia del mundo hasta llegar a un estadio donde resultan plenamente imbricados con las acciones públicas y, por tanto, donde no es posible ni fácil resolver cuál de esos derechos tiene primacía.

En efecto, cuando se observa el desarrollo del mundo moderno, se advierte la influencia notable que tiene la sociedad en la vida de las personas. Existe en cada etapa una suerte de búsqueda por la burguesía porque instalados en esa posición resultaba más simple relacionarse y obtener influencia. Un mundo que abandonó la sociedad feudal requería del poder vinculado a los terratenientes pero con un sentido más social que económico.

Sostiene Jürgen Habermas que:

> el espacio público se constituye en la modernidad desde la búsqueda por la burguesía de una esfera donde proyectar su modo de experimentar la vida, en medio de sociedades donde el poder se articulaba desde la nobleza que lo ejercía en representación de todo el cuerpo social. La burguesía, basándose en las posibilidades y requerimientos de comunicación y noticias de un mundo en expansión, concibió, en oposición al Estado estamental, un espacio donde, utilizando la expresión oral y sobre todo la tecnología de la escritura (correspondencia, archivo, circulación de documentos), personas carentes del poder político legítimo, es decir, privadas, podían desarrollar relaciones sociales intensas mediadas por el razonamiento, generalizando idealmente sus experiencias subjetivas de

[75] ALPA, Giuseppe, *Compendio del nuovo Diritto Privato,* UTET, Torino, 1985, p. 34.

> vida en la familia nuclear. Recíprocamente, lo privado ha dejado de ser, como lo era en la sociedad feudal, el sitio de procura de las necesidades, o sea, un lugar de producción, puesto que el modo de producir había desbordado latamente las fronteras de la economía doméstica hacia el mercado, desterrando de ella el esfuerzo social para dejarla exclusivamente ocupada de las relaciones familiares. De este modo es que nacen íntimamente vinculadas las esferas de publicidad y privacidad.[76]

328.8. La vida cortesana va a demostrar la influencia del orador y del escritor, cada uno con su público y su inagotable poder para instalar conceptos sobre temas que "a todos interesa". Esta primera etapa nos sirve para comprender la fuerza y pujanza de la opinión transmitida y de algunas de las razones por las que debe mantenerse esta suerte de libertad de expresión que forja una sociedad.

Sin embargo, la familia se reconduce hacia lo personal (*my home is my castle*). Se estrechan las relaciones y comienza una etapa donde la intimidad es el producto de la necesidad de pensar por sí mismos. El Estado, los burgueses, no podían continuar aquel estado de dominación.

El estudio de Carlos Peña, en la compilación de monografías efectuada por la Universidad Diego Portales, es elocuente cuando expone:

> …Allí es cuando la privacidad incorpora el ideal de la intimidad, como algo diverso tanto de lo propiamente público, el poder legítimo que no pertenecía a la burguesía, pero ante el que poseía una autonomía asegurada por la propiedad privada, por un lado; por otro lado, también respecto a la producción económica, de su dinámica de enfrentamiento racional en la publicidad del mercado, respecto del cual ofrecía el lugar adecuado para depositar los sentimientos, y en tercer lugar, en relación a la publicidad cultural de la "vida social" que hacía la burguesía, de la cual, sin embargo, era su antesala al asumir la familia la función educativa de los miembros de ella.[77]

Cuando el individuo se convierte en ciudadano (siglo XVIII), la polaridad entre lo público y privado se hace más intensa, en razón de que se institucionaliza la representación política y el poder de la opinión pública (eludiendo el significado que había tenido la burguesía en la vida cortesana); frente a la sociedad que, en definitiva, era un agrupamiento de personas privadas y esencialmente emancipadas del poder económico del Estado.

Así, la vida privada se transforma en una idea pública que al menos ideológicamente ofrece a toda la sociedad un espacio público ampliado (Peña).

La última etapa nos muestra el intervencionismo del Estado en las relaciones privadas y con una absoluta indiferencia por la intimidad y reserva que tenía el núcleo familiar. Se difumina la autonomía económica y comienza una sociedad de masas donde el consumo marca las preferencias. Queda en evidencia la destrucción del ideal de aislamiento (entre lo público y privado) y la defensa de lo propio se re-

---

[76] HABERMAS, Jürgen, *Historia y crítica de la opinión pública,* traducción de Antoni Domenech, Ediciones de Gustavo Gili, Barcelona, 1994, pp. 45 y ss.

[77] *Cfr.*: MEDINA, Cecilia, MERA FIGUEROA, Jorge, *Sistema jurídico y derechos humanos*, Escuela de Derecho de la Universidad Diego Portales, Santiago de Chile, 1996.

suelve desde los derechos fundamentales, dando lugar a un nuevo orden internacional para los derechos humanos.

> En esta etapa —dice Peña— se produce la degradación de la autonomía privada, ideal radicado en el hogar familiar, la cual pierde su fundamento en la propiedad privada disponible arbitrariamente y ahora sobre regulada y con ello disgregada, mudándose en una autonomía de consumo. El consumo, a su vez, tampoco es esencialmente privado, por cuanto muchas veces empiezan a depender del Estado para procurar sus necesidades básicas. De este modo es que la familia pierde toda relación con el mundo del trabajo. Ello traerá por consecuencia el descargar a la familia también de su capacidad de intimación personal, debido a la férrea dependencia de la vida familiar del Estado social y la sociedad organizada. Dicha situación tiene dos paradigmáticas expresiones que nos interesarán: el fracaso del ideal del aislamiento, tanto física (en la gran urbe) como psicológicamente (desvalorización de la vida solitaria), y la socialización inmediata de las personas a través de los medios de comunicación social (con lo que pierde la familia su función protectora respecto de lo público, quedando a merced, antes bien, más que de lo público en sentido político, de lo semipúblico).[78]

328.9. El tránsito por distintas etapas evidencia la transformación del concepto de privacidad, como la tensa relación entre el dominio de lo público y lo privado.

La aspiración de ser dejado a solas; de vivir una vida propia con el mínimo de injerencias exteriores; de autodeterminar sus relaciones sociales; de desarrollar la personalidad sin ataduras ni compromisos, cada una de estas expresiones que son, definitivamente, derechos de las personas, tienen ante sí las dificultades de su propia concreción.

Las citadas etapas, en la explicación del derecho a la intimidad o bien, acotando la mención, del derecho a la privacidad, son presentadas habitualmente bajo dos teorías posibles que, en realidad, pretenden focalizar —cual si fuera el haz de luz de una linterna— qué derechos deben protegerse.

328.10. Estas teorías son las denominadas "de las esferas" y "del mosaico". Mientras la primera refiere al derecho de la intimidad representado en círculos concéntricos donde el anillo central es la esfera de máxima reserva y los demás, dirigidos hacia el exterior, van hilando sucesivamente, las esferas del secreto, la confidencialidad, la confianza, hasta llegar a las cercanías de lo público que constituyen las relaciones del hombre con los demás persiguiendo crear una imagen de sí mismo.

> La teoría del mosaico —explicada por Diana de Slavin— resalta los diferentes roles que desempeña el individuo. Este conforma un complejo de informaciones, y según se articulen éstas el resultado final será diferente. Aquí se debe entender no solamente el carácter intrínseco del dato, a su intimidad, sino también a quienes tienen derecho para acceder a él.[79]

---

[78] PEÑA, ob. cit., en compilación de nota anterior.

[79] DE SLAVIN, Diana, *Mercosur: La protección de los datos personales,* Depalma, Buenos Aires, 1999, pp. 33 y ss.

Concretar la defensa constitucional en terreno de lo público o lo privado, frente a la situación que advierte un desarrollo simultáneo en ambos niveles, obliga al poder del Estado a promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas. Han de removerse los obstáculos que dificulten o impidan la plenitud del derecho constitucional creado, de forma tal que los siguientes derechos proyectados desde la privacidad, pueden encontrar una auténtica respuesta:

a) La intromisión en el ámbito de reserva y soledad que una persona pretende crearse (intrusión que se puede dar hacia los bienes o en la intimidad del hogar). Derecho que se afecta de manera directa con la grabación de conversaciones privadas, las intervenciones telefónicas, la filmación intrusiva de actos de la vida familiar, la observación vigilante de la familia o de la persona, el acoso irrazonable en el círculo de una persona, etc. También son agresiones indirectas la publicidad estentórea (a viva voz, por medios parlantes aéreos o viales, etc.) en horas pensadas para la tranquilidad y reposo; las llamadas telefónicas que no reconocen origen (por eso, como antes dijimos, la localización del número desde nos llaman, antes que un servicio es un derecho).

b) La divulgación de hechos privados, dados en secreto o confidencialidad. No importa que la exposición pública afecte o no el honor de la persona, pues la lesión se produce en la intimidad. Recordemos el caso Melvin c/ Reid en el cual la jurisprudencia americana sostiene que se violenta el derecho de toda persona al olvido, al narrarse en una película su pasado como prostituta.

c) La difamación que consiste en hacer públicos hechos relativos a un individuo, presentados en forma disimulada, totalmente falsos o con una imagen distorsionada con el fin de afectar o dañar a la persona concernida. Se incluyen aquí las protecciones que necesita el nombre, la voz, la imagen, y en definitiva, la fama o reputación.

d) La falsificación de atributos, por el cual una persona pretende atribuirse identidades o características que a otro pertenecen, pretendiendo con ello utilizar una imagen ajena.

e) La identidad, por el cual una persona persigue ser reconocida por su nombre y apellido, sus calidades personales, sus atributos intelectuales, y todo aquello que hace a su personalidad. Por eso, cuando un banco de datos contiene información inexacta, desactualizada o equívoca, es menester corregir el archivo desde la garantía del *habeas data*.

328.10. Con esta visión se puede aplicar el *habeas data* para la defensa del derecho a la privacidad sobre las cosas. La legislación comparada permite confrontar la preferencia de algunos para indicar espacios o lugares donde no se puede penetrar sin afectar el derecho a la privacidad.

> Novoa Monreal sostiene como privados a los hechos que presentan las siguientes características: *a)* ser desconocidos para los extraños o ajenos al círculo familiar, o que no suceden normalmente a la vista de ellos; *b)* cuyo conocimiento provoque generalmente

> turbación moral en el sujeto, por dañar su pudor o recato; *c)* que el sujeto no quiera que otros los conozcan.[80]

De este modo, si los actos se ejecutan en el interior de una vivienda o espacio exclusivo, sin importar el tiempo o el motivo en que ello suceda, al lugar se le garantiza la reserva y exclusividad.

Es este un sistema objetivo casuista que emplea el criterio de tutela de acuerdo a las circunstancias donde y como se produce. De alguna forma es una oposición al sistema subjetivo que distingue entre lo público y lo privado según la calidad de la persona en cuestión. Si es un funcionario o tiene una actividad que lo expone al contacto general del público, se interpreta que esa actuación le limita su derecho a tener una vida privada absolutamente intangible; situación que tienen también otras personas notorias o famosas.

328.11. Finalmente existe el derecho a la privacidad sobre los datos.

La evolución tecnológica produjo una intromisión impensada en la intimidad de las personas, y sobre todo, demostró que la defensa tradicional de los derechos individuales, era absolutamente insuficiente.

> Se ha dicho que la utilización de nuevas tecnologías y la entrada de nuevos intervinientes exigen esfuerzos continuamente renovados para consultar y educar, tanto al ciudadano particular acerca de los derechos que le asisten, como a los sectores público y privado acerca de las obligaciones que tienen de tratar la información personal de manera responsable y lícita. Aquí, las autoridades de control de todo el mundo para la protección de datos y la intimidad tienen un papel clave y una gran responsabilidad.[81]

Primero fueron las Convenciones Internacionales las que advirtieron la penetración del fuero íntimo mediante la técnica de recolección de datos para su posterior transmisión con objetivos diversos, o simplemente con fines de archivo estadístico o informativo.

328.12. El concepto de intimidad varió, como amplió asimismo la idea acostumbrada para resolver las invasiones ilegítimas en el reducto de lo personal. Se habló de un campo propicio para una libertad nueva: la informática y el uso responsable del dato.

Ya vimos como se produce este fenomenal cambio y de qué manera sucede la aparición del *habeas data* como proceso destinado a resolver el problema de la penetración de los derechos a través de la informática. De todos modos es conveniente recordar que en el ámbito de la contratación individual una persona no puede disponer de los derechos de la personalidad, teniendo en cuenta que no tienen conte-

---

[80] NOVOA MONREAL, Eduardo, *El derecho a la vida privada y libertad de información. Un conflicto de derechos,* Siglo XXI, México, 1979, pp. 59 y ss.

[81] BRÜEHANN, Ulf, *La escena internacional y la directiva comunitaria: 5 semanas antes de su entrada en vigor,* en XX Conferencia Internacional de autoridades de protección de datos (1998), Agencia de Protección de Datos, Madrid, 1999, pp. 133 y ss.

nido patrimonial y, como tales, resultan intransferibles, fuera del comercio. Lo que no puede ocurrir es que un sujeto enajene su derecho al honor, a la intimidad, a la privacidad o a la imagen, quedando en definitiva privado de los mismos.

Es el campo donde anida, esencialmente, la protección derivada del *habeas data*, y que sigue principios internacionales respecto a formas, modalidades y controles que debe mantener el individuo cuando se archivan sus datos en bancos destinados a cualquier efecto.

328.13. Ellos son:

a) *El principio de la calidad de los datos,* por el cual se pretende que los archivos o registros sean absolutamente fidedignos. Además, la pertinencia obliga a que la recolección y el tratamiento sean acordes con los fines del banco, incurriendo en ilegalidad cuando se aplica a objetivos diferentes a los autorizados.

b) *El principio de información del afectado*, que supone mantener informada adecuadamente a la persona sobre el motivo por el que se lo incluirá en un fichero o archivo.

c) *El principio del consentimiento* que inspira la participación de la persona en las tres etapas posibles en que actúa el registro. Primero, cuando se toma el dato; después para el mantenimiento y conservación en el archivo, y finalmente, para la cesión o transferencia a terceros de información que le concierne.

d) *El principio de protección de los datos sensibles*, que se vincula con la información estrictamente confidencial por su carácter privado y personalísimo (*v. gr.:* raza, credo, religión, salud, inclinaciones sexuales, hábitos y costumbres, etc.). La LORTAD los clasifica en tres tipos: -los relativos a la ideología, religión o creencias; los datos relativos al origen racial, a la salud o a la vida sexual y, los datos relativos a los antecedentes penales.

e) *El principio de seguridad de los datos*, considerado a los fines de evitar la introducción de terceros al archivo, de manera directa o indirecta, legítima o ilegítima, para preservar la confidencialidad y, también, para conseguir que los registros no se pierdan, alteren o modifiquen por accesos no autorizados.

328.14. El *habeas data* otorga al individuo la posibilidad de concretar el cumplimiento de cualquiera de estos principios, sea mediante el acceso inmediato, irrestricto y sin condiciones económicas que lo dificulten o esterilicen; o para la actualización, rectificación o supresión del dato que le concierne.

Según el Convenio 108 de la CEE, estos principios pueden ser limitados cuando constituyan una medida necesaria para una sociedad democrática para la protección de la seguridad del Estado: seguridad pública, intereses financieros, imposición de infracciones penales, y cuando están dirigidas a la protección de la persona concernida y de los derechos y libertades de terceras personas. Señala Garzón que, en circunstancias normales, las medidas restrictivas de los Estados deber ser, en primer lugar, motivadas y han de fundamentarse en una de las razones reconocidas internacionalmente; en segundo lugar, la acción del Estado debe emprenderse de buena fe; y por último, las medidas no deben

ser discriminatorias para los individuos sometidos a la jurisdicción del Estado, ni deben suponer un trato discriminatorio en las relaciones económicas internacionales.[82]

329. El derecho a la autodeterminación informativa

329.1. A medida que se tamiza el derecho constitucional creado, la última escala pareciera estar en la *autodeterminación informativa*. Es decir, desde la amplia libertad creadora que permite el derecho a la intimidad se llega al reducto de la libertad informática controlada por la persona respecto a sus propios datos.

Es verdad que entre uno y otro extremo se levanta voces polémicas para el reconocimiento propio e independiente de la autodeterminación o propiciando un refuerzo de las garantías de la intimidad, pero en ambos casos, queda de manifiesto que el problema está en el control que se tiene sobre los registros o archivos personales.

> Las constantes disquisiciones en torno a la independencia de un derecho a la autodeterminación informativa han evitado acuerdos coincidentes. Según Herrán Ortiz se distinguen dos sectores enfrentados, uno de los cuales rechaza la consideración del derecho a la autodeterminación informativa como derecho fundamental argumentando que es suficiente para ofrecer garantías individuales adecuadas una reformulación del derecho a la intimidad; el otro sector sostiene, por el contrario, la idea de la necesidad insoslayable de admitir la existencia de un nuevo derecho fundamental, cuya construcción se asienta sobre el reconocimiento al individuo de unas facultades de disposición y decisión respecto a sus propios datos personales que no sería posible deducir del tradicional derecho a la intimidad.[83]

329.2. La autodeterminación, como lenguaje técnico, tiene reminiscencias equívocas que nos sugiere sustituirlo por el "*derecho a la libre disposición de los datos personales*".

Lo mismo sucede cuando se aplica el término "libertad informática" pues pareciera indicar la libre utilización de los medios informáticos en el tratamiento de los datos, cuando en realidad, se trata precisamente de lo inverso: poner límites y control a esa libertad.

De esta manera, el *habeas data* surge como la mejor herramienta procesal para encausar el amparo prometido, sea para acceder a las informaciones que sobre él se tengan, así como para controlar la exactitud y autorizar, o no, la circulación de esos datos.

Si se admite que el derecho a la autodeterminación informativa reconoce la facultad del individuo a decidir cuándo y cómo está dispuesto a permitir que sea difundida su información personal o a difundirla él mismo, esto es, la facultad de la persona de controlar y conocer los datos que sobre ella se encuentran en soportes informáticos, se reconoce al individuo una tutela legal para conocer y acceder a las informaciones almacenadas en ficheros de datos que les conciernen, así como la

---

[82] GARZÓN, ob. cit., pp. 36 y 56.

[83] HERRÁN ORTIZ, ob. cit., p. 238.

facultad de controlar por el interesado la calidad de los datos inexactos o indebidamente automatizados y consentir su transmisión que define el contenido que integra la libertad informática.

329.3. Sin embargo, la garantía no reposa en el reconocimiento de un derecho subjetivo propio e individual que pueda catalogarse, indeseablemente, como derecho patrimonial (tal como acontece con la profusa enumeración de derechos que emanan de los códigos sustanciales). La fuente que nutre la defensa constitucional no es sobre un derecho de propiedad sobre los datos, cual si ellos fueran el objeto de pertenencia exclusiva que resulta inalienable e intangible. El basamento está en la libertad de resolver con plena libertad sobre el destino que se pretende dar a los datos y, en su caso, si se autoriza o no el acopio informativo de ellos.

Por eso, algunos autores prefieren hablar de intimidad informática para aludir al bien jurídico protegido frente al poder informático. Sería una proyección de los derechos personalísimos de fuente constitucional.

En este sentido, Ruíz Miguel manifiesta que:

> esta identificación constitucional constituye el medio idóneo para eludir las dificultades que se derivan de la protección de la persona frente a la utilización informática; así, entre las posibles dificultades cita a la problemática en torno al rango de la ley que desarrolle este derecho, el acceso al amparo ordinario y al constitucional reconocidos en el artículo 53.2 de la Constitución española.[84]

329.4. Ahora bien, si uno aplica esta idea también puede tomar una dirección errada, pues la defensa constitucional emergente del artículo 43 quedaría circunscripta al campo de los archivos personales o familiares eludiendo la amplitud que antes le dispensamos.

De todos modos, la libertad para disponer sobre los datos personales sería una especie dentro de la generosa tutela judicial prometida a los derechos derivados de vida privada (intimidad y privacidad).

La construcción de este nuevo derecho fundamental excede la tradición jurídica que tuvo el derecho a la intimidad, permitiendo que toda información que concierna a cualquier persona pueda ser controlada por él mismo como un freno al poder informático.

> Hoy nadie duda que la vida privada de la persona es un bien que debe respetarse, porque el ataque a la misma es susceptible de causar un daño irreparable a la persona en una sociedad como la actual cuyo único límite al almacenamiento y tratamiento de datos personales es el que procede de la imaginación humana. Información relativa al ocio, a los comercios o a la educación de los hijos, así como a las actividades profesionales no son inocuas en nuestro desarrollo personal y en la honorabilidad o imagen que se ofrece al exterior, por lo que oportunamente entrelazadas y almacenadas "dicen" mucho de cada individuo, y de su personalidad; inmiscuirse en ellas, para conocerlas y tratarlas sin consentimiento representa un peligro del que debe ser consciente si se quiere una sociedad

[84] RUIZ MIGUEL, ob. cit., pp. 77 y ss.

> libre y en igualdad de oportunidades. Sentir que constantemente se está siendo observado, seguro de que la totalidad de las acciones serán "registradas" impide el derecho a manifestarse en una sociedad con libertad y dificulta el libre desarrollo de la personalidad. Habida cuenta de los nuevos peligros y amenazas que el tratamiento informático trae consigo, se sugiere una conceptuación del derecho a la autodeterminación informativa a través de una extensión de su protección frente al uso ilícito o abusivo de la informática a cualquier información personal que represente una amenaza para la persona en "manos de terceros"; la interceptación no consentida de la información, debe controlarse y limitarse sin detenerse a averiguar la índole íntima o no de la información.[85]

329.5. En pocas palabras, el derecho a la libre disposición de los datos personales supone recrear un derecho fundamental que, derivado del derecho a la vida privada del hombre, le permite resolver por sí mismo el tratamiento que quiera asignar a los datos que sobre su persona se almacenen con destinos diferentes. La garantía específica para salvaguardar el derecho es el proceso constitucional de *habeas data*.

De este modo se responde a la especificidad que contiene la promesa constitucional, ampliando las fronteras de la intimidad, el honor y la propia imagen, para ocupar espacios mucho más ambiciosos que los recortados en leyes y constituciones.

Una vez más transcribimos la opinión de Herrán Ortiz, quien concreta el alcance del derecho en estos términos:

> Si la protección de datos personales no ha podido enmarcarse en los instrumentos de tutela propios del derecho al honor o a la propia imagen por la limitación conceptual y garantista que implican tales derechos, tampoco el derecho a la intimidad resulta de utilidad para explicar y fundamentar el fenómeno de la autodeterminación informativa. Desde la consideración de un sistema de resarcimiento o meramente indemnizatorio no sería deseable ni posible jurídicamente estructurar el sistema de protección de datos, porque, en ese caso, la protección de la persona se vería limitada a medidas de naturaleza represiva, con lo que un aspecto fundamental de la protección de los datos personales, cual es el carácter preventivo o precautorio, carecería de total relevancia jurídica. El sistema jurídico que se acoge desde el derecho a la intimidad no responde a unos criterios fundamentales de precaución sino que deben identificarse con un sistema puramente indemnizatorio para la víctima del agravio. Como fácilmente puede comprenderse, con este esquema parece especialmente complicada la configuración jurídica de la protección de los datos personales desde la perspectiva del derecho a la intimidad; al afectado, titular de los datos, se le atribuyen en las leyes de protección de datos personales derechos y facultades individuales que sólo pueden contemplarse desde la óptica de un derecho principalmente preventivo que dota al individuo de garantías suficientes para evitar y controlar la utilización abusiva o ilícita de la información personal registrada en soportes informáticos.[86]

329.6. El resumen de derechos que tutela el *habeas data* muestra que el punto de mira no es sólo impedir intromisiones ilegítimas en la esfera privada, sino evitar

---

[85] *Cfr.* HERRÁN ORTIZ, cit., p. 105.

[86] HERRÁN ORTIZ, ob. cit., p. 255.

que los datos obtenidos sean utilizados o transferidos sin el resguardo y control que pueda tener la persona; de este modo se elimina —al menos parcialmente— el llamado "rumor informático" y se instala una valla a las empresas que hacen de las bases de datos su fuente de comercialización.

> Inclusive, afirma Panuccio, se impone una doble vertiente de responsabilidad al titular del banco de datos: diligencia en el mantenimiento de la calidad del contenido de la misma, en términos de veracidad, licitud y caducidad, y la obligación de responder por las consecuencias lesivas que su negligencia, en términos de responsabilidad objetiva, pueda ocasionar el afectado.[87]

Precisamente, como la figura no tiene antecedentes en nuestra legislación (Argentina), más allá de las actuaciones logradas en materia civil respecto a la tutela de la intimidad; o en el derecho penal en aras de la defensa del honor y la confianza, lo cierto es que el *habeas data* tiene un perfil acotado que se resuelve desde la pretensión del afectado. Es un derecho individual que, partiendo desde el derecho a la intimidad y con posadas en la privacidad, la identidad o la dignidad de la persona fragmenta su unidad como proceso para aplicar su garantía a otras cuestiones como la tranquilidad espiritual, el derecho al aislamiento, la protección del nombre civil o comercial, la integridad física, el secreto profesional, etc.

Esta es una primera visión del derecho fundamental creado por el artículo 43 de la Constitución Nacional argentina. La promesa de protección a la intimidad es amplia, sin embargo, no procede si el acto lesivo (la afectación, propiamente dicha) no proviene de un tratamiento informático o manual de nuestros datos compilados en una base, archivo o registro.

329.7. Por ello, la garantía antes que una herramienta procesal, es un derecho disponible por el individuo que encuentra de esta forma una vía de acceso a información que le concierne, e inmediatamente, la potestad de resolver, por sí mismo —con algunas pocas limitaciones— si quiere que esos datos se transmitan a otros, se conserven bajo reserva o confidencialidad, o se supriman por afectar la sensibilidad de la persona. Este conjunto de atributos suele nominarse como "derecho de autodeterminación informativa".

> Se hace notar que el derecho a la autodeterminación informativa se construye tomando como fundamento el concepto de intimidad o vida privada; puesto que trata de ofrecer tutela a la persona respecto a sus datos de carácter personal una posible utilización abusiva de los mismos mediante la informática u otro tratamiento automatizado. Ahora bien, que nadie se confunda —dice Herrán Ortiz—, mediante el derecho a la autodeterminación informativa no se salvaguardan tan solo los datos que se denominan sensibles, sino también aquellos que sin pertenecer a la esfera más próxima al individuo, son susceptibles de daños su imagen o el ejercicio plano de sus derechos. Más aún, ni tan siquiera los considerados como datos sensibles representan siempre información íntima o secreta de la persona, el origen racial o determinadas enfermedades son tan evidentes y reconocibles

[87] PANUCCIO, Vittorio, *Banche de dati e diritti della persona,* CEDAM, Milan, 1985, p. 3.

externamente que de ellas poco permanece reservado en la intimidad del individuo y, sin embargo, no puede dudarse de su carácter sensible como informaciones personales.[88]

329.8. La subjetividad natural que impera en esta potestad de control sobre la base de datos caracteriza, entonces, al derecho emergente como:

a) Un derecho individual, previsto para atacar las intromisiones en la intimidad concretadas con un fin específico (en el caso, compilar las acciones para registrarlas en un archivo).

b) Un derecho de acceso irrestricto, a excepción de fuentes de información que puedan mantener su secreto por razones de seguridad justificadas (*v. gr.:* datos policiales; registros fiscales; etc.).

c) Un derecho de requerir la verdad del registro (principio de exactitud y actualidad del dato archivado), o de promover su rectificación o supresión.

d) Un derecho de exigencia por el cual se pretende que el titular de la base de datos utilice la información compilada con la finalidad concreta para la que fue autorizado el archivo.

A su vez, el proceso garantista, si bien sujeto al principio dispositivo (n*e proceda iure ex officio; nemo iudex sine actore*), por sí mismo constituye un sistema cautelar o preventivo, que no requiere de reglamentación para obrar en tal sentido, dentro del marco de posibilidades que el derecho otorga (amparo, conocimiento, rectificación o cancelación).

La ley española parte de un "derecho a la autodeterminación informática" que se inspira en el principio de que ha de ser el sujeto quien decida qué datos pueden ser almacenados, por quién y para qué fines, lo cual comporta una capacidad de decisión que descansa en una información previa o en el requerimiento inicial de su consentimiento para recabar, tratar o ceder los datos sensibles a él referentes. Estamos pues ante el "*habeas data*" en virtud del cual la persona tiene la facultad de controlar la información que le concierne y que se encuentra recogida en el fichero automatizado; le asegura una esfera de libre decisión con respecto a una categoría de datos sobre los cuales el ordenamiento le confiere la facultad de prestar su consentimiento para ser objeto de tratamiento automatizado.

330. El derecho a la dignidad personal

330.1. La voz "dignidad", dice el *Diccionario de la Real Academia Española*, cuando se usa de una manera absoluta, indica siempre buen concepto y se utiliza en contraposición a indigno.

También es la gravedad y decoro de las personas en la manera de comportarse. De algún modo, la dignidad, en los términos como se presenta, puede englobar los supuestos de defensa al honor, la imagen y reputación que antes desarrollamos. Sin embargo, es algo más.

Miguel A. Ekmekdjian, pionero entre los autores argentinos que desarrollan el "derecho a la dignidad de las personas", afirma que el fundamento del *habeas data* es otorgar una

[88] HERRÁN ORTIZ, ob cit., pp. 246 y ss.

> garantía especial al derecho a la intimidad. Agregando que el derecho a la privacidad o a la intimidad es una consecuencia o derivación del derecho a la dignidad.[89]

Ese "plus" proviene de su propia generalización. Es un concepto jurídico que identifica varios presupuestos, pero donde se destacan especialmente dos: de un lado, la posibilidad efectiva de encontrar una respuesta positiva dentro del ordenamiento legal para defender los derechos de la intimidad, que es de carácter personalísimo; y por otro, la configuración en los correlativos términos de reserva de una esfera de acción humana y de la consiguiente capacidad de generación de una privacidad protegida mediante el correspondiente poder de exclusión.

> En cuanto al bien jurídico protegido —sostiene Martínez Sospedra— la doctrina más aceptada subraya que el mismo consiste cuasi exclusivamente en la libertad de disposición sobre el ámbito de lo íntimo, dimanante de la propia dignidad [...]. La diferenciación entre asuntos privados y asuntos públicos, entre vida privada y vida pública, constituye una estructura cultural sin cuya preexistencia y hegemonía social, poco menos que absoluta, es impensable el mismo régimen de Estado, y en todo caso, sin la cual es impensable la concepción moderna de la libertad en términos de autodeterminación personal y del consiguiente poder legal de exigir a los demás, incluidos los poderes públicos, las conductas necesarias para asegurar su subsistencia y reproducción. En consecuencia es predicable de la vida privada, y de la intimidad con mayor motivo al ser ésta el eje o centro de aquella, la doctrina del papel institucional de las libertades que la amparan.[90]

330.2. Si tomamos la dignidad como género desde el cual proyectar los contenidos que ocupa el *habeas data*, se consigue vulnerar el reducto de los presupuestos que lo condicionan al solo control de datos afectados por el uso inapropiado.

En efecto, la idea se ocupa de los casos de acopio informativo sobre las personas, con el fin de evitar inexactitudes en la transmisión de esos datos, o que el archivo donde los contiene sea una fuente de discriminación para los individuos. Este sería el campo del proceso constitucional. Sin embargo, si la dignidad se aplica como marco de referencia que permite ampliar el objeto y las pretensiones, toma sentido y fundamento la sentencia de la Corte Suprema de Justicia de la Nación Argentina en el "caso *Urteaga*".

Recordemos algunos párrafos de esta sentencia. Inicialmente se sostuvo que:

> la ausencia de normas regulatorias de los aspectos instrumentales de la acción de *habeas data* no es óbice para su ejercicio, incumbiendo a los órganos jurisdiccionales determinar provisoriamente —hasta tanto el Congreso Nacional proceda a su reglamentación—, las características con que tal derecho habrá de desarrollarse en los casos concretos. El voto del ministro Bossert, ejemplifica la generalidad del caso y la apertura que se consigue desde esta visión. Dijo: "Los derechos de los hombres que nacen de su propia naturaleza, no pueden ser enumerados de manera precisa. No obstante dicha deficiencia de la letra

---

[89] EKMEKDJIAN, Miguel Ángel, "El *habeas data* en la reforma constitucional", en Rev. *La Ley*, 1995-E, 946 y ss.

[90] MARTÍNEZ SOSPEDRA, ob. cit., p. 237.

> de la ley, ellos forman el derecho natural de los individuos y de las sociedades, porqué fluyen de la razón del género humano, del objeto mismo de la reunión de los hombres en una comunión política y del fin que cada individuo tiene derecho a alcanzar.[91]

Surge así una primera proyección en el llamado "derecho a la verdad" antes referida. De igual modo aparecen los derechos a la reserva y confidencialidad, que no deben asociarse a la idea del secreto absoluto de la persona o de la inabordable posibilidad de conocer aspectos de su intimidad.

330.3. En los hechos, la dignidad no supone que cuanto menos se conozca de uno, y cuanto más se conserve en secreto, permite reservar la intimidad en su mejor hábitat. En realidad, lo perseguido no es ocultar la información relativa a una persona, sino que ésta pueda desarrollar su vida con libertad y posibilidades de resolver, por sí mismo, que aspectos de su vida admite poner en exposición y conocimiento de los demás.

> Ya se ha indicado —dice Herrán Ortiz— que no es mayor el ámbito de intimidad cuanto menos se conozca de la vida personal y familiar, que la intimidad no se debe vincular directamente con la reserva u ocultamiento de la información relativa a la persona, sino con el libre desarrollo interior de una vida individual que faculta a la persona a conocerse y realizarse intelectual y psicológicamente. Es por ello, que aunque los demás penetren en la vida privada ajena conociendo aspectos del mundo interior, a ellos sólo acceden a través de lo que la persona les facilita, pero además, les será imposible acceder al "mundo interior", integrado por los más valiosos sentimientos, pensamientos y recuerdos de la persona, en los que cada individuo se recrea y proyecta como ser humano. En resumen, la intimidad constituye un bien personal al que, en modo alguno, puede renunciar sin resentirse en su dignidad humana.[92]

Por eso intimidad y privacidad no son términos contrapuestos, sino manifestaciones de la vida. Una que se conserva "hacia adentro" y reposa en los deseos, los sentimientos, las inclinaciones, los miedos, etc.; y otra que ocurre en el diario vivir, el hombre "hacia afuera", con sus relaciones, sus compromisos, su imagen y formación de una personalidad social que, de alguna manera, se debe distanciar de la personalidad familiar. No porque sean diferentes, sino porque la privacidad es distinta.

En suma, todo queda enmarcado por la dignidad. Una vida digna tiene un aspecto ético y moral que hace a una filosofía personal de la conducta; y también una proyección necesaria de los límites que deben imponerse a los demás para evitar agresiones innecesarias a los derechos de la personalidad.

---

[91] Fallos, 309:1762.

[92] HERRÁN ORTIZ, ob. cit., p. 288.

Sección 3ª La protección de datos de personas jurídicas o ideales

331. El régimen legal

331.1. Una de las dificultades más importantes que encuentra la determinación de los bienes jurídicos que tutela el *habeas data* está en saber si la garantía se puede extender a las personas jurídicas, a cuyo fin nos detendremos para su análisis en el estudio del sujeto activo del proceso.

El esclarecimiento es necesario ante la asimetría que tiene el régimen legal; mientras Europa considera que los datos personales son derechos humanos de las personas físicas, la mayoría de los reglamentos latinoamericanos involucra a las empresas (personas jurídicas o ideales).

Si la base del razonamiento se asienta en la defensa de la intimidad parece imposible encontrar este derecho en las personas jurídicas, pues no hay intimidad propiamente dicha, como sí un derecho al secreto, a la discreción, o bien a la reserva de la vida privada que bien puede tener una empresa, entidad, asociación o cualquiera otra forma de personalidad ideal.

En consecuencia, la personalización del derecho, propio de la consagración del subjetivismo jurídico, no se podría extender a quienes no tienen individualidad física, pensando que la dimensión jurídica de la persona no alcanza para atribuirle un derecho al honor, a la vida privada y, en menor medida, a la imagen.

La causa de la limitación se sostiene en el carácter de derecho humano que tiene la intimidad, condición que no poseen las personas ideales; y además, en la exigencia de tutelar un interés propio, directo y exclusivo como es la vida privada de las personas, que no son naturales en los grupos que, por su propia calidad, viven en permanente relación pública.

> El objeto del derecho radica en la intimidad, como algo que es al tiempo diferente tanto de la vida privada, como de la privacidad, como de la vida pública. Siendo como es el de intimidad un concepto jurídico indeterminado la cuestión radica en trazar siquiera sea aproximadamente sus perfiles, diferenciarle de los conceptos afines y establecer directrices para su concretización. De esta forma sostiene Martínez Sospedra que, la diferenciación entre privacidad, vida privada e intimidad dista de ser clara, al menos por lo que a los dos últimos conceptos afecta. Si la *privacy* anglosajona se corresponde parcialmente con el derecho que estudiamos, pero también con otros derechos del art. 18 CE sustantivizados por el constituyente español, como pone de relieve el antecitado informe Cutter,

> lo que facilita la diferenciación, es preciso reconocer que trazar el perfil de la intimidad es harto complicado, razón por la cual ha podido señalarse que el concepto mismo de intimidad es una mala herramienta de trabajo, es un cesto para recoger agua.[93]

331.2. Si el planteo anterior se realiza desde otra perspectiva, las respuestas podrían cambiar. En efecto, la afirmación que precede sostiene que la intimidad es un derecho personalísimo, y los datos —como una parte de ella— que se encuentran contenidos en archivos afectan de manera directa a la persona física cuando se revelan o almacenan en condiciones ilegítimas o desautorizadas por su titular.

Otra visión encuentra que la intimidad no se la vincula estrictamente con la vida privada y sí con un derecho de exclusión y reserva, desde el cual se puede construir un derecho propio para las personas jurídicas. En lugar de proteger la intimidad en sí misma, se defiende la intimidad de quien la reclama, abriendo panorámicamente los objetos y razones de la pretensión.

> Determinada persona jurídica podría interponer la acción de *habeas data*, frente a los registros o bancos de datos de un organismo oficial o privado, si considera que estos datos podrían afectar su honor comercial (*v. gr.:* figurar como deudor de un crédito, cuando ya se ha cancelado la deuda) o su intimidad (*v. gr.:* datos que revelan la donación de fondos a algún partido político o credo religioso). A estos ejemplos de Ekmekdjian y Pizzolo, los autores agregan: "Si en situaciones iguales se les concede tal facultad a las personas físicas, ¿porqué discriminar a las jurídicas cuando las consecuencias no se discriminan? En otras palabras, si los individuos pueden ejercer un derecho de acceso a los bancos de datos personales almacenados en una entidad ¿por qué no podrían hacerlo las personas jurídicas?".[94]

La cuestión no es pacífica si la intimidad se adquiere como derecho absoluto, pero cambia sustancialmente si la interpretación se asume confrontando la realidad del diario acontecer.

331.3. Es evidente que el criterio tradicional como se interpreta a la intimidad deja fuera de las posibilidades de reclamo a los entes ideales, por ejemplo, para el derecho al secreto de las conductas sexuales, la vida familiar, las creencias religiosas, las inclinaciones políticas, o en suma, los datos sensibles *lato sensu*. En cambio, si la visión se focaliza en los datos, exclusivamente, evidentemente la protección diferida por el *habeas data* no se puede restar de las garantías que tienen las personas jurídicas.

Son varias las razones por las que se argumenta la protección de los datos aunque puedan variar los motivos. Con ello se quiere decir que no es igual la protección del honor de la persona física que la reputación de la persona jurídica; que es distinta la imagen individual respecto a la corporativa; que difiere la dignidad individual de

---

[93] MARTÍNEZ SOSPEDRA, *Sobre la intimidad. Derecho a la intimidad, vida privada y* privacy. *El art. 18 CE* in principio *en la jurisprudencia del Tribunal Constitucional,* en *Sobre la intimidad,* cit., p. 59.

[94] EKMEKDJIAN, Miguél Ángel, PIZZOLO, Calógero, *Habeas Data. El derecho a la intimidad frente a la revolución informática*, Depalma, Buenos Aires, 1996, p. 22.

aquella que privilegia el objeto social; y así, sucesivamente, podrán aparecer diferencias por la naturaleza de las personas, pero que a la par de los derechos encuentran simetrías posibles.

El caso del honor es una probabilidad a tener en cuenta. Este puede ser atacado por la divulgación de actos, hechos, noticias, etc., relativas a personas tanto físicas como sociales; y cuando el prestigio o la confianza de una sociedad se pone en duda a consecuencia de la revelación de datos, es indudable que ese conocimiento que los demás asumen sobre la persona ideal afecta su activo patrimonial.

> Ahora bien, dice Herrero Tejedor, distinto es el caso de las instituciones sin fines de lucro, sino de participación, opinión o defensa de ideas o creencias. Nos referimos, por ejemplo, a los partidos políticos, sindicatos, asociaciones, confesiones religiosas, fundaciones, etc. En ellas se hace indispensable la posesión de una honorabilidad clara, pues su desprestigio haría muy difícil la obtención de sus fines sociales. Por ello, el autor acepta la idea de extender la protección de datos personales hacia las personas jurídicas.[95]

331.4. De todos modos podemos coincidir con aquellos que sostienen que las empresas tienen un derecho de identidad (marca o registro), un nombre que las identifica; un prestigio que proteger, o una trayectoria que conservar. Por todo eso, el archivo que reúne información debe ser cierto y confiable, circunstancias que permitirían defender el derecho a una propia identidad.

La conclusión no significa afirmar que el *habeas data* sea el remedio procesal preciso para lograr la protección que se persigue, pues aunque sea lógico que las entidades jurídicas puedan disfrutar de un derecho de acceso o de corrección sobre la información que le concierne; también es cierto que el derecho constitucional que se garantiza es un valor para el hombre y sus libertades, mientras que el mundo de los negocios se presenta dando preferencia a valores económicos; y el honor y la imagen, entre otros derechos, tienen en este aspecto un tinte crematístico innegable.

> ¿Poseen las personas jurídicas el mismo derecho a la intimidad que las físicas? Se interroga Estadella Yuste. En su parecer es difícil negar que las personas jurídicas carezcan de un derecho general de conducir sus actividades en secreto, o de evitar que cierta información confidencial pase a manos de la competencia o del público en general. No obstante, la necesidad de proteger ciertos secretos empresariales o la confidencialidad de información comercial no implica que se pueda atribuir a las entidades jurídicas un derecho individual a la intimidad, ya que el significado de éstos términos no es el mismo. En mi opinión —agrega—, la conveniencia legal que se haya podido encontrar en atribuir a las entidades jurídicas una "personalidad", no implica que éstas sean humanas y que tengan que disfrutar de los mismos derechos que los individuos. Parece ser más apropiado atribuirles derechos y obligaciones propios de la actividad que desempeñan y relacionarlos con aquellas ramas del derecho encargadas de regular tales actividades, en lugar de fundamentar sus Derechos en instrumentos legales que no han sido diseñados para personas jurídicas.[96]

---

[95] HERRERO TEJEDOR, *Honor, intimidad y propia imagen,* cit., p. 59.

[96] ESTADELLA YUSTE, ob. cit., pp. 116 y ss.

331.5. La ley de privacidad (*Privacy act*) de Estados Unidos (1974) define el término *individuo* asignando el derecho de referencia al ciudadano de los Estados Unidos, sea natural o extranjero con residencia permanente legalmente admitida. Pero cuando se refiere a *datos de carácter personal* significa cualquier información relativa a una persona física o jurídica identificada o identificable.

A diferencia de Europa que legisla solo para las personas físicas. Por ejemplo, la ley francesa 78/17 del 6 de enero de 1978 relativa a la informática, archivos y los derechos emergentes, sostiene que la protección a dispensar es para cada ciudadano "[…] su desarrollo debe desenvolverse en el marco de la cooperación internacional. No debe afectar la identidad humana ni los derechos humanos, ni la vida privada, ni las libertades individuales o públicas".

Siempre la relación se relaciona con derechos de las personas físicas, por eso dice el art. 2° que:

> Ninguna decisión judicial, que implicara apreciación en cuanto al 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.

Igual alcance y medida tiene España con la Ley Orgánica de Protección de Datos vigente que protege sólo a las personas físicas (las llamadas personas de carne y hueso); habiéndose dicho que:

> […] las personas jurídicas (corporaciones, sociedades, asociaciones, fundaciones, cooperativas) no merecen tal protección porque los datos de las personas jurídicas son públicos; y ello no impide que ellas personas puedan encontrar una protección de sus datos personales en ámbitos concretos como en el Código Penal (en el delito de descubrimiento y relevación de secretos mediante el acceso y cesión inconsentido de datos de la empresa o la revelación de secretos) o en la normativa de protección de las comunicaciones electrónicas. En nuestra opinión —dice Plaza Penadés— la exclusión de las personas jurídicas, con carácter general, del ámbito de la protección de datos de carácter personal, parte de una concepción equivocada en la que se cree que todos los datos de las empresas y demás personas jurídicas son públicos y en el que se desconoce tanto la existencia de datos que las empresas y personas jurídicas quieren mantener en secreto, de forma reservada y bajo su control, así como que el daño derivado del tratamiento erróneo de los datos es el mismo en las personas físicas que en las jurídicas y que, en consecuencia, deberían de gozar de los mismos derechos de acceso, rectificación y cancelación de los datos, por lo que de cara a futuras modificaciones legales sobre la materia se sugiere una reforma en este sentido.[97]

331.6. Además, en el continente europeo se creó en el año 2001 un consejo de vigilancia en la materia, de conformidad con el artículo 286 del Tratado de la

---

[97] PLAZA PENADÉS, Javier, *Protección de datos de las personas jurídicas,* publicado el 28 de enero de 2009, en www.legaltoday.com

Comunidad Europea, que había dispuesto que a partir del 1º de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de los datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente tratado o sobre la base del mismo.

Esta es en si la filosofía y el eje central del concepto: el máximo respeto a los datos personales y su consiguiente protección y cuidado en orden a incorporarlos en las mencionadas instituciones comunitarias. Como garantía y refuerzo, el párrafo segundo del mismo artículo 286 dice:

> El Consejo establecerá […] un organismo de vigilancia independiente responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la comunidad y adoptará en su caso cualesquiera otras disposiciones pertinentes.

La consideración, entonces, de los datos personales como derechos de las personas físicas es un principio que la Unión Europea respeta y continúa. Nada se dice, por el momento, en lo atinente a una eventual protección de las personas jurídicas; tal vez, se ha querido seguir con la línea llevada a cabo por los países del entorno sociocultural europeo, por lo que preguntarse por la atención hacia las personas jurídicas, nos llevaría a los mismos debates que se venían estableciendo para el caso español o similares. Lo que sí queda claro es que es un órgano de vigilancia estricta sobre un derecho fundamental como es el de la protección de los datos; ahora bien, no actúa siempre solo; sino que mantiene en muchas ocasiones una estrecha colaboración con el *Defensor del Pueblo Europeo*, materializándose dicho vínculo en el Memorándum de Acuerdo (2007/ C 27/07), cuyas líneas generales podrían resumirse en: *a)* La información que el reclamante tiene derecho a obtener, debido a la solicitud que previamente ha presentado; *b)* la celeridad a la hora de actuar, evitando en todo momento, la duplicidad de procedimientos y consecuentemente permitiendo la obtención de una resolución mas rápida; *c)* llevar a cabo la ejecución de todo lo establecido anteriormente.[98]

> Existe un documento de gran importancia que es la Decisión del Parlamento Europeo, del Consejo y de la Comisión y de la Comisión relativa al estatuto y a las condiciones generales de ejercicio de las funciones del Supervisor Europeo de Protección de Datos; en éste hay 12 consideraciones y 5 artículos, de los que surge:
>
> *A.* La protección de las libertades y los derechos fundamentales de las personas físicas en lo relativo al tratamiento de los datos personales.
>
> *B.* La necesidad de establecer un estatuto.
>
> *C.* La necesidad de actuar siempre conforme las directrices del derecho comunitario.
>
> *D.* La determinación del salario del Supervisor Europeo y Supervisor Adjunto, equiparándose las asignaciones y cantidades retributivas del primero a las del Defensor del Pueblo y las de éste a su vez se asimilan a las de un juez del Tribunal de Justicia y en el caso del Supervisor Adjunto su equivalencia en materia de salario corresponde a la del

[98] MACÍA TORRES, Pedro Jesús, *La figura del supervisor europeo de protección de datos,* Revista Informática Jurídica, 2007, Sevilla, pp. 23 y ss.

Secretario del Tribunal de Justicia de las Comunidades Europeas, estableciéndose una jerarquía en referencia al Supervisor Europeo.

E. La sede del Supervisor Europeo de Protección de Datos está en Bruselas con el fin de hacer más próximas y estrechas las relaciones entre las diversas instituciones comunitarias.

F. Celebración de audiencia abierta a todos los diputados al Parlamento, de los candidatos que figuren en una lista que anteriormente ha sido elaborada por la Comisión. El Supervisor Europeo y el Supervisor Adjunto serán nombrados finalmente tras una convocatoria pública de candidaturas.[99]

331.7. El Tribunal Constitucional español, en la sentencia 64/1988, en el marco de un análisis general de la "capacidad de derechos fundamentales", afirmó que:

> [...] por lo que se refiere al derecho establecido en el art. 24.1 de la Constitución, como derecho a la prestación de actividad jurisdiccional de los órganos del Poder Judicial del Estado, ha de considerarse que tal derecho corresponde a las personas físicas y a las personas jurídicas, y entre estas últimas, tanto a las de Derecho privado como a las de Derecho público, en la medida en que la prestación de la tutela efectiva de los jueces y tribunales tiene por objeto los derechos e intereses legítimos que les corresponden. Sin embargo, por lo que concierne a este último derecho, se ha dicho que no se puede efectuar una íntegra traslación a las personas jurídicas de Derecho público de las doctrinas jurisprudenciales elaboradas en desarrollo del citado derecho fundamental en contemplación directa de derechos fundamentales de los ciudadanos.
>
> Por ello, hay que entender que, en línea de principio, la titularidad del derecho que establece el art. 24 de la Constitución corresponde a todas las personas físicas y a las personas jurídicas a quienes el ordenamiento reconoce capacidad para ser parte en un proceso y sujeta a la potestad jurisdiccional de Jueces y Tribunales, si bien en este último caso el reconocimiento del derecho fundamental debe entenderse dirigido a reclamar del órgano jurisdiccional la prestación a que como parte procesal se tenga derecho.

En la sentencia 197/1988, tras reiterar dicha doctrina, precisó diciendo que:

> [...] cuando los órganos públicos no actúan como decisores de conflictos de intereses, ni ostentan un interés propio que se oponga al de otro ente público implicado en la decisión, sino que ejercen funciones de control de la legalidad, la decisión de estos órganos públicos, garantes de la legalidad de los actos de otros órganos igualmente públicos, no compromete, ni incide en el interés legítimo de estos últimos», por lo que la falta de un recurso jurisdiccional no menoscaba, en tales supuestos, el derecho a la tutela judicial.

En consecuencia, si, cuando de entes públicos se trata, el art. 24.1 de la Constitución, en su vertiente de derecho de acceso a la jurisdicción no puede aplicarse sin las modulaciones a que acaba de hacerse referencia, es obvio que otro tanto cabrá decir si se examina su contenido desde la perspectiva del derecho a una resolución de fondo. En efecto, en la STC 257/1988 se denegó el amparo pretendido por una Diputación Foral y fundado en la presunta vulneración del art. 14 de la Constitución, precisando que la legitimación para interponer el recurso de amparo

---

[99] MACÍA TORRES, ver nota anterior.

requiere que "quien aparezca como demandante se halle en una específica relación con el objeto de las pretensiones que pueden deducirse en esta vía, ya consista tal relación en la titularidad propia de un derecho o libertad fundamental presuntamente vulnerado o, incluso, en un mero interés legítimo en la preservación de derechos o libertades, igualmente fundamentales, de otros".

Señalaron entonces que el recurso de amparo "no constituye una vía abierta a los poderes públicos para la defensa de sus actos y de las potestades en que éstos se basan, sino, justamente, un instrumento para la correcta limitación de tales potestades y para la eventual depuración de aquellos actos, en defensa de los derechos fundamentales y libertades públicas de los particulares"; criterio que plenamente se aplica en materia de defensa de datos en su relación subjetiva.

332. La situación en América Latina

332.1. La ley Argentina de Protección de Datos Personales nº 25.326 tomó como fuente la norma española de 1982, solo que no la siguió en la tutela exclusiva que aquello dispuso. La generosa inclusión de las personas jurídicas no fue obstáculo para que la Unión Europea certificara la legislación acordando que contaba con "*un nivel adecuado de protección*" (Decisión 2003/490/CE del 30 de junio de 2003).

Solamente Chile y Paraguay se suman al elenco de países con legislación adecuada, recordando que en ambos, se tutela también a las personas jurídicas.

332.2. Cuando se incorpora a las personas ideales en el conjunto de sujetos alcanzados por las leyes de protección de datos personales, el inconveniente se manifiesta con los preceptos sustanciales que tuitivamente quedan en la dimensión de los derechos de protección equivalente.

Por ejemplo, la Ley uruguaya 18.331 del 11 de agosto de 2008, estableció que el derecho a la protección de los datos personales es inherente a la personalidad humana y por lo tanto está comprendido en el artículo 72 de la Constitución Nacional; por ende, ese derecho, es propio de las personas físicas (respecto de sus datos personales contenidos "*a través de cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo*") y por extensión, también de "*las personas jurídicas, en cuanto corresponda*" (según lo establece el artículo 2º de la ley y el artículo 1º de su Decreto Reglamentario Nº 414/009 de 31 de agosto de 2009).

Pero cuánto es "lo que corresponda". Tomemos el caso del derecho al *honor* que no se puede mancillar con el uso inapropiado de los datos personales. Una persona física que cumple regularmente con sus obligaciones puede quedar afectada en su buena reputación, si la información comercial que se proporciona es inexacta y lo comunica como deudor del sistema financiero.

Es evidente que el caso trata sobre un derecho derivado de la dignidad humana, que consiste en no ser escarnecido o humillado ante uno mismo o ante los demás. El honor interno estaría representado por la estimación que cada persona tiene de sí misma, mientras que el honor externo estaría integrado por el reconocimiento que los demás hacen de nuestra dignidad.

> Tal diferencia podría considerar que la dimensión interna resultaría del todo subjetiva al apelar a las apreciaciones de cada persona que se vea afectada en tal derecho. Las consecuencias serían, al propio tiempo, absurdas, pues atendiendo a tal dimensión, encontraríamos personas que tienen un nivel de autoestima mayor que otras, con lo que la dimensión interna del honor resultaría hasta discriminatoria. Otro tanto habría que decir de la dimensión externa del honor, pues sujeta a las apreciaciones colectivas, sociológicas o culturales diversas, el honor de las personas resultaría del todo incontrolable jurídicamente y el derecho se vería así sometido a un suerte de escrutinio social que podría desvirtuar su nivel de garantía.[100]

No obstante, este tipo de concepto para el honor quizás no sea muy apropiado al quedar acotado al margen de las apreciaciones subjetivas; teniendo en cuenta que, actualmente, no se trata de estimular o propiciar un concepto de honor que defienda ni un sentimiento de casta o de sangre, como pareciera ser el origen en la historia de tal derecho, ni tampoco de caer en la subjetividad de una concepción del honor perceptible por uno mismo o por los demás integrantes de un grupo social. Si bien no puede negarse que el concepto o las concepciones sobre el honor están íntimamente vinculadas a la cultura, las creencias y convicciones de un tiempo y un lugar determinados, también es verdad que el Estado Constitucional, al objetivar un modelo de organización social y político, establece unos parámetros mínimos donde el operador jurídico debe tratar de construir un concepto de honor que, partiendo de la dignidad humana, sea compatible también con los valores como la igualdad, la libertad y los demás valores sobre los que se asienta el modelo político del Estado constitucional y democrático.

En este contexto, y para decirlo en términos sencillos, el honor está constituido por aquella esfera de inmunidad frente a cualquier trato que ofenda o agrede la condición de la persona humana en su relación con los demás o en su relación con los poderes públicos. El derecho al honor protege, entonces, la intangibilidad de la dignidad en la dinámica social de un tiempo determinado.

Como ha sostenido el Tribunal Constitucional español:

> [...] El contenido del derecho al honor, que la Constitución garantiza como derecho fundamental (...) es, sin duda, dependiente de las normas, valores e ideas sociales vigentes en cada momento. Tal dependencia se manifiesta tanto con relación a su contenido más estricto, protegidos por regla general con normas penales, como a su ámbito más extenso, cuya protección es de naturaleza meramente civil. Por otra parte, es un derecho respecto al cual las circunstancias concretas en que se producen los hechos y las ideas dominantes que la sociedad tiene sobre la valoración de aquél son especialmente significativas para determinar si se ha producido o no lesión (STC 185/1989, FJ, 4).

332.3. En este contexto, una persona individual vería severamente comprometida sus relaciones sociales si el honor fuera atacado con información carente de verdad, ya sea por ofensas directas (injurias) o por imputaciones carentes de asidero,

---

[100] Sentencia del Tribunal Constitucional del Perú, 2006/08/29, expediente 04099/2005

o incluso cuando estas fueran ciertas y son propaladas con el solo ánimo de agredir la condición de persona y su indesligable condición de ser social por naturaleza.

De este modo, un dato caduco; una información inexacta; un perfil inapropiado; una valoración subjetiva sin parámetros serios de confirmación, son estándares de violación al honor; pero no son posibles de espejar cuando se trata de referir al honor de una persona jurídica o ideal.

En todo caso, la "buena reputación" de la empresa podría ser la fuente de un honor asimilado al grupo de derechos que con la autodeterminación informativa se pretende. También la entidad ideal forma parte de un grupo social y se relaciona cotidianamente con sus semejantes; de allí que se diga que

> […] mientras que la dimensión del honor individual se refiere a un derecho personalísimo indelegable, en su dimensión de buena reputación, el honor se expande como una posición *iusfundamental* que puede también ampliar sus efectos para proteger posiciones similares no solo de personas naturales, sino incluso en los entes que, amparados en alguna manifestación de personalidad jurídica que les confiere el sistema jurídico, actúan en la sociedad proyectando una imagen o un nombre o una "razón social".[101]
>
> El honor no es pues ni "interno" ni "externo", como ha sugerido cierta doctrina para expresar las formas en que puede ser padecida su agresión, frente a uno mismo o frente a los demás. Se mancilla el honor cuando se humilla y se degrada en la condición de ser humano a una persona lanzándole ofensas o agrediéndola directamente o haciéndolo ante el público y de cualquier forma. La diferencia es, en todo caso, que en el segundo supuesto, en el caso de la agresión a la reputación social, el honor está comprometido doblemente, como una ofensa hacia uno mismo, y como un desprestigio frente a los demás, desmereciendo la condición de ser social por excelencia que es toda persona. El honor corresponde, así, a toda persona por el solo hecho de serlo y se manifiesta, sobre la base del principio de igualdad, contrario a las concepciones aristocráticas, plutocráticas o meritocráticas. La valoración diferente del honor que alguien pretenda fundar en el linaje, la posición social y económica o incluso en los méritos, resulta irrelevante en el marco de la concepción pluralista del Estado Social y Democrático de Derecho y desde la función que cumplen los derechos fundamentales. Si bien es verdad que, desde una perspectiva de la responsabilidad civil, pueden identificarse particularidades para establecer los montos de reparación en función de determinadas características personales, profesionales o circunstanciales inclusive, ello no debe llevarnos necesariamente a vislumbrar una distinta calificación del honor de las personas individuales desde la perspectiva de sus derechos fundamentales. El derecho al honor, tal como lo configura la Constitución, corresponde a todos por igual y ha de tener, por consiguiente, un contenido general compatible con los demás principios y valores que la propia Constitución también reconoce y da objetividad.

332.4. A partir de aquí, ¿es posible afirmar la titularidad del derecho fundamental al honor por parte de las personas jurídicas? Ciertamente, si se lo considera desde una perspectiva subjetiva es difícil, por no decir imposible, predicar que un ente tenga una dimensión moral en polémica con la ética empresarial. Ahora bien, entendido el honor en sentido objetivo, esto es, considerado el honor en sentido de

---

[101] *Cfr*. Sentencia del Tribunal Constitucional del Perú, expediente C 905-2001-AA/TC.

buena reputación, buena fama, ¿es posible extenderlo también a las personas jurídicas? En el ámbito de sociedades tan complejas como las actuales, en las que los individuos, conscientes de sus limitaciones y en ejercicio del libre desarrollo de sus personalidad, pone en común sus intereses con otros individuos con vistas a la consecución de determinados fines, no parece posible defender que el derecho al honor en tanto que consideración social sea un interés exclusivamente individual.

Como con acierto ha puesto de manifiesto Carrillo,[102] en un modelo social y político como el actual el derecho a la reputación incide sobre ámbitos que superan el reducto individual de la persona para incidir también sobre grupos sociales de naturaleza heterogénea, que son también sensibles a la consideración que el entorno social tenga de ellos y fundamentalmente de la actividad que realizan y de la coherencia de sus presupuestos fundacionales con la práctica cotidiana.

El derecho fundamental al honor no es, entonces, patrimonio único de las personas físicas, sino que habida cuenta de su significado, ni puede ni debe excluir de su ámbito de protección a las personas jurídicas.[103]

332.5. Queda en claro, pues, que el ámbito de protección que reciben las personas morales son idénticas a las que tienen los sujetos individuales. Los derechos de acceso y control, en América Latina, no tienen resignaciones cuando la pretensión se presenta por una persona jurídica que acredite el uso inadecuado de la información que le concierne.

---

[102] CARRILLO, Marc, "Libertad de expresión, personas jurídicas y derecho al honor", en *Derecho Privado y Constitución*, nº 10 (1996), p. 91

[103] VIDAL MARÍN, Tomás, "Derecho al honor, persona jurídica y Tribunal Constitucional", *Indret*, Revista para el análisis del derecho, Barcelona, 2007, pp. 397 y ss.

Sección 4ª ⋮ La información y los datos

333. Derecho a la información. Conflictos entre derechos

333.1. La previsión amplia del derecho a la intimidad y la vida privada, el marco del derecho a la dignidad personal, y la relación como derecho personalísimo que pueden tener también las personas jurídicas (solo en Latinoamérica, no así en Europa que considera que los datos de las personas ideales son públicos, y por tanto, tienen otras vías de protección) termina concretando el derecho a la autodeterminación informativa, cuyo preocupación central asienta en el uso racional de los datos personales que se compilan en archivos y registros, informáticos o no, y cualquiera sea su carácter (públicos y privados).

> Es clásica la expresión utilizada por Perez Luño al referir a una "libertad informática" que asegura, por un lado, la identidad de las personas ante el riesgo de que sea invadida o expropiada por determinados usos (más bien abusos) de las nuevas tecnologías. Para ello pone en manos de las personas los instrumentos procesales pertinentes para ejercer su derecho a acceder y controlar las informaciones que les conciernen y, por el otro, contribuye a conformar un orden político basado en la equilibrada participación cívica y colectiva en los procesos de información y comunicación que definen el ejercicio del orden en las sociedades informatizadas de nuestra época.[104]

333.2. Si bien el tema se presenta como evolución, en algunas legislaciones el programa puede ser alternativo, y hasta en franca contradicción. Por ejemplo, cuando un país decide proteger el derecho a la intimidad con leyes de fondo o en el Código Civil, el ámbito de circunscribe a los derechos a la personalidad, que protegen el contorno privado de una persona. Son derechos subjetivos donde anidan el honor, la intimidad y la propia imagen.

Pero también, cuando se ingresa a la Constitución la tutela de datos personales, aparece el derecho a la autodeterminación informativa con el objetivo de otorgar al afectado un derecho de control y de oposición al uso indebido de la información que le concierne.

Es evidente, entonces, que una persona que sabe o toma conocimiento de la utilización de sus datos personales, puede sentir que la información transmitida

---

[104] Pérez Luño, Antonio Enrique, "Los derechos humanos en la sociedad tecnológica", en *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, pp. 1989 y ss.

afecta su honor (*v. gr.:* se comunican aspectos de su personalidad que quiere mantener ocultos o en confidencia); o la intimidad (*v. gr.:* cuando se revela información sensible); o se altera su reputación con datos inexactos (*v. gr.:* solvencia patrimonial o cumplimiento de obligaciones); en estos casos, la doble vía de legislación podría trazar senderos paralelos y permitir que en uno se resuelva el derecho de uso que tiene el titular o responsable de la base de datos, y por otro, se ataque el error informativo, la invasión informática y el derecho a una reparación indemnizatoria.

333.3. El derecho a la intimidad pretende que una persona pueda controlar el acceso y la divulgación de información sobre su vida privada. La legitimidad de las intromisiones depende fundamentalmente del consentimiento del titular. Si hay consentimiento del titular no hay violación del derecho a la intimidad; y lo mismo sucede con los datos personales, aunque en estos casos, la aceptación puede ser revocada en cualquier momento. Aquí no es importante la exactitud de la información, porque el derecho a la intimidad se vulnera por la simple imputación de un hecho que forma parte de la esfera íntima y más personal de un ser humano.

> La ley española contempla tres (3) casos: *a) Obtención de la información*. Si no hay consentimiento. Colocación de aparatos de escuchar, de filmación, de dispositivos ópticos o cualquier otro medio para grabar o reproducir la vida íntima de las personas; *b) Divulgación de la información*. Dar a conocer hechos de la vida privada de una persona o revelar el contenido de cartas, memorias, etc. u otros escritos personales de carácter íntimo. *c) Quebramiento de la confianza*. Revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela. Se trata de una desviación de la información del fin para el que se ha dado. Ejemplo: asistentas de casas de los famosos. Además de estos casos que prevé la ley orgánica 1/82, el Tribunal Constitucional también ha introducido otras intromisiones ilegítimas, como registros o indagaciones corporales.

En consecuencia, los objetivos pueden ser distintos, pero en ambos casos se trata de atender el control que tiene la persona concernida (afectada) sobre los datos personales que le pertenecen.

333.4. Otra particularidad del conflicto surge entre la eventual contradicción entre el *derecho de acceso a la información pública;* el *derecho a la información,* y el ejercicio del proceso constitucional de *habeas data*, como herramienta de protección de los datos personales.

En efecto, el derecho a la información surge como prerrogativa fundamental en 1948, en la Declaración Universal de los Derechos Humanos; pero tardó mucho tiempo hasta que los Estados reconocieran el derecho dentro de sus legislaciones. Fue aún más tardía la admisión constitucional.

El derecho a la información en su sentido *lato* supone, en primer lugar, el derecho a informar —fórmula moderna de la libertad de expresión— y en segundo lugar, el derecho a ser informado, el cual se refiere fundamentalmente al público, a la colectividad, siendo también un aspecto que supone también el deber de informar a cargo de los gobernantes. A partir del derecho a la libertad de expresión —donde

todo individuo tiene el derecho a la libertad de opinión y expresión, y comprende el derecho a no ser molestado, el de investigar y recibir informaciones y opiniones, sin limitación de fronteras, por cualquier medio de expresión— se va a construir el contenido del derecho a la información.

Este último derecho se convirtió en un elemento indispensable para que el ciudadano tomara parte activa en las tareas públicas, es decir, se entiende a la información como participación y toma de decisiones. Ello es así, puesto que la información es requisito e impulso para que el hombre, individualmente, adopte decisiones políticas que adquieran un valor comunitario.

Lo anterior vendrá a reformular las libertades tradicionales de expresión e imprenta con la firme intención de adaptarlas a la situación actual, constituyendo, así, el moderno contenido (reciente) del derecho a la información.[105]

333.5. Del contexto histórico donde nace y se desarrolla el derecho a la información, se puede constatar que, a veces, fue la respuesta que consiguieron las minorías políticas para ser escuchadas, y ese sentido de protección social al más débil terminó por aquilatar la tutela más allá de las fronteras del individualismo.

Por eso una de las primeras manifestaciones la ocupa el derecho a expresar ideas por la prensa, como una manifestación propia del derecho a informar y ser informado; de lo que se desprende que, frente al acto concreto de una autoridad, debe establecerse la relación con el gobernado y si este acto arbitrario vulnera directamente el derecho de informar o el de estar informado, se estará ante a un derecho fundamental —derecho a la libertad de información— y si se requiere de la implementación de una serie de medidas a través de la legislación ordinaria, se estará frente a uno de carácter *social* —derecho de acceso a la información pública.[106]

333.6. Ahora bien, tratar de identificar el derecho a la información con el derecho de acceso a la información pública, no es cosa sencilla, porque las normas sobre transparencia del accionar público puede acordar que es una prerrogativa que atañe al control sobre los poderes y el gobierno; pero no es igual al sentido de ser informado, puesto que la información pública consiste en el registro, archivo de cualquier dato que se encuentre recopilado, se mantenga, procese o se este en posesión de las entidades públicas; mientras que el derecho a la información constituye la facultad —atraerse información, a informar y a ser informado— para poder acceder a dichos registros en manos de la administración pública.

Es por ello que con el vocablo "derecho de acceso a la información pública" no se agota la discusión en torno al derecho a la información, sin embargo, constituye un excelente punto de partida en el reconocimiento de otros derechos fundamentales.[107]

---

[105] GARCÍA GONZÁLEZ, Aristeo, "La protección de datos personales dentro del ámbito judicial de México. Una visión estatal". *Revista de Derecho Informático*, nº 110 (2006), diciembre, versión on line.

[106] GARCÍA GONZÁLEZ, Aristeo, "La protección de datos personales dentro del ámbito judicial de México. Una visión estatal", *Revista de Derecho Informático*, nº 110 (2006), diciembre, versión on line.

[107] GARCÍA GONZÁLEZ, Aristeo, "La protección de datos personales dentro del ámbito judicial de México. Una visión estatal", *Revista de Derecho Informático*, nº 110 (2006), diciembre, versión on line.

333.7. Así como derecho de acceso a la información, establece sus parámetros de alcance y protección, lo mismo debe acontecer en lo que respecta a aquellos datos que son objeto de un tratamiento informatizado, es decir que mediante la utilización de técnicas informáticas y tecnológicas modernas se hace posible agrupar y tratar en forma conjunta datos de las personas que se encuentran dispersos y que puede construir un perfil de ella misma.

Datos personales que en un principio constituyen una información concerniente solo a la persona, sin embargo, cuando estos datos son conocidos por otra persona o una entidad pública, esto se convierte en información confidencial, o bien, en objeto de reserva que a su vez debe ser garantiza por mecanismos idóneos de protección [...]

Así, los datos dispersos de una persona, no dicen nada de ella, sin embargo, cuando estos son tratados de manera conjunta pueden arrojar un perfil determinado de la persona objeto de un interés público, siendo controlados y conocidos por ella misma, pero en otras, puede vulnerar al individuo en unos de sus derechos fundamentales, como lo es *la protección de sus datos personales*. Esto es, mientras que, para el derecho de acceso a la información el principio fundamental lo constituye la publicidad, en cambio, para *la protección de sus datos personales* lo será el consentimiento a la hora de recabar datos, tratarlos o comunicarlos a terceros.

Es por ello, que para establecer un equilibrio con otros derechos fundamentales, se debe tener presente que tipo de información personal se muestra sensible, por lo que en materia de datos personales el principio de consentimiento se encuentra vinculado con el principio básico de la información.

En este contexto, es donde cada persona debe conocer en todo momento, quien tratará sus datos personales, para qué finalidad, si se podrá ceder o permitir el acceso a terceros, y los casos en que la información debe ser objeto de publicidad. Para ello, todo tratamiento de datos personales debe encontrarse sujeto a obligaciones específicas de seguridad y confidencialidad, dando por resultado el que cualquier persona no sea identificada o identificable por virtud de los mismos, y que por ende, no se vea vulnerada en su ámbito personal.

Consecuentemente, en el ámbito normativo el concepto de datos personales alude a "la información concerniente a una persona física, identificada o identificable".[108]

333.8. La libertad de información trasciende el quid que, en su tiempo, produjo la libertad de expresión. Mientras ésta pretende resolver el problema de la intervención de los poderes públicos en materia de censura o prohibición previas, la libertad informativa tiene que afrontar una dimensión muy diferente a la de otrora, si se tiene en cuenta el alcance inusitado de los medios de comunicación y la mentada globalidad que ella alcanza.

John Stuart Mill dijo que:

> la necesidad de libertad de opinión y de libertad de expresión se sostenía en cuatro fundamentos. Primero, una opinión reducida al silencio puede ser verdad. Negarlo es asumir nuestra infalibilidad. En segundo lugar, aunque la opinión censurada sea un error, puede contener algo de cierto. Tercero, aun en el caso de que la opinión general sea no sólo

[108] GARCÍA GONZÁLEZ, Aristeo, "La protección de datos personales dentro del ámbito judicial de México. Una visión estatal", *Revista de Derecho Informático*, nº 110 (2006), diciembre, versión on line.

> verdadera, sino toda la verdad, se tendrá como una suerte de prejuicio con escasa comprensión de sus fundamentos racionales a menos que sea contestada de manera seria y enérgica. Y cuarto, de convertirse en un dogma, se traduciría en un obstáculo e impediría el desenvolvimiento de otras convicciones.[109]

Mientras en origen la libertad de manifestarse (expresar ideas y reunirse sin obstáculos ni impedimentos de orden legal) era un expreso reconocimiento a una sociedad libre; actualmente la libertad admitida no se puede interpretar sin límites.

Es evidente que hay múltiples maneras de colegir el concepto, tantas como existen formas de pensar y actuar la comunicación humana. De la expresión deriva el conocimiento, la inteligencia, la sensibilidad ante los valores humanos, y en definitiva, la capacidad para emitir un juicio objetivo. Estas son referencias lógicas y algunos las utilizan como pautas para afirmar la imposibilidad de establecer limitaciones.

Sin embargo, en la búsqueda de información aparece una etapa previa de reunión de datos, noticias, investigación, entre otras actividades que pueden comprometer la vida privada de las personas.

333.9. Por ejemplo, si en la compilación de antecedentes es preciso buscar en archivos o registros los conocimientos logrados se obtienen conociendo datos que hipotéticamente son reservados o confidenciales.

> Podría definirse como "fuente periodística" —dicen Pierini, Lorences y Tornabene—, al sólo efecto de presentar la cuestión y sin ánimo de ser plenamente abarcativos de todas las hipótesis, toda noticia, informe, comentario, trascendido, rumor, etc., y toda actuación de informantes —voluntarios o involuntarios— que sirva para obtener la información. Se trata de la etapa previa a la publicación, y comprende la información recibida y la investigación. Entendida como tal, está expresamente prevista en el artículo 43 de la Constitución Nacional y es allí donde se produce la controversia sobre la preeminencia de un derecho sobre otro.[110]

Comienza así el conflicto entre preferencias. ¿Qué es más importante? ¿Proteger la libertad de información o la libertad de intimidad? ¿Acaso es posible establecer jerarquías? Inclusive, hasta se podría establecer una diferencia entre Europa y América sobre la forma de entender este fenómeno y optar por uno de ellos o compatibilizarlos.

Tocqueville comparó el periodismo europeo con el americano indicando una severa distancia en el estilo de practicarlo. Uno respetaba la libertad de las personas en el sentido individual que ello supone; el otro también lo respetaba pero desde la generalidad de sus conductas y el interés que ellas tienen hacia los demás. Uno reserva la información, el otro la divulga.[111]

---

[109] MILL, John S., *On liberty,* Cambridge, 1989, p. 17.

[110] PIERINI, Alicia, LORENCES, Valentín, TORNABENE, María Inés, *Habeas Data,* Universidad, Buenos Aires, 1998, p. 38

[111] TOCQUEVILLE, Alexis de, *La democracia en América*, Sarpe, Madrid, 1984, p. 38.

El espíritu del periodista, en América, es el de atacar groseramente, sin ambages ni arte, las pasiones de aquellos a quienes se dirige; el de dejar a un lado los principios y hacer prensa en el hombre; el de seguir a éste en su vida privada y poner al desnudo sus flaquezas y sus vicios.

De esta forma, afirma Aznar Gómez, los medios de comunicación servirían para conjurar el peligro de una sociedad individualista, donde cada uno en su retiro privado ignoraría el destino común y compartido de lo público.[112]

Una distinción demasiada efímera, elástica, absolutamente discrecional y peligrosa para la seguridad jurídica y la certidumbre que requieren las conductas humanas. Por ello es preciso hurgar en la vida privada para saber —o reconocer— aquello que es intangible y que, aun invocando libertades fundamentales, no pueden socavarse por la dignidad que exige la persona humana.

339.10. En este sentido, la intimidad individual y familiar, la honra, la propia imagen, la reputación son valores que la prensa no puede comprometer amparada por la libertad de expresión y opinión.

Esto, reflejado en la dimensión del *habeas data*, supone que los datos conocidos de fuentes informativas registradas en soportes manuales o informáticos, no pueden publicarse o darse a conocer, sin caer en responsabilidad por esa actitud imprudente.

> Conviene recordar la diferencia que existe entre invasión de la intimidad y publicación de información sobre la vida íntima o privada. Y ello, porqué a diferencia de otras faltas legales y morales cometidas en el ámbito de la información, en el caso de la intimidad su violación constituye de por sí un daño. Por ejemplo, en lo relativo al honor o la verdad se requiere, necesariamente, la publicación de la información para que exista la falta. Los rumores que en gran cantidad circulan día a día en las redacciones de los periódicos no constituyen faltas si no se difunden o editan. Sin embargo, ocurre algo muy distinto en el caso de la intimidad: aquí la persona experimenta ya un daño moral al sufrir la violación de su privacidad, al sentirse desprotegida o invadida su intimidad. Por consiguiente —concluye Aznar— las exigencias éticas y legales de respeto a la intimidad comienzan en el mismo momento de la obtención de la información.[113]

Aun así, uno se podría interrogar si aspectos de la intimidad como la fama o reputación constituyen violaciones cuando la revelación por la prensa pone al descubierto actitudes simuladas o apariencias solo mantenidas para cubrir verdades que no son tales.

Para Espinar Vicente:

> en principio, todo pensamiento, afecto o asunto de un individuo que tenga un carácter antijurídico o que sirva para la construcción de su fama social puede y debe ser conocido más allá del ámbito que el sujeto pretende mantener reservado para sí mismo o su fami-

---

[112] AZNAR GÓMEZ, Hugo, "Intimidad e información en la sociedad contemporánea", en *Sobre la intimidad*, Fundación Universitaria San Pablo C.E.U., Valencia, 1996, pp. 55 y ss.

[113] AZNAR, ob. cit., p. 58.

> lia. De lo contrario, el derecho a la intimidad personal y familiar se convertiría en un instrumento al servicio de una doble moral de costumbres, poco compatible con la idea prefacial de establecer una sociedad democrática avanzada, amén de operar como un factor susceptible de extraer ciertas actitudes y conductas de la esfera de ordenación del Derecho.[114]

339.11. La primacía de la información sobre la intimidad pareciera inmediata, aunque para reafirmarlo es necesario establecer otros criterios que no sean tan abiertos como el caso mencionado. En efecto, la intimidad tiene un plano de vida privada y familiar que permite la realización de la persona sin interferencias ni intromisiones. Este es un punto sin discusión.

La averiguación de datos sobre una persona puede constituir una actividad lícita cuando la forma de practicarlo no se inmiscuye con artilugios en la vida privada, o a través de maniobras que eluden el consentimiento necesario para lograr la información.

Por eso es inviolable el domicilio, son secretas las comunicaciones y la correspondencia, y se impiden las escuchas de conversaciones realizadas por medios técnicos invasivos (intervención en líneas telefónicas; irrupción en los correos electrónicos; grabación de conversaciones, etc.).

339.12. Igualmente existen datos que por su sensibilidad con la persona no se pueden registrar (y, de serlo, deben tener el consentimiento del afectado) ni divulgar (vinculados con la ideología, el credo, las preferencias íntimas, las inclinaciones de conducta, enfermedades, etc.). Por otra parte, en el derecho a la información la necesidad de expresar la verdad y conocer la verdad son aspectos esenciales para ella y un límite preciso para su justificación. Informar lo que no es cierto transforma la difusión en una calumnia.

En cambio, uno puede expresar ideas o pensamientos a través de la prensa sin involucrar a terceros, ejerciendo un legítimo derecho que no refiere a la información. Por eso, la libertad de expresión es más amplia que la libertad de información.

> A los medios de comunicación no se les puede dar carta blanca —sostiene Concepción Rodríguez—, dejando a los particulares sin protección. La prensa (en un sentido amplio) tiene una función social y política que cumplir y en la mayoría de los casos es perfectamente cumplimentada a través del ejercicio responsable de la función periodística… La importante función que desempeñan los medios de comunicación y periodistas conlleva no sólo el reconocimiento de derechos y garantías del ejercicio libre de la profesión, sino también ciertas obligaciones consistentes en suministrar una información de calidad, evitando abusos y violencias morales. De ahí que los propios periodistas, los ciudadanos y los poderes públicos estén interesados en dotar a los profesionales de una organización y una regulación de su actividad informadora.[115]

---

[114] ESPINAR VICENTE, José María, "La primacía del derecho a la información sobre la intimidad y el honor", en *Estudios sobre el derecho a la intimidad*, Tecnos, Madrid, 1992, p. 177.

[115] CONCEPCIÓN RODRÍGUEZ, ob. cit., p. 88.

339.13. Simplificando la presentación (porqué el tema merece un tratamiento mucho más amplio que lo acotado de estas referencias) entre la libertad de expresión y el derecho a la intimidad existe un conflicto que sólo se puede resolver con prudencia y adecuación a los tiempos y las personas.

Cuando los individuos tienen una exposición al público casi permanente (políticos, artistas, etc.) la inmiscusión en sus reductos privados suele consentirse más que en supuestos de personas comunes, o de menor trascendencia social.

339.14. Sin embargo, existen algunas reglas que no pueden olvidarse:

a) Sólo la defensa del interés público justifica las intromisiones o indagaciones sobre la vida privada de una persona sin su previo consentimiento.

b) En el tratamiento informativo de los asuntos en que medien elementos de dolor o aflicción en las personas afectadas, el periodista evitará la intromisión gratuita y las especulaciones innecesarias sobre sus sentimientos y circunstancias.

c) Las restricciones sobre invasiones en la intimidad deberán observarse con especial cuidado cuando se trate de personas ingresadas en centros hospitalarios o en instituciones similares.

d) El periodista deberá evitar nombrar en sus informaciones a los familiares y amigos de personas acusadas o condenadas por un delito, salvo que su mención resulte necesaria para que la información sea completa y equitativa.

e) Se evitará nombrar a las víctimas de un delito, así como la publicación de material que pueda contribuir a su identificación, actuando con especial diligencia cuando se trate de delitos contra la libertad sexual.

f) Los criterios indicados en los dos principios anteriores, se aplicarán con extremo rigor cuando la información pueda afectar a menores de edad. En particular, el periodista deberá abstenerse de entrevistar, fotografiar o grabar a los menores de edad sobre temas relacionados con actividades delictivas o enmarcables en el ámbito de la privacidad.

g) El periodista, asimismo, deberá evitar la publicación de datos (sobre la raza, color, religión, origen social o sexo de una persona, o cualquier enfermedad o minusvalía física o mental que padezca), salvo que guarden relación directa con la información publicada.

> Las consideraciones expuestas —según son explicadas por Aznar Gómez— corresponden al Código Deontológico de la Federación de Asociaciones de Prensa de España, y reflejan una situación tan variable y circunstancial como es la relación entre información e intimidad. Igualmente, manifiestan la imposibilidad última de dar una respuesta definitiva, sin conocer cada caso en concreto. Hay pues un margen siempre abierto para la reflexión del propio profesional. Los medios, como entorno habitual de trabajo donde se dan estas situaciones, deben hacer lo posible por proveer los medios y mecanismos para que los profesionales puedan ejercer dicha reflexión y llevar a cabo un aprendizaje moral tan valioso o más que el puramente técnico.[116]

---

[116] AZNAR, ob. cit., pp. 59 y ss.

En suma, simplificado el tema en relación con la amenaza o violación a la vida privada y otros derechos de la personalidad, el problema es más profundo pues afecta y va a dañar más en el futuro a la libertad y a la igualdad, pues resulta evidente que al ser vulnerada la vida privada o la privacidad, en su caso, el equilibrio se rompe y se establece una relación de dominio y control de quien posee la información sobre la persona a quien desnuda; y en consecuencia todo dominio personal restringe la libertad e impone desigualdad entre quien posee información y quien no tiene acceso a ella.

334. El control sobre los datos personales

334.1. Frente a la probable dificultad para evitar el origen de la base de datos se ha previsto la participación del involucrado permitiendo que sea éste quien defina la calidad del registro que le concierne.

Este control le posibilita corregir el dato equívoco o inexacto; suprimir la información incorrecta y, aun resolver la transmisión del mismo. Claro está que para ello, existe un derecho natural al acceso a la información que debe preferirse en la dispensa de tutela con el fin de evitar la evasión del mencionado derecho al control sobre la base de datos.

La potestad que referimos suele nominarse como "*autodeterminación informativa*", en el sentido de dispensar al hombre un derecho de administrar la información personal que le atañe propiciando que controle los datos registrados y, en su caso, resuelva cuáles son aquéllos que admite su transmisión a terceros.

En síntesis, es una garantía básica de la persona decidir por sí misma cuándo y dentro de qué límites procede revelar situaciones referentes a su propia vida.

Sostenía el Tribunal Constitucional Alemán en el año 1983 que:

> la libertad informática ya no es la libertad de negar información sobre los hechos privados o datos personales, pretensión que hoy no podría encontrar adecuada tutela en muchos casos, sino la libertad de controlar el uso de los propios datos personales insertos en un programa informático. Es el *habeas data* correspondiente al antiguo *habeas corpus* del respeto debido a la integridad y libertad de la persona…Por tanto, derecho de acceso a los bancos de datos, derechos de control sobre su exactitud, derecho de puesta al día y de rectificación, derecho de secreto para los datos ´sensibles´, derecho de autorización para su difusión, todo este conjunto es lo que hoy constituye el *´right to privacy´*.
>
> La Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983, que declaró inconstitucionales algunos artículos de la Ley del Censo de la República Federal Alemana, ha marcado un hito en la defensa de los derechos de la persona a preservar su vida privada.
>
> El recurso contra dicha Ley fue interpuesto por simpatizantes del movimiento de "los verdes", quienes obtuvieron una resolución cautelar del Tribunal Constitucional el 13 de abril de 1983, por la que se suspendió la entrada en vigor de la Ley del Censo y posteriormente la decisión definitiva sobre el fondo del recurso. En esta sentencia el Tribunal Constitucional germano señala que la proliferación de centros de datos ha permitido, gracias a los avances tecnológicos producir "una imagen total y pormenorizada

de la persona respectiva —un perfil de la personalidad—, incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en "hombre de cristal". El Tribunal Federal ha sido rotundo en su decisión de que la persona posee un derecho de libre decisión y libre disposición sobre sus datos personales y que puede decidir qué es lo que otros pueden saber sobre él.

La sentencia del tribunal Constitucional alemán señala que las limitaciones a este derecho a la autodeterminación informática sólo son admisibles en el marco de un interés general superior y suscitan un fundamento legal basado en la Constitución. El legislador, en su regulación, debe observar el principio de proporcionalidad y tiene que adoptar, asimismo, precauciones de índole organizativa y de derecho procesal susceptible de contrarrestar el peligro de vulneración del derecho a la salvaguardia de la personalidad.

Se declara lícita la recogida de gran parte de los datos del censo referidos a nombre, apellidos, dirección, estado, nacionalidad, utilización de la vivienda, fuente de los medios principales de subsistencia, datos académicos y profesionales, rama de actividad.

Declara ilícitos, entre otros, los preceptos relativos al cotejo de datos para ser utilizados contra las personas obligadas a suministrar esa información.

Hay que tener presente que, muchas veces, los datos de carácter personal recogidos hoy empleados con fines demográficos y científicos, sufren desviaciones de la finalidad para la que fueron recabados. Estos datos, pese a su carácter anodino, suelen ser los más apetecidos pues facilitan verdaderos perfiles de las personas y son, por otra parte, los que mayor peligro de desprotección suponen.

Lo que en definitiva ha sucedido es que el derecho a la intimidad ha pasado de ser un status negativo de la persona a convertirse en un status positivo, activo. De una actitud pasiva de simple defensa de nuestra intimidad, delimitadora de un ámbito de no interferencia, hemos pasado a una postura activa con la posibilidad de ejercer el control sobre el caudal de información que puede existir en los diferentes bandos de datos sobre nuestra persona.[117]

334.2. La posibilidad que se concede tiene dos facetas a cubrir. De un lado el mecanismo que cada país resuelva adoptar en orden al cumplimiento de principios y garantías de mínima, necesarios para definir un esquema procesal para la protección de datos personales; y en segundo lugar, quizás lo más importante, precisar qué se entiende por datos personales y bajo que condiciones son éstos protegidos.

En el primer aspecto es bueno recordar el impacto que trae para Europa el "Convenio 108", cuyo art. 4.1 le facilita a cada uno a decidir, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos".

La adopción de leyes fue consecuencia inmediata a diferencia de América que las origina dentro de sus Constituciones. Y la distinción no es baladí en la medida que confrontadas las situaciones se observa que hay textos continentales (de Europa y América) que son inconciliables, pese a la fuente que uno admite del otro.

Por el caso, España, apoyo normativo de muchas leyes americanas, se ha valido del derecho a la intimidad, en sentido amplio, para bosquejar los derechos funda-

[117] CUERVO, José, "Autodeterminación informativa", *Revista Informática Jurídica*, versión on line

mentales que el Convenio le marcó; sin embargo, cuando dicta la primera Ley Orgánica de Tratamiento de Datos Personales (la famosa Lortad, 1/1982) solo se dirige a tutelar una serie de derechos de la personalidad, sin atender el centro neurálgico de la cuestión como era y es la defensa del derecho a la intimidad por el uso de la informática).

En cambio en América, los principios englobados en la "calidad de los datos" y el control sucedáneo sobre ellos, ha mitigado el problema de la invasión informática, pero ha dispersado la figura procesal, al punto que el *habeas data* procede en situaciones diferentes. Algunos solo lo admiten cuando los datos que se vulneran están destinados a proporcionar información a terceros; otros, cuando son afectados por archivos públicos; algunos más incluyen a los bancos de datos privados pero excluyen a los de información crediticia y/o solvencia patrimonial; en fin este es el cuadro que después veremos *in extenso*, debiendo en más, centrarnos en el punto siguiente.

> Lucas Murillo ha expuesto los rasgos principales del Convenio, enumerando los siguientes principios: de lealtad (informaciones no recogidas por procedimientos desleales o ilícitos); de exactitud de los datos; finalista (el fin que justifica la creación del banco de datos debe precisarse); de publicidad (a través de un registro público); de acceso individual (posibilidad de rectificación o destrucción); de seguridad (seguridad física y lógica de los datos). Por su lado, Olga Estadella Yuste, afirma que, la labor normativa del Consejo de Europa también se ha desarrollado a través de recomendaciones que abordan sectores necesitados de regulación específica (telecomunicaciones, medicina, etc.). Por tratarse de simples recomendaciones, no son de carácter vinculante. La aproximación sectorial al problema es una necesidad de la legislación europea en esta materia, pues las leyes informáticas del viejo continente son normas de carácter general que necesitan, al ser confrontadas con la realidad social, de una regulación específica adaptada a cada sector concreto.[118] Rasgo distintivo del Convenio es la posible adhesión al mismo de Estados no miembros del Consejo de Europa (art. 23), lo cual no viene sino a reafirmar la vocación internacionalista del Convenio.

335. Significado y alcance de la voz: *datos personales*

335.1. ¿Qué es un dato? La pregunta constituye el punto de partida para reconocer la preocupación constitucional y la pretensión objetiva que trae la garantía creada.

El dato es una referencia. Puede ser descriptivo, indicador, dar una pauta, pero no se vincula a la información mientras el conocimiento no se transmita. Igual sucede con las noticias o las investigaciones.

Afirma Puccinelli que:

> el vocablo "dato" se refiere a un elemento circunscripto y aislado (*v. gr.:* nombre o nacionalidad), que no alcanza a tener el carácter de información, pues para que se transforme

[118] ESTADELLA YUSTE, ob. cit., p. 233.

en ella se requiere la interconexión de esos datos de manera que, vinculados, se conviertan en una referencia concreta (*v. gr.:* nombre y nacionalidad).[119]

La misma voz (dato) es anfibológica: define varias cosas y mantiene incertidumbre. Por lo general muestra una característica parcial que se utiliza como indicio o fuente. El dato tiene referencia en algo o alguien, igual que la información. Sin embargo difieren.

El dato puede ser la representación de hechos, conceptos o instrucciones bajo una forma adaptada a la comunicación, a la interpretación o al tratamiento por seres humanos o máquinas; mientras que "informaciones" son aquellos datos que se toman para referirlos dentro de un contexto dado. Asimismo se interpreta por "sistemas de información", los ordenadores, instalaciones de comunicación y redes de ordenadores y de comunicación, así como los datos e informaciones que permiten conservar, tratar, extraer o transmitir, incluidos los programas, especificaciones y procedimientos destinados a su funcionamiento, utilización y mantenimiento.

335.2. Los datos de alguien son personales y tienen el derecho a la reserva y confidencialidad o a la cobertura mayor de la libertad de intimidad. Por su parte, el derecho a la información es una garantía de las sociedades libres y democráticas, lo cual supone no poner trabas a sus mecanismos de expresión y difusión.

Entre ellos impacta el fenómeno informático que toma los datos como fuentes de información para darles un uso determinado. El ejercicio dinámico del registro para actividades diferentes (*v. gr.:* comercio electrónico —*e-commerce*); la transferencia de datos por medios de comunicación que no reconocen fronteras; la comunicación a través de redes, etc., muestra sin dificultades de qué manera la sociedad convierte en públicas las acciones privadas y, por ello mismo, la necesidad de encontrar un límite natural a esta invasión impensada en la intimidad de las personas.

Hay que diferenciar estos tres conceptos —dice Davara Rodríguez— que, aunque es evidente que tratan distintas cuestiones, tienen una incidencia grande en el momento de analizar cualquier normativa sobre protección de datos. Si entendemos por dato el antecedente o noticia cierta que sirve de punto de partida para la investigación de la verdad y aceptamos que ese dato se encuentra en un documento o soporte —físico o lógico— con la calidad de testimonio, debemos distinguirlo de información, entendiendo por tal la acción de informar o dar noticia de alguna cosa. El dato es difícil que, por sí solo, pueda tener una incidencia grande o grave en la llamada privacidad. Esto es, mientras el dato no resuelva una consulta determinada, no sirva a un fin, no dé respuestas o no oriente la posible solución a un problema, es el antecedente o punto de partida para la investigación de la verdad; pero, en el momento en que ese mismo dato da respuesta a una consulta determinada, o sirve a un fin, o se utiliza para orientar la solución de un problema, se ha convertido en información. En este sentido se expresa el apartado primero de la exposición de motivos de la ley española de protección de datos, indicando que: "…el

[119] PUCCINELLI, Oscar Raúl, *El habeas data en Indoiberoamérica,* en "El amparo constitucional. Perspectivas y modalidades", AAVV, Depalma, Buenos Aires, 1999, pp. 187 y ss.

conocimiento ordenado de esos datos (los de carácter personal) puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor, y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos".[120]

335.3. A veces las leyes son amplias para definir. La 25.326 de *Argentina* (art. 2) entiende por datos toda información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

En *México* la fracción II del artículo 7 de la Ley de Transparencia define como datos personales a la información concerniente a una persona física identificada o identificable, que entre otras características, sea relativa a su origen étnico o racial, a características físicas, morales o emocionales, a la vida afectiva o familiar, el domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales o cualquier otro dato análogo a los anteriores que afecten la intimidad de la persona.

Relevando información, también se afirma que dato personal es cualquier información relativa a una persona concreta.

Lo cierto es que cualquiera sea el concepto, un dato es personal cuando identifica al individuo y lo caracteriza; de este modo, y con esa información, se conocen actividades en la sociedad, tanto públicas como privadas.

335.4. El que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos protegidos son todos aquellos que identifican o permiten, al combinarlos, obtener un perfil individual del que se extraen conclusiones sobre ideología, raza, hábitos o costumbres de tipo sexual, actividades y desenvolvimiento económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituye una amenaza personal.

Se consideran datos personales:

- Nombre y apellidos, fecha de nacimiento,
- Número de teléfono, dirección postal y electrónica
- Datos biométricos (huellas, iris, datos genéticos, imagen, raza, voz, etc.)
- Datos sanitarios (enfermedades, cirugías, intervenciones quirúrgicas, etc.)
- Orientación sexual
- Ideología, creencias religiosas, afiliación sindical, estado civil
- Datos económicos: bancarios, solvencia, compras, consumos (agua, gas, electricidad, teléfono…) suscripciones prensa, etc.
- Datos judiciales (antecedentes penales).

---

[120] DAVARA RODRÍGUEZ, Miguel Ángel, *La protección de datos en Europa*, Universidad Pontificia Comillas, Madrid, 1998, p. 34.

335.4. La breve descripción de relaciones entre información, dato y uso informático, releva de alguna manera, cuál es la actividad que se piensa establecer para los jueces. La idea sugiere interpretar que el *habeas data* tiende a dejar en manos del juez la información referida a una persona contenida en un soporte convencional o mecánico (base o banco de datos), para que pueda ordenar sobre su uso y destino.

En síntesis: *que el juez tenga los registros, o los datos, significa habeas data*.

Luego, la función tuitiva, abarca el control sobre las bases de datos (cumplimiento de principios mínimos para su constitución y funcionamiento); la estimación acerca de cuando un dato debe ser protegido en el sentido de las acciones que el *habeas data* recibe (acceso a los archivos, confidencialidad del dato o rectificación o supresión del mismo); la tarea de supervisar, a pedido de parte interesada, la forma como se recolectan los datos y el tratamiento que a ellos se asigna, donde aparecen otras manifestaciones como la cesión y las responsabilidades emergentes.

336. Particularidades de los datos sensibles

336.1. Dato sensible, según la ley argentina (art. 2º) es el dato personal que revela origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

En esta categoría de datos hay reglas especiales: *a)* ninguna persona puede ser obligada a proporcionar datos sensibles; *b)* 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; *c)* 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; *d)* 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 (art. 7, Ley 25.326).

En el ámbito de la ciudad autónoma de Buenos Aires, como testigo de reglamentos que también asumen la definición, se dice que son datos sensibles los mismos que señala la ley nacional, con el agregado que la protección se concede también a cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de ellos (ley 1845, art. 3º).

Para sumar opiniones asimétricas, Colombia nada dispone sobre el dato sensible, pues en la Ley estatutaria divide entre: a) *dato público*, que es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la norma. De allí que son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas; b) *dato semiprivado*, que es que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no

sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley; y c) el *dato privado*, que por su naturaleza íntima o reservada sólo es relevante para el titular.

> No obstante, la jurisprudencia colombiana ha seguido muy de cerca los principios internacionales sobre la protección de datos personales que han sido incorporados en documentos de la Organización de las Naciones Unidas y la Unión Europea. Desde la primera sentencia (T 414/92) la Corte Constitucional de Colombia estableció que la persona es el titular y propietario del dato personal. Para ella es obligación de los administradores de bancos de datos administrar correctamente y proteger los archivos y bases de datos que contengan información personal o socialmente relevante y no atentar contra los derechos fundamentales de los ciudadanos. Dijo además, de manera general, que "*la función de administrar una base de datos debe fundamentarse en los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad*". Concretamente, ha precisado que los administradores deben: (1) Obtener previamente la autorización de la persona cuyos datos se pretende incluir en la base; (2) Notificar a la persona sobre la inclusión de sus datos en el banco e informarle que va a reportar su información en una base de datos con miras a que el titular pueda desde un comienzo ejercer sus derechos de rectificación y actualización; (3) Actualizar permanente y oficiosamente la información para que ésta sea veraz, completa y no se omitan factores que pueden cambiar el buen nombre de la persona; (4) Eliminar de oficio la información negativa que ha caducado con el paso del tiempo; (5) Indemnizar los perjuicios causados por la falta de diligencia o por posibles fallas en el manejo, tratamiento o administración de datos personales; (6) Garantizar el derecho de acceso, actualización y corrección. Estos derechos implican que el ciudadano tenga "*la posibilidad (...) de saber en forma inmediata y completa, cómo, por qué y dónde aparece cualquier dato relacionado con él"; (...) si la información es errónea o inexacta, el individuo puede solicitar, con derecho a respuesta también inmediata, que la entidad responsable del sistema introduzca en él las pertinentes correcciones, aclaraciones o eliminaciones, a fin de preservar sus derechos fundamentales vulnerados*". Finalmente, la Corte ha precisado que, por regla general, "*no puede recolectarse información sobre datos "sensibles" como, por ejemplo, la orientación sexual de las personas, su filiación política o su credo religioso, cuando ello, directa o indirectamente, pueda conducir a una política de discriminación o marginación*".

336.2. Como se observa el dato sensible se toma de acuerdo con un factor acordado (ideología, raza, privacidad, vida social y cultural, etc.) pero no se define con precisión el significado aunque se otorgue dimensión en la órbita de cada situación a remediar.

Dicho esto para advertir que poco importa saber cuando existe un dato sensible si con él no hay afectaciones directas o indirectas en la persona concernida. Por el caso, un hombre o mujer de raza negra, poco podrían ocultar su origen y, en realidad, sería intrascendente; pero si el dato se asume como un presupuesto para la desigualdad o la discriminación, evidentemente el correctivo es necesario.

De allí que la naturaleza del dato personal sea importante para resolver cuando se puede tomar conocimiento de información individual, y cuando el sujeto puede

ocultar de la pesquisa el aporte de datos que por su propiedad secreta y confidencial quiera mantener oculta.

> En Argentina se releva el caso de una persona de 40 años que siendo portador de HIV por mantener relaciones homosexuales con otro portador del virus., al ingresar a trabajar en una sucursal de Citibank Argentina, donde ganó muchos premios como ejecutivo de cuentas, y logró varios ascensos en poco tiempo, fue despedido de ella, cuando la empresa se enteró que era portador de HIV. Las amenazas y el hostigamiento para que renuncie se sumaron a la denuncia de sostener que al ingresar al trabajo no había informado al departamento de personal sobre sus padecimientos de salud. La demanda se inició por discriminación laboral, y la que fue favorable, dijo que no tenía que informar ni proporcionar información que fuera sensible.

336.3. Los datos sensibles deben ser puestos en el ámbito de la dignidad personal; su información depende del consentimiento expreso del titular, y el orden de preferencia que las leyes le asignen puede variar la categoría donde se los instale.

En líneas generales son de "categoría especial" con un régimen más estricto que el que tienen los demás datos personales.

La clasificación depende de la disponibilidad y de la necesidad de formar archivos personales con datos de dicho carácter especial. La categorización no incide en la definición que comprenda la idea de prohibir la recolección y tratamiento de esta categoría de datos, porqué se trata nada más que observar el énfasis de alguna información sensible sobre otra u otras; por ejemplo, sería más importante proteger el secreto del dato sobre costumbres sexuales antes que el dato revelador de una creencia religiosa; o bien, preferir acentuar la tutela en la información que puede ocasionar discriminación de la persona en lugar de aquélla que se puede ocultar sin mayor relevancia.

En cualquier caso, los datos sensibles pertenecen a una categoría única que atiende esencialmente el derecho a la privacidad personal; son informaciones que afectan la esfera máxima de intimidad y que merecen un tratamiento particular.

> La Directiva 95/46 CEE sobre Protección de datos personales establece en el artículo 8º que los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

336.4. La enumeración de cuáles son puede llevar a un *numerus clausus* peligroso, porqué no es pertinente establecer qué datos deben protegerse de acuerdo con su propia naturaleza o por el carácter secreto o confidencial que tengan, sin observar el ámbito concreto de su aplicación.

> La ley 15/99 del 13 de diciembre, prefiere establecer en España, un listado de datos sensibles a los que se asigna carácter de "especialmente protegidos". Ellos se refieren a la ideología, religión o creencias. Luego, para permitir su uso, el artículo 7 agrega que "sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creen-

> cias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado".

En cambio se prohíbe expresamente la difusión de datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual, que sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

La ley argentina dice que quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual. Esto supone que si un dato considerado neutro o irrelevante, al ser utilizado se convierte en un elemento agresor de la intimidad o privacidad de la persona, ese dato se torna sensible por sus efectos.

> Por razones se seguridad —sostiene Sánchez Bravo— es cierto que debe procederse a la determinación legal de aquellos supuestos subsumibles bajo el ámbito de los datos sensibles. Ahora bien, será necesaria la utilización de cláusulas abiertas o generales, lo suficientemente precisas, en su vaguedad, como para determinar su ámbito de aplicación, pero, lo suficientemente amplias como para permitir la modelación en la conceptuación de los datos de acuerdo a las exigencias que demande el efectivo cumplimiento y garantía de los derechos de los ciudadanos.[121]

336.5. No obstante, es común encontrar clasificaciones de cierta utilidad para la aplicación correctora de una ley de tratamiento de datos personales. Por ejemplo, se consideran *datos ultrasensibles* y absolutamente prohibidos de archivo, registro o almacenamiento en bancos o bases de datos, los que revelen información de las personas sobre ideología, religión o creencias. Asimismo, se toman como *datos especialmente sensibles* los referidos al origen racial, la salud y la vida sexual, los que sólo se podrían colectar y guardar con expresa autorización del titular. Además hay *datos sensibles particulares* que son los que se relacionan con la historia individual de las personas físicas, como los antecedentes penales y contravencionales; los que de acuerdo con la norma sólo pueden ser objeto de tratamiento por las autoridades públicas competentes, aun debiendo considerar el carácter provisional de estos de acuerdo con la prescripción de las penas.

> Las consecuencias del tratamiento ilícito de la información personal se agravan cuando ésta pertenece a alguna de las categorías de los denominados datos «sensibles». Las informaciones sensibles son aquellas que se refieren a cuestiones íntimamente ligadas al núcleo de la personalidad y de la dignidad humana. Por ello, las posibles agresiones a la libertad, a la intimidad, las posibilidades de ser discriminado o cualquier otra contra el

---

[121] SÁNCHEZ BRAVO, Álvaro, "La regulación de los datos sensibles en la Lortad", en *Revista Informática y Derecho*, números 6/7, UNED, Mérida, 1994, p. 77.

ejercicio de los derechos fundamentales de las personas serán más directas y virulentas. La particular naturaleza de estos datos personales, por lo íntimo de las informaciones a las que hacen referencia, así como por lo particularmente graves que pueden ser las consecuencias de su utilización fraudulenta para las personas a las que se refieren, ha propiciado que en todas las regulaciones, tanto nacionales como internacionales, hayan gozado de una especial posición traducida en un reforzamiento de las medidas adoptadas para su garantía y protección. Así, tanto el Convenio número 108 del Consejo de Europa (artículo 6º), como la Directiva 95/46/CE (artículo 8º) establecen la necesidad del reforzamiento de las garantías para el tratamiento de los datos personales que tengan esta particular consideración.

336.6. *Ideología y creencias*

La afinidad con un partido político o la pertenencia a un sector gremial, son datos sensibles porqué se considera de riesgo para la persona denunciar tal situación. Así lo exponen entre sus motivos las legislaciones que, mayoritariamente, los comprenden como datos de protección especial.

En Argentina la sensibilidad de esta información es relativa. En primer lugar porqué los ideales políticos pueden ser manifiestos en los casos de afiliación partidaria (que son bancos de fácil acceso) o sindical (en España para considerar dato sensible se agrega el requisito de la agremiación).

En segundo término, porqué nos parece suficiente la defensa constitucional que parte del artículo 43 de la Constitución Nacional cuando otorga derecho de amparo contra "cualquier forma de discriminación".

Luego, porqué en un estado democrático no se puede pensar con la sospecha incorporada en cada acto, sino todo lo contrario, obrar con lealtad y buena fe, creyendo que la ideología no puede ser motivo de diferencias o de privaciones.

En todo caso, si el dato ideológico es reservado (y permanecer en el banco de datos como confidencial), el deber de mantenerlo en secreto es de la base respectiva antes que de la característica intrínseca del dato.

La Cámara Nacional Electoral de Argentina estableció oportunamente que el dato de afiliación política no puede ser incluido dentro de la categoría de dato sensible, toda vez que el hecho de la afiliación en sí implica un acto voluntario y complejo que se perfecciona con la admisión por parte de la agrupación política partidaria, y que el hecho de que la ley preserve las opiniones políticas dentro del ámbito denominado de los datos sensibles no supone que esa protección deba extenderse a los registros de afiliación político-partidaria, ello debido a que resulta consecuencia de la expresión pública de la voluntad del ciudadano.

Para Marcela Basterra:

[…] el derecho a la autodeterminación informativa implica la posibilidad de decidir qué datos queremos se conozcan en relación a cada uno de nosotros para construir nuestra imagen o nuestro propio perfil. Significa la facultad de una persona de poder decidir la oportunidad y el momento en que está dispuesta a permitir que se difunda una información de carácter personal. La protección legal de los datos sensibles, sin duda, está orientada a que cada persona, titular de un dato, tenga la posibilidad de controlar la ve-

racidad de la información y el uso que de ella se haga. Este derecho forma parte de la vida privada de cada uno y jamás puede ser vulnerado por el Estado ni por los particulares, ponderando ningún otro bien.

La información referida a los datos sensibles tiene especial protección en la ley, dado que la recolección y tratamiento de este tipo de datos sirven para formar *perfiles* y pueden ser en sí mismos discriminatorios. Las ideas u opiniones políticas están comprendidas indudablemente dentro de la esfera de la intimidad personal y, su incorporación a un registro debe considerarse ilegal y arbitraria, además estaría claramente encaminada a elaborar perfiles, actividad vedada por la ley. La primera conclusión es que la idea u opinión política de una persona pertenece a su intimidad de conciencia, y está alojada en una esfera de señorío disponible solamente por el propio titular del ese dato íntimo. Es su intimidad y sólo él puede disponer de la misma.

[…] La esfera de la intimidad se abandona al tomar la decisión de afiliarse, y es allí cuando una "opinión" o "idea política" (privada y protegida por la normativa referente a los datos sensibles) se transforma en un "acto voluntario": el de afiliarse, quedando sometido a esta normativa. Es la persona la que al afiliarse corre "el velo de intimidad" que el Estado tiene el deber de proteger sobre su opinión o idea política. De hecho la calidad de afiliado se adquiere no por una simple expresión de voluntad unilateral sino por la adopción de una resolución al respecto por el órgano partidario competente. Si fuera una cuestión limitada a la esfera íntima no podría estar sujeta a la decisión, necesariamente pública de órganos colegiados de los partidos políticos.

Pertenecer como afiliado a un partido político y en consecuencia figurar en el registro de electores partidarios implica el ejercicio de uno de los derechos políticos que consagra la Constitución Nacional, (art. 37): "Esta Constitución garantiza el pleno ejercicio de los derechos políticos con arreglo al principio de la soberanía popular y de las leyes que se dicten en consecuencia..."; de allí que la exhibición de los padrones de electores partidarios, por los medios reglados en la ley, no revelan un "dato sensible.[122]

No obsta lo dicho para sostener que hay posiciones en contrario que afirman:

[…] que los datos sensibles son aquellos que están esencial, pero no excluyentemente vinculados con la privacidad y, por tanto, poseen una mayor potencialidad discriminatoria, y por tal razón su respeto constituye uno de los principios rectores para la reglamentación de los ficheros computarizados en datos personales (…) la pertenencia a determinado partido político es una información que sin lugar a duda alguna revela directa o indirectamente opiniones políticas.[123]

La diferencia entre los conceptos de afiliación política y opinión política se torna entonces forzosa. Conociendo la afiliación se podría deducir entonces la opinión política. Al respecto, Lena Hjelm-Wallen, ex vice premier sueca y reconocida especialista en temas vinculados al derecho de los ciudadanos a tener acceso a la información pública, sostiene que "Una persona tiene derecho a pertenecer a un partido y dar dinero para ese partido y votar por ese partido, pero eso es algo privado y secreto".

---

[122] BASTERRA, Marcela I., L*a "opinión política" o la "idea política" es un dato sensible. La "afiliación partidaria" no*, La Ley del 4 de mayo de 2005, p. 1.

[123] PUCCINELLI, Oscar Raúl, *La protección de datos personales*, cit., pp. 267 y ss.

Por eso, otros coinciden para afirmar que "la información sensible es aquella cuyo contenido se refiere a cuestiones privadas y cuyo conocimiento general puede ser generador de perjuicio o discriminación".[124] En este sentido, también se afirma que son características de los hechos protegidos por la esfera de la intimidad: *a)* la veracidad de los hechos o datos; *b)* el carácter de desconocidos; y *c)* la potencialidad dañosa del descubrimiento; por lo que la protección jurídica de la vida privada de las personas debe ser garantizada y la justicia debe tomar las medidas preventivas para que tiendan a evitar la producción del daño o su agravamiento y no limitarse a la solución de los conflictos mediante la pertinente sanción.

> La amplitud que toma la divulgación de los datos de afiliación política abre la puerta a un sinnúmero de acciones discriminatorias, algunas de ellas, difíciles de probar. Además, la facilidad con que se accede al conocimiento de estos datos (libremente y desde cualquier lugar) podría incentivar determinadas prácticas políticas que se desean desterrar en nuestro país, como las afiliaciones compulsivas para mantener una fuente de trabajo, o bien, la pérdida de éste por pertenecer a una organización política diferente al gobierno de turno.[125]

En otra variable, si la persona es famosa, o puede considerarse "pública" por su nivel de exposición, el dato que surge de sus actos cotidianos le otorga un perfil difícil de ocultar, y si a ello se suma la relevancia pública de los hechos (como la asistencia a un templo; el solicitar la bendición; confesarse; etc.), la calidad de dato sensible parece inadecuado para requerir el nivel de secreto perseguido.

336.7. *Origen racial*

Se considera en estos datos la pertenencia a una etnia, pueblo o lugar, al margen de la nacionalidad que le corresponda. Se incluye el color de la piel y los rasgos fisonómicos.

El rasgo racial y sus implicancias, tanto como la ideología las creencias son datos sensibles por definir una personalidad de manera directa, pero no lo serían si el ángulo de observación fuera la aplicación que del dato se haga.

Una vez más, la diferencia está en la discriminación resultante, y no en la exclusión del dato o en el secreto absoluto impuesto como deber.

¿Qué ocurriría, por ejemplo, con la política inmigratoria, que necesita conocer datos referidos al origen racial y las circunstancias derivadas de ello para el individuo y su grupo familiar? ¿Puede excluirse un dato tan vital para una base de datos específica como es la de Migraciones de un país determinado?

Se podrá afirmar que son archivos públicos excluidos de las previsiones reglamentarias habituales para los ordenamientos sobre tratamientos de datos, pero a nadie escapa que el dato referido no es una información de por sí privada, reservada

---

[124] PIERINI, Alicia, LORENCES, Valentín, TORNABENE, María Inés, *Habeas data*, Universidad, Buenos Aires, 1999, p. 35.

[125] TULA, María Inés, SOLANO, Mauro, *La difusión de las afiliaciones partidarias frente al derecho de la privacidad*, La Ley Actualidad, del 6 de septiembre de 2005, p. 1

o confidencial, porqué esta a la vista y sólo se podría proteger cuando tiene una finalidad discriminatoria.

336.8. *Datos de Salud*

La fuerte pertenencia a la esfera de la privacidad de estos datos es incuestionable y, como tales, necesitan la máxima protección. Ello determina mantenerlos secretos y confidenciales.

En efecto, los datos del paciente han sido resguardados bajo el secreto profesional en la historia de la medicina, sin embargo en la actualidad, el tratamiento informático de la información médica permite interconectar los archivos y poner en riesgo el presunto anonimato del enfermo.

En Argentina, la ley 25.326 (art. 8° dispone como *datos relativos a la salud):* "Los hospitales y demás instituciones sanitarias públicas o privadas y los profesionales vinculados a la ciencia médica pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando los principios del secreto profesional".

El Consejo de Europa emitió la "*Recomendación 81/1*", donde se insiste en que los datos médicos forman parte de la esfera de intimidad de las personas, de manera que su transmisión o divulgación, solamente puede hacerse en temas y problemas muy puntuales y restringidos.

> Debe considerarse —dice Del Peso Navarro— que el almacenamiento de determinadas informaciones relacionadas con la salud conlleva un peligro añadido, en otras palabras, no será preciso para conocer la enfermedad de un paciente registrar ésta explícitamente, porqué a través de la información relativa a determinados fármacos puede deducirse fácilmente la enfermedad que padece la persona. Por tanto, tales informaciones no deberían salvo excepciones muy especiales como la necesidad de tenerlos a los fines de una investiga salvo excepciones muy especiales como la necesidad de tenerlos a los fines de una investiga figurar en bases de datos a las que tengan acceso directo cualquier colectivo sanitario, sin restringir el acceso de alguna manera a los profesionales médicos que más directamente se relacionen con el paciente.[126]

La privacidad del dato sobre la salud de las personas es confidencial porqué está en un reducto privado (círculo social, familiar y del médico, en particular), pero si el individuo presta conformidad para su cesión o exposición, no advertimos problemas para ello.

> A diferencia de los datos de carácter social, la mayoría de los datos de tipo médico no son objeto de tratamiento por autoridades públicas sino por entidades privadas. La mayor parte de estas entidades son consultadas por médicos que guardan en sus bases de datos la información de sus pacientes para utilizarlos en tratamientos futuros o para comunicarlos a otros médicos de manera individual. Pero no existe una red de bases de datos de carácter médico. Si el paciente así lo desea, el médico que él designe puede desem-

---

[126] DEL PESO NAVARRO, Emilio, "La protección y la seguridad de los datos automatizados de carácter médico", en *Actas del II Congreso Internacional de Informática y Derecho*, Mérida, 1995, pp. 122 y ss.

> peñar una función esencial, en la medida en que se le mantiene informado de los hallazgos de otros médicos, en particular de los especialistas, y de los resultados de las pruebas clínicas. En consecuencia este médico puede disponer de un abanico de datos, más o menos completo, con el consentimiento del paciente.[127]

La contrariedad puede aparecer cuando los datos se transfieren sin consentimiento, lo que es habitual, por ejemplo, cuando la obra social pide información al establecimiento clínico, hospitalario o al médico de su planta profesional, sobre las atenciones prestadas a una determinada persona con el fin de reintegrar las inversiones o gastos por ella practicadas.

Para el caso, la limitación del informe a los puntos solicitados puede resolver la situación porqué, en definitiva, se trata de una relación médico-paciente que interesa a un tercero que soporta los costos necesarios del tratamiento y, para ello, debe estar tan informado como los demás interesados.

> También hay otros contextos que muestran que ya no es válido el antiguo concepto de restringir la protección de datos de carácter médico y social a los organismos que tradicionalmente los han conservado y tratado. Esto se debe a las nuevas formas de división del trabajo, según las cuales los que prestan servicios especializados asumen funciones particulares y, en este contexto, adquieren conocimiento de datos personales. Esto es aún más cierto en el caso de la investigación moderna. La investigación social, por ejemplo, se ocupa de las causas y consecuencias de la pobreza social y la investigación epidemiológica, de la forma en la que el ambiente de trabajo o factores ambientales especiales influyen en las personas. Los investigadores no están interesados en los datos de las personas en cuanto tal, sino exclusivamente en el contexto. Sin embargo, a menudo, tienen que registrar los datos individuales y utilizar sus nombres con el fin de reconocer las relaciones objetivas. Para que la investigación sea aceptable para las personas que la realizan, es preciso no proteger los datos de carácter médico y social relacionados temporalmente para dicha investigación. De lo contrario, para proteger los intereses de las personas involucradas, tal investigación no podría realizarse.

El dato de salud puede ser actual o pasado o referir a una característica que tuvo una persona fallecida. En ningún caso existen diferencias de trato.

Se incluyen en esta categoría los informes sobre adicciones y costumbres que puedan ubicarse como inimputables.

> Habrá que tener especial cuidado —repara Sánchez Bravo— respecto a los datos referentes a la salud mental en el futuro, pues se corre el riesgo de ingresar a los afectados en una especie de "censos negros", con el paralelo peligro para el ejercicio de sus derechos. Se puede así proceder al tratamiento de estos datos sensibles basándose en meras sospechas que no presentan ninguna constatación fáctica. Serían las verdaderas necesidades del tratamiento médico y la evolución de la enfermedad, junto a unas razonables previsiones de futuro, las que deben determinar la inclusión de estos datos.[128]

---

[127] GOZAÍNI, Osvaldo A., *Derecho Procesal Constitucional – Habeas Data,* Rubinzal Culzoni, Buenos Aires, 2001, pp. 176 y ss.

[128] SÁNCHEZ BRAVO, ob. cit., p. 79.

Ahora bien, todos quienes intervienen en tratamientos clínicos y toman información sobre la salud de un paciente, son quienes suelen elaborar la historia clínica, que de este modo, se convierte en el archivo de datos de salud que concierne a una persona.

La historia clínica es un documento médico, legal y administrativo que pasa por varias manos. Están quienes la confeccionan; aquellos que la leen por razones administrativas e intervienen quienes monitorean constantemente en ella para ver la evolución del tratamiento médico.

Uno de los aspectos más críticos es lograr una representación estructurada de la información sobre la evolución de los pacientes, ya que es muy difícil lograr un diseño universal que satisfaga todas las especialidades médicas. El ingreso de información se realiza de forma combinada y precisa, y siempre con la idea de agregar información que pueda ser recuperada para fines estadísticos u otras aplicaciones de rutina (*v. gr.:* ayuda médica, algoritmos, diagramas de toma de decisión, etc.).

De allí que la historia clínica debiera conformar un sistema de información cuyo secreto sea al menos liviano cuando se deba utilizar en el tratamiento. Recuérdese que el médico tiene libertad para agregar comentarios o matices que no pueden generalizarse en una forma estructurada. Las evoluciones o consultas médicas, tal como en un sistema tradicional de historia clínica un dato no debe ser modificado o removido una vez que ha sido firmado así debe suceder con su par computarizado.

La "Recomendación R (97) 5, del 13.02.97, del Comité de Ministros del Consejo de Europa a los Estados Miembros sobre Protección de Datos Médicos", ha dispuesto la necesidad de regular la recogida y procesamiento de datos médicos, con el fin de salvaguardar la confidencialidad y la seguridad de datos personales relativos a la salud.

Ella establece que "los datos médicos deber ser recogidos y procesados honrada y legalmente y sólo para fines especificados", y entre otras razones, afirma que es para "establecer, ejercitar o defender una reclamación judicial". Por último, reviste especial interés la recomendación efectuada en torno a las medidas de seguridad que tal sistema deberá reunir: "Se tomarán las medidas técnicas y de organización adecuadas para proteger los datos personales procesados de acuerdo con esta recomendación contra su destrucción accidental o ilegal y su pérdida accidental, así como contra el acceso, alteración, comunicación o cualquier otra forma de procesamiento no autorizados.

Estas medidas resguardan un nivel apropiado de seguridad, teniendo en cuenta, de una parte, el estado de la técnica y, de otra, la naturaleza sensible de los datos médicos y la evaluación de los riesgos potenciales. Estas medidas se revisan periódicamente.

En líneas muy amplias se tiende a que para la confidencialidad, integridad y exactitud de los datos procesados, así como la protección de los pacientes, se han de tomar medidas apropiadas para:

1) Impedir que cualquier persona no autorizada tenga acceso a las instalaciones de procesamiento de datos personales (control de entrada a las instalaciones)

2) Prohibir que el soporte de los datos sea leído, copiado, alterado o retirado por personas no autorizadas (control del soporte de los datos)

3) Imposibilitar la introducción no autorizada de datos en el sistema de información, y cualquier consulta, modificación o borrado no autorizados de datos personales procesados (control de memoria)

4) Reprimir que los sistemas de procesamiento automatizado de datos sean usados por personas no autorizadas a través de equipos de transmisión de datos (control de utilización)

5) Garantizar que es posible comprobar y establecer "*a posteriori*" quién ha tenido acceso al sistema y qué datos personales han sido introducidos en el sistema de información, cuándo y por quién (control de introducción de datos);

6) Disuadir la lectura, copia, alteración o borrado no autorizados de datos personales durante la comunicación de datos personales y el traslado de soportes de datos (control de transporte);

7) Salvaguardar los datos mediante copias de seguridad (control de disponibilidad) cuando sea necesario, los administradores de archivos de procesamiento de datos médicos deben designar a una persona independiente como responsable de la seguridad de los sistemas de información y de la protección de los datos, y que sea competente para asesorar en estas materias.

En síntesis, si dentro del grupo de informaciones sensibles necesariamente hemos de situar los datos relativos a la salud es indiferente que se trate de una persona de buena o mala salud o, incluso, de un fallecido. Se encuentran incluidas en esta categoría las informaciones relativas a todo tipo de vinculación clínica y asistencial, como el abuso de alcohol o el consumo de drogas. Es decir, cualquier dato que tenga una clara y estrecha relación con la salud.

Por otra parte, conviene reiterar que la Recomendación (97) 5 ya citada, agrega que los datos médicos relativos a niños no nacidos deben considerarse datos personales relativos a la salud, correspondiendo a los padres actuar en representación de los intereses del no nacido (puntos 4.5 y 4.6). Dentro de la categoría de datos médicos, se incluye, también, los datos genéticos.

RECOMENDACIÓN N. R (97) 5, DE 13 DE FEBRERO DE 1997,
DEL COMITÉ DE MINISTROS DEL CONSEJO DE EUROPA
A LOS ESTADOS MIEMBROS SOBRE PROTECCIÓN DE DATOS MÉDICOS

El Comité de Ministros, bajo los términos del artículo 15.b del Estatuto del Consejo de Europa;

Considerando que el fin del Consejo de Europa es alcanzar una mayor unidad entre sus miembros;

Recordando los principios generales sobre protección de datos de la Convención para la Protección de los Individuos en relación al Tratamiento Automatizado de Datos

Personales (Series Tratados Europeos, n. 108) y en particular su artículo 6, que estipula que los datos personales relativos a la salud no pueden ser procesados automatizadamente a menos que el ordenamiento nacional proporcione medidas de seguridad apropiadas;

Consciente del incremento del uso de datos médicos tratados automatizadamente por sistemas de información, no sólo para la asistencia médica, la investigación médica, la gestión hospitalaria y la salud pública, sino también fuera del sector sanitario;

Convencido de la importancia de la calidad, integridad y disponibilidad de los datos médicos para el afectado por tales datos y su familia;

Consciente de que el progreso de la ciencia médica depende en buena medida de la disponibilidad de datos médicos sobre individuos;

Convencido de que es deseable regular la recogida y procesamiento de datos médicos, salvaguardar la confidencialidad y la seguridad de los datos personales relativos a la salud, y asegurar que se emplean de acuerdo con los derechos y libertades fundamentales del individuo, y en particular con el derecho a la intimidad;

Consciente de que el progreso en la ciencia médica y los avances en la tecnología informática desde 1981 hacen necesario revisar varias disposiciones de la Recomendación N. R (81) sobre la regulación de los bancos de datos médicos automatizados;

Recomienda que los gobiernos de los Estados miembros:

- Den pasos para asegurar que los principios contenidos en el apéndice a esta recomendación se reflejen en sus leyes y en la práctica;
- Aseguren una amplia difusión de los principios contenidos en el apéndice a esta recomendación entre las personas implicadas, por razón de su profesión, en la recogida y procesamiento de datos médicos;

Decide que esta recomendación sustituirá a la Recomendación N. R (81) sobre la regulación de bancos de datos médicos automatizados.

Apéndice a la recomendación n. r (97) 5, de 13 de febrero de 1997

1. *Definiciones*

A los fines de esta recomendación:

- La expresión "datos personales" abarca cualquier información relativa a un individuo identificado o identificable. Un individuo no se considerará "identificable" si la identificación requiere una cantidad de tiempo y de medios no razonables. En los casos en que el individuo no sea identificable, los datos son denominados anónimos;
- La expresión "datos médicos" se refiere a todos los datos personales relativos a la salud de un individuo. Se refiere también a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos;
- La expresión "datos genéticos" se refiere a todos los datos, cualquiera que sea su clase, relativos a las características hereditarias de un individuo o al patrón hereditario de tales características dentro de un grupo de individuos emparentados.

También se refiere a todos los datos sobre cualquier información genética que el individuo porte (genes) y a los datos de la línea genética relativos a cualquier aspecto de la salud o la enfermedad, ya se presente con características identificables o no.

La línea genética es la línea constituida por similaridades genéticas resultantes de la procreación y compartidas por dos o más individuos.

2. *Ámbito*

2.1. Esta recomendación es aplicable a la recogida y tratamiento automatizado de datos médicos, salvo que la ley nacional, en un contexto específico fuera del sector sanitario, proporcione otras medidas de seguridad apropiadas.

2.2. Un Estado miembro puede extender los principios establecidos en esta recomendación a datos médicos no procesados automatizadamente.

3. *Respeto a la intimidad*

3.1. Se garantizará el respecto a los derechos y libertades fundamentales, y en particular al derecho a la intimidad, durante la recogida y procesamiento de datos médicos.

3.2. Los datos médicos sólo pueden recogerse y procesarse si existen medidas de protección adecuadas establecidas por la ley nacional.

En principio, los datos médicos deben ser recogidos y procesados sólo por profesionales sanitarios o por individuos u órganos que trabajen en representación de profesionales sanitarios. Los individuos u órganos que trabajen en representación de profesionales sanitarios recogiendo y procesando datos médicos deben estar sujetos a las mismas normas de confidencialidad que pesan sobre los profesionales sanitarios o a normas de confidencialidad comparables.

Los administradores de archivos que no son profesionales sanitarios sólo deben recoger y procesar datos médicos cuando estén sujetos a normas de confidencialidad comparables a las que pesan sobre el profesional sanitario o a medidas de seguridad igualmente eficaces proporcionadas por la ley nacional.

4. *Recogida y procesamiento de datos médicos*

4.1. Los datos médicos deben ser recogidos y procesados honrada y legalmente y sólo para fines especificados.

4.2. Los datos médicos deben obtenerse, en principio, del afectado. Sólo pueden ser obtenidos de otras fuentes si se hace de acuerdo con los Capítulos 4, 6 y 7 y si esto es necesario para alcanzar los fines del procesamiento o si el afectado no está en posición de proporcionarlos.

4.3. Los datos médicos deben ser recogidos y procesados:

a. si lo dispone la ley por:

i. Razones de salud pública; o

ii. Bajo las condiciones del Principio 4.8, la prevención de un riesgo real o la represión de un crimen específico; o

iii. Otro interés público importante; o

b. si lo permite la ley:

i. Para fines médicos preventivos o para fines diagnósticos o terapéuticos relativos al afectado o a un pariente en línea genética; o

ii. Para salvaguardar intereses vitales del afectado o de una tercera persona; o

iii. Para el cumplimiento de obligaciones contractuales específicas; o

iv. Para establecer, ejercitar o defender una reclamación legal; o

c. Si el ha dado su consentimiento el afectado, su representante legal o la autoridad, persona u órgano previsto por la ley, y en la medida en que la ley nacional no disponga otra cosa.

4.4. Si los datos médicos se han recogidos con fines médicos preventivos, diagnósticos o terapéuticos relativos al afectado o a un pariente en línea genética, también pueden procesarse para la gestión de un servicio médico que trabaje en interés del paciente, en

los casos en que su manejo esté previsto por el profesional sanitario que los recogió, o cuando los datos sean comunicados de acuerdo con los principios 7.2 y 7.3.

Niños no nacidos

4.5. Los datos médicos relativos a niños no nacidos deben considerse datos personales y gozar de una protección comparable a la de los datos médicos de un menor.

4.6. Salvo que la ley nacional disponga otra cosa, quien ostente la responsabilidad paterna o materna puede actuar como la persona legalmente legitimada para actuar por el niño no nacido como sujeto de los datos.

Datos genéticos

4.7. Los datos genéticos recogidos y procesados para el tratamiento preventivo, el diagnóstico o el tratamiento del afectado o para investigación científica sólo deben emplearse con esos fines o para permitir al afectado tomar una decisión libre e informada en estas materias.

4.8. El procesamiento de datos genéticos con fines judiciales o de investigación criminal debe ser objeto de una ley específica que ofrezca medidas de salvaguardia adecuadas.

Los datos sólo deben emplearse para establecer si hay un eslabón genético en el conjunto de pruebas aportadas, para prevenir un peligro real o para reprimir un delito específico. En ningún caso deben emplearse para determinar otras características que pueden ser establecidas genéticamente.

4.9. La recogida y procesamiento de datos genéticos con cualquier otro fin distinto de los previstos en los Principios 4.7 y 4.8 sólo debe permitirse, en principio, por razones de salud y en particular para evitar un serio perjuicio a la salud del afectado o de terceros.

Sin embargo, puede permitirse la recogida y procesamiento de datos genéticos en orden a predecir enfermedades en casos en que exista un interés superior y bajo la sujección a las medidas de salvaguardia definidas por la ley.

5. *Información a los afectados*

5.1. Los afectados deben ser informados de los siguientes extremos:

a. La existencia de un archivo que contiene sus datos médicos y el tipo de datos recogidos o que se van a recoger;

b. El fin o fines para los que son o serán procesados;

c. En su caso, el individuo u organismos de los que han sido o serán obtenidos;

d. Las personas u órganos a los que pueden ser comunicados y con qué fines.

e. La posibilidad, si existe, de que el afectado niegue su consentimiento o retire el ya dado, y las consecuencias de tal cesación del consentimiento;

f. La identidad del administrador del archivo y de su representante, si existe, así como las condiciones bajo las que se puede ejercer el derecho de acceso y de rectificación.

5.2. Se debe informar al afectado, como muy tarde, en el momento de recogerlos. Sin embargo, cuando los datos no se obtengan del afectado, se le debe comunicar tal recogida tan pronto como sea posible y, en una forma apropiada, la información a que hace referencia el Principio 5.1, salvo que claramente sea no razonable o impracticable, o salvo que el afectado haya recibido ya la información.

5.3. La información al afectado será apropiada y adaptada a las circunstancias. La información se dará preferiblemente a cada uno de los afectados de forma individual.

5.4. Antes de llevar a cabo un análisis genético, se debe informar al afectado sobre los objetivos del análisis y la posibilidad de hallazgos inesperados.

Personas legalmente incapacitadas

5.5. Si el afectado es una persona legalmente incapacitada, incapaz de tomar una decisión libre y consciente, y la ley nacional no le permite actuar en su propia representación, la información se facilitará a la persona reconocida como legalmente habilitada para actuar en interés del afectado.

Si una persona legalmente incapacitada es capaz de entender, se le debe informar antes de recoger o procesar sus datos.

Derogaciones

5.6 Cabe hacer derogaciones a los principios 5.1, 5.2 y 5.3 en los siguientes casos:

a. La información al sujeto de los datos puede restringirse si así lo dispone la ley y constituye una medida necesaria en una sociedad democrática:

i. Para prevenir un peligro real o reprimir un crimen.

ii. Por razones de salud pública;

iii. Para proteger al afectado y los derechos y libertades de otros;

b. En emergencias médicas, los datos considerados necesarios para el tratamiento médico pueden recogerse previamente a la información.

6. *Consentimiento*

6.1. Al solicitar el consentimiento del afectado, éste debe ser libre, expreso e informado.

6.2. Los resultados de cualquier análisis genético se deben formular dentro de los límites de los objetivos de la consulta, el diagnóstico o el tratamiento para el que se obtuvo el consentimiento.

6.3. Cuando se trate de procesar datos médicos de una persona legalmente incapacitada que es incapaz de una decisión libre, y cuando la ley nacional no le permita actuar en su propia representación, es preciso obtener el consentimiento de la persona legalmente habilitada para actuar en interés de éste, o de la autoridad o persona u órgano designados por la ley con este fin.

Si, de acuerdo con el Principio 5.5, una persona legalmente incapacitada ha sido informada de la intención de recoger o procesar sus datos médicos, sus deseos deben tenerse en cuenta, a menos que la ley nacional disponga otra cosa.

7. *Comunicación*

7.1. Los datos médicos no se comunicarán, salvo en las condiciones establecidas en este capítulo y en el Capítulo 12.

7.2. En particular, salvo que la ley nacional proporcione otras medidas de salvaguardia, los datos médicos sólo pueden comunicarse a una persona sujeta a las normas de confidencialidad que pesan sobre un profesional sanitario o a normas de confidencialidad comparables, y que acate las normas de esta recomendación.

7.3 Los datos médicos pueden comunicarse si son relevantes y:

a. Si la comunicación está prevista por la ley y constituye una medida necesaria en una sociedad democrática por:

i. Razones de salud pública; o

ii. La prevención de un peligro real o la represión de un delito específico; o

iii. Otro interés público importante; o

iv. la protección de los derechos y las libertades de otros; o

b. Si la comunicación es permitida por la ley con fines de:

i. Protección del sujeto de los datos o de un pariente en línea genética;

ii. Salvaguarda de intereses vitales del afectado o de una tercera persona; o

iii. El cumplimiento de obligaciones contractuales específicas; o

iv. El establecimiento, ejercicio o defensa de una reclamación legal; o

c. Si el afectado o su representante legal o la autoridad o persona u órgano previstos por la ley han dado su consentimiento para uno o más fines, y en la medida en que la ley nacional no disponga otra cosa; o

d. Sentado que el afectado o su representante legal o la autoridad, persona u órgano previstos por la ley no se ha opuesto explícitamente a cualquier comunicación no obligatoria, si los datos han sido recogidos en un contexto de prevención, diagnóstico o terapia libremente elegidos, y el propósito de la comunicación, en particular si se trata de la prestación de cuidado al paciente o del funcionamiento de un servicio médico que trabaje en interés del paciente, no es incompatible con el fin del procesamiento para los que los datos fueron recogidos.

8. *Derechos del afectado*

Derechos de acceso y de rectificación

8.1. Se permitirá a toda persona el acceso a sus datos médicos, ya directamente o a través de un profesional sanitario o, si lo permite la ley nacional, a través de una persona designada por el titular de los datos. La información debe ser facilitada de modo inteligible.

8.2. El acceso a los datos médicos puede ser denegado, limitado o rechazado sólo si lo prevé la ley y si:

a. Constituye una medida necesaria en una sociedad democrática por su interés en proteger la seguridad del Estado, la seguridad pública o la represión de crímenes; o

b. El conocimiento de la información es probable que cause un serio daño a la salud del afectado; o

c. La información sobre el afectado revela también información sobre terceros o, respecto a los datos genéticos, si esta información es probable que cause un serio daño a un pariente consanguíneo o uterino o a una persona que tiene un vínculo directo en línea germinal; o

d. Los datos son empleados para fines de investigación científica o estadística y se aprecia con nitidez que no hay riesgo alguno de violación de la intimidad del afectado, especialmente el de usar los datos en decisiones o medidas que afecten a un individuo en particular.

8.3. El afectado puede pedir la rectificación de los datos erróneos sobre su persona y, en caso de negativa, tendrá la capacidad de recurrir la decisión.

Hallazgos inesperados

8.4. La persona sometida a un análisis genético debe ser informada de los hallazgos inesperados si concurren las siguientes condiciones:

a. La ley nacional no prohibe dar tal información;

b. La persona en cuestión la ha solicitado;

c. No es probable que la información le cause un daño serio:

i. A su salud; o

ii. A su parentela consanguínea o uterina, a un miembro de su familia social o a una persona que tenga un vínculo directo con su línea genética, salvo que la ley nacional proporcione otras medidas de salvaguarda adecuadas.

Sin perjuicio de lo dispuesto en el sub-parágrafo *a)*, la persona debe ser también informada si tal información es de importancia directa para él en el ámbito del tratamiento o la prevención.

9. *Seguridad*

9.1. Se tomarán las medidas técnicas y de organización adecuadas para proteger los datos personales procesados de acuerdo con esta recomendación contra su destrucción accidental o ilegal y su pérdida accidental, así como contra el acceso, alteración, comunicación o cualquier otra forma de procesamiento no autorizados.

Estas medidas asegurarán un nivel apropiado de seguridad, teniendo en cuenta, de una parte, el estado de la técnica y, de otra, la naturaleza sensible de los datos médicos y la evaluación de los riesgos potenciales.

Estas medidas serán revisadas periódicamente.

9.2. En orden a asegurar en particular la confidencialidad, integridad y exactitud de los datos procesados, así como la protección de los pacientes, se tomarán medidas apropiadas para:

a. Impedir que cualquier persona no autorizada tenga acceso a las instalaciones de procesamiento de datos personales (control de entrada a las instalaciones);

b. Impedir que el soporte de los datos sea leído, copiado, alterado o retirado por personas no autorizadas (control del soporte de los datos);

c. Impedir la introducción no autorizada de datos en el sistema de información, y cualquier consulta, modificación o borrado no autorizados de datos personales procesados (control de memoria);

d. Impedir que los sistemas de procesamiento automatizado de datos sean usados por personas no autorizadas a través de equipos de transmisión de datos (control de utilización);

e. Asegurar —teniendo en cuenta, por un lado, el acceso selectivo a los datos y, por otro, la seguridad de los datos médicos— que el diseño del sistema de procesamiento, como norma general, es tal que permite la separación de:

- identificadores y datos relativos a la identidad de las personas,
- datos administrativos,
- datos médicos,
- datos sociales,
- datos genéticos (control de acceso);

f. Garantizar la posibilidad de comprobar y verificar a qué personas u órganos se pueden comunicar los datos a través de equipos de transmisión de datos (control de comunicación);

g. Garantizar que es posible comprobar y establecer '*a posteriori*' quién ha tenido acceso al sistema y qué datos personales han sido introducidos en el sistema de información, cuándo y por quién (control de introducción de datos);

h. Impedir la lectura, copia, alteración o borrado no autorizados de datos personales durante la comunicación de datos personales y el traslado de soportes de datos (control de transporte);

i. Salvaguardar los datos mediante copias de seguridad (control de disponibilidad).

9.3. Los administradores de archivos médicos deben, de acuerdo con la ley nacional, elaborar normas internas apropiadas que respeten los principios pertinentes de esta recomendación.

9.4. Cuando sea necesario, los administradores de archivos de procesamiento de datos médicos deben designar a una persona independiente como responsable de la seguridad de los sistemas de información y de la protección de los datos, y que sea competente para asesorar en estas materias.

10. *Conservación*

10.1. En general, los datos médicos no deben conservarse más tiempo del necesario para alcanzar el propósito para el que se recogieron y procesaron.

10.2. Cuando se acredite la necesidad de conservar los datos médicos que ya no tienen uso alguno para el fin con el que se recabaron por un interés legítimo de la salud pública o de la ciencia médica, o de la persona a cargo del tratamiento médico o del controlador del archivo en orden a permitirles la defensa en o el ejercicio de una reclamación legal, o por razones históricas o estadísticas, se adoptarán las medidas técnicas oportunas para asegurar su correcta conservación y seguridad, teniendo en cuenta la intimidad del paciente.

10.3 A petición del afectado, sus datos médicos deben ser eliminados, a menos que se hayan anonimizado o concurran intereses superiores y legítimos para no hacerlo, en particular los reseñados en el Principio 10.2, o si existe una obligación de conservar los datos grabados.

11. *Flujos transfronterizos*

11.1 Los principios de esta recomendación son aplicables al flujo transfronterizo de datos médicos.

11.2 No debe someterse a condiciones especiales de protección de la intimidad el flujo transfronterizo de datos médicos a un Estado que ha ratificado la Convención para la Protección de los Individuos en relación al Tratamiento Automatizado de Datos Personales, y que dispone de legislación que proporciona al menos una protección equivalente de los datos.

11.3. Donde la protección de los datos médicos pueda considerarse en línea con el principio de protección equivalente sentado por la convención, no se debe aplicar restricción alguna al flujo transfronterizo de datos médicos a un Estado que no haya ratificado la Convención, pero que disponga de normas legales que aseguren una protección acorde con los principios de tal Convención y de esta recomendación.

11.4. Salvo que la ley nacional disponga otra cosa, el flujo transfronterizo de datos médicos a un Estado que no asegura la protección de acuerdo con la Convención y con esta recomendación, el flujo no debe tener lugar a menos que:

a. Se hayan tomados las medidas necesarias, incluidas aquellas de naturaleza contractual, para que se respeten los principios de la Convención y de esta recomendación, y el afectado haya tenido la posibilidad de oponerse a la transferencia; o

b. El afectado haya dado su consentimiento.

11.5. Salvo en caso de emergencia o de una transferencia a la que el titular de los datos haya dado su consentimiento informado, se deben tomar medidas apropiadas para asegurar la protección de los datos médicos transferidos de un país a otro, y en particular:

a. La persona responsable de la transferencia debe indicar al destinatario los fines específicos y legítimos para los que se recogieron los datos, así como las personas u organismos a los que éstos pueden comunicarse;

b. Salvo que la legislación nacional disponga otra cosa, el destinatario debe comprometerse ante la persona responsable de la transferencia a respetar los fines específicos y legítimos que éste último ha aceptado, y a no comunicar los datos a personas u organismos distintos de los indicados por la persona responsable de la transferencia.

12. *Investigación científica*

12.1. Siempre que sea posible, los datos médicos usados para fines de investigación científica deben ser anónimos. Los profesionales y organizaciones científicas y las autoridades públicas deben promover el desarrollo de técnicas y procedimientos para asegurar el anonimato.

12.2. Sin embargo, si tal anonimización hiciese imposible un proyecto científico de investigación, y el proyecto se va a realizar con fines legítimos, podría llevarse a cabo con datos personales a condición de que:

a. El titular de los datos haya dado su consentimiento informado para uno o más fines de investigación; o

b. Otorguen el consentimiento el representante legal o la autoridad o persona u órgano previstos por la ley cuando el afectado sea una persona legalmente incapacitada e incapaz de una decisión libre, y la ley nacional no le permita actuar en su propia representación, siempre que este consentimiento se dé en el marco de un proyecto de investigación relacionado con la condición médica o la enfermedad del afectado; o

c. El órgano u órganos designados por la ley nacional hayan autorizado la revelación de los datos con el fin de llevar a cabo un proyecto de investigación médica relacionado con un interés público importante, pero sólo si:

i. El titular de los datos no se ha opuesto expresamente a la revelación; y

ii. A pesar de los esfuerzos razonables que se puedan adoptar, sería impracticable contactar con el titular de los datos para pedir su consentimiento; y

iii. El interés del proyecto de investigación justifica la autorización; o

d. la investigación científica está prevista por la ley y constituye una medida necesaria por razones de salud pública.

12.3. Bajo las previsiones complementarias que la ley nacional establezca, debe permitirse a los profesionales sanitarios habilitados para realizar su propia investigación médica el uso de los datos médicos que tienen en la medida en que el sujeto afectado haya sido informado de esta posibilidad y no se haya opuesto.

12.4. Respecto a cualquier investigación científica basada en datos personales, los problemas incidentales —incluidos aquellos de naturaleza ética y científica— que puedan surgir como consecuencia del respeto a las disposiciones de la Convención para la Protección de los Individuos en relación al Tratamiento Automatizado de Datos Personales deben ser examinados también a la luz de otros instrumentos pertinentes.

12.5. Los datos personales usados para investigación científica no pueden publicarse en forma que permita identificar a los titulares de los datos, salvo que éstos hayan dado su consentimiento a la publicación y ésta sea permitida por la ley nacional.

Finalmente resta ver cómo trabaja el proceso de *habeas data* con relación al dato médico y su archivo en la historia clínica.

Hemos advertido sobre la ausencia en nuestra legislación de un sistema que tenga en cuenta la posibilidad de elaborar un registro médico o, directamente, la historia clínica, por medios informáticos. También señalamos el deber de mantener incólume a la persona afectada imposibilitando que los datos almacenados puedan ser con él relacionados.

Ahora bien, la finalidad que tiene la tutela especial a los datos sensibles proviene de la necesidad de custodiar uno de las aspectos más privados de la persona, donde sólo ella puede autorizar la difusión de aquellos datos que considere se pueden dar a publicidad, o ponerlos al conocimiento de terceros. De otro modo, quien archive, directa o indirectamente, datos médicos debe ser sumamente precavido con la seguridad interna y externa de la base de datos, otorgando al tema de la disociación, la prioridad que tiene y merece.

Con esta advertencia es perfectamente lógico propiciar una historia clínica informatizada. Ella podría aumentar los campos de información y posibilitar los agregados de comentarios en hipertexto o del médico que la realiza (con finalidades académicas, por ejemplo).

Ahora, con relación a la procedencia del *habeas data* como remedio para el acceso y para concretar cualquiera de las acciones de control (actualización, rectificación, supresión o confidencialidad) que la ley posibilita.

La jurisprudencia ha sido restrictiva para admitir la acción de protección de datos personales como medio para obtener una historia clínica, o tener acceso a ella por esta vía. En la causa *Bianchi de Sáenz, Delia A. c/ Sanatorio Greyton S.A* (CNCiv., Sala F, 6 de julio de 1995), se sostuvo que:

1) Si bien el *habeas data* deducido por la actora para lograr que el sanatorio demandado le entregue su historia clínica es improcedente para tal fin, el principio "*iura novit curia*" autoriza a los jueces a efectuar la calificación jurídica de las pretensiones de las partes. 2) Las diligencias preliminares no necesariamente deben ser el antecedente de una demanda. Su promoción se limita a la exhibición de una cosa mueble, un título, documentos, elementos útiles al interesado en un proceso posterior, cuya iniciación y modalidades pueden depender del resultado de la diligencia.

> La actora fue internada en el Sanatorio Greyton para ser operada de una fractura de cadera. Al día siguiente de la operación, y por razones que desconoce, su estado de salud comenzó a agravarse. Ante la pasividad del personal del sanatorio que retaceaba explicaciones acerca de las complicaciones, su hija recurrió al asesoramiento de un médico que evaluó que debía ser internada inmediatamente en terapia intensiva. Para ello, la hija solicitó el traslado de su madre al Hospital Británico culpando de negligentes al personal del Sanatorio. Previo a autorizar el retiro, las autoridades del Sanatorio exigieron a la hija firmar una declaración asumiendo la responsabilidad del traslado, conocer el estado de salud de la enferma y "prestar conformidad" con la historia clínica, documento del cual no se le permitía sacar fotocopias Una vez internada en el Hospital Británico en terapia intensiva y con diagnóstico, el nuevo médico solicitó al Sanatorio la historia clínica pero le fue denegada. Con este fin promueve acción de amparo (*habeas data*).

En principio, la decisión del juez *a quo* de rechazar el amparo es irreprochable en cuanto a que no es dudoso concluir que la actora no ha escogido el camino adecuado. *Pero por aplicación de la regla "*iura novit curia*", el juzgado puede decidir el proceso aplicando distintas normas a las invocadas.*

Se habló de una actuación negligente de la demandada, por lo que bien podrían traerse a este caso las disposiciones procesales que regulan la prueba anticipada o las diligencias preliminares, y de esta manera, obtener la información requerida, a pesar de ser utilizada para un fin distinto que el común. Es que si bien las medidas preparatorias preliminares son el antecedente de una demanda, de ello no se sigue que necesariamente tenga que ser así.

336.9. *Datos sexuales*

Se llaman datos sexuales aquellos que recopilan información sobre hábitos o preferencias que se relacionan con la actividad de una persona en sus relaciones sexuales. En un caso, la información compila el comportamiento sexual del individuo así como la ausencia de dicha actividad, y las consecuencias derivadas.

En las preferencias se sustraen datos objetivos como las suscripciones a revistas de contenido erótico, anuncios de contacto, pertenencia a agrupaciones homosexuales o afines, etc.

Cada uno de estos datos, naturalmente, es esencialmente privado y corresponden a la intimidad personal de cada uno, circunstancia que permite sustraerlos de una base de datos o mantenerlos en estricta confidencialidad.

Para nosotros este tipo de datos sensibles que se almacenan tienen dos particularidades relevantes para su protección procesal. Si el fichaje se toma sin consentimiento, quien lo realiza viola la ley y merece una sanción por ello. Si tiene consentimiento para el acopio y la transmisión la situación varía y se debe observar la aplicación que tiene la información proporcionada (por ejemplo, si la persona concernida tiene la costumbre de filmar sus actos de pareja, la reproducción del video tomado de una base de datos privada para hacerlo público es la violación consistente).

336.10. *Las condenas penales*

Esta modalidad de registro de antecedentes penales que supone archivar toda condena sufrida por la persona, suele plantearse como datos sensibles. Así los considera el artículo 7 inciso 4° de la ley 25.326 (*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*).

No es este un criterio corriente que se encuentre en otras legislaciones. Veamos, entonces, cuáles son las razones que hacen la diferencia.

La prohibición de almacenamiento se dirige a la creación de archivos destinados exclusivamente a la historia de conductas personales que hayan generado penalidades. La idea no es obstaculizar la acción del Estado a través de sus organismos es-

pecíficos, sino de impedir que la información almacenada sea fuente productora de discriminación.

De todos modos, la sensibilidad del dato no llega del secreto que sobre el mismo se quiera mantener, pues las sentencias son públicas (con algunas excepciones como las condenas a menores de edad que según las *reglas de Bijing* del 29/11/95 aprobadas por "Naciones Unidas" obliga a su carácter estrictamente confidencial), sino del uso discriminatorio que se haga de él.

En tal sentido, el *habeas data* no procede como vía de reparación porqué el dato no se puede excluir, al ser público. Obviamente no se pueden borrar los antecedentes carcelarios o las condenas que haya tenido una persona. Lo contrario, inutilizaría muchas reglas procesales en lo penal y seguramente provocaría una ruptura en el sistema de protección de los derechos de la sociedad.

La Ley 23.444 (Argentina) del 28 de octubre de 1986, aprobó el convenio sobre comunicación de antecedentes penales y de información sobre condenas judiciales por narcotráfico y uso indebido de estupefacientes, adoptado por la VI Conferencia de Ministros de Justicia de los Países Hispano-Luso-Americanos y Filipinas que se llevó a cabo en la ciudad de Lisboa entre el 5 y el 12 de octubre de 1984.

El dispone:

ART. 1.—Las partes contratantes se comprometen a prestarse mutuamente de conformidad con las disposiciones del presente Convenio, la más amplia asistencia posible en los procedimientos seguidos por actividades delictivas referentes a actos de cultivo, producción, fabricación, extracción, preparación, posesión, almacenamiento, oferta, distribución, compra, venta, despacho en cualquier concepto, corretaje, expedición, tránsito, transporte, importación y exportación de sustancias estupefacientes y sustancias psicotrópicas. […].

ART. 6.—1. Toda denegación de facilitar los antecedentes penales solicitados deberá ser motivada.

ART. 7.—1. Sin perjuicio de facilitar los antecedentes penales cuando sean solicitados, cada una de las Partes informará a cualquier otra Parte interesada de las sentencias penales y medidas posteriores que afecten a los nacionales de esta última y que hayan sido objeto de inscripción en el Registro de Antecedentes penales como consecuencia de condenas o medidas adoptadas en causas seguidas por tráfico ilícito de estupefacientes o sustancias psicotrópicas. Los Ministerios de Justicia, se comunicarán recíprocamente esta información una vez por año.

2. En relación a la transmisión de informaciones a que alude el número anterior, podrán las partes solicitar informaciones complementarias.

ART. 8.—1. El presente Convenio está abierto a la firma de todos los Estados miembros de la Comunidad Hispano-Luso Americana. Los instrumentos de ratificación, adhesión o aceptación serán depositados en la Secretaría General Permanente de la Conferencia de Ministros de Justicia.

2. El convenio entrará en vigor tres meses después de la fecha del depósito del segundo instrumento de ratificación o aceptación.

3. Entrará en vigencia, con respecto a todo Estado que ratifique o acepte posteriormente el Convenio, tres meses después de la fecha del depósito de su instrumento de ratificación, adhesión o aceptación.

Desde otra perspectiva, puede enfocarse el problema como deficiencias que encuentra el ex penado para reinsertarse en el medio social en que vive. El dato antecedente le impide integrarse porque se lo descalifica o segrega. En estas situaciones, no es el dato el que causa la crisis, ni la ocultación del mismo llevaría a solucionarlo.

Por eso la redacción que tiene la ley argentina no esclarece el alcance que permite para el tratamiento de datos vinculados con antecedentes penales y contravencionales, porqué la mención de leyes y reglamentos respectivos no es suficiente para encontrar límites precisos para el tratamiento de este tipo de datos personales. No obstante, se ha dicho que esta norma es independiente de las que regulan y reglamentan los antecedentes penales como el cumplimiento de sentencias dictadas en los procesos penales y contravencionales.

> Sostiene Eduardo Menem que el nuevo texto legal se aplica también a los registros públicos, por lo que el registro permanente y el tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las Fuerzas Armadas, fuerzas de seguridad, organismos policiales o inteligencia están sometidos al nuevo régimen legal que obliga a respetar la confidencialidad, limita la cesión de los datos y permite el acceso a ellos del interesado para verificar su exactitud. La incorporación de estos registros tiene por objeto evitar el mantenimiento por parte de esas fuerzas, de datos que no resulten imprescindibles para su función, por ejemplo aquellos datos que la ley denomina sensibles, que son los que revelan el origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. Por otra parte, la ley expresamente establece que no se altera de ningún modo el registro de antecedentes penales o contravencionales, que se regirán por la legislación específica que los regula, cuyo pleno funcionamiento queda así garantizado de modo que la Justicia pueda disponer de amplia información para evaluar la eventual reincidencia del imputado. Es decir, la Ley de *Habeas Data* no flexibiliza ni permite de ninguna manera la alteración de aquellos datos que hacen a la seguridad pública, los que se mantendrán registrados por los plazos y en las condiciones que prevén las leyes especiales que los rigen, sin que nadie que tenga antecedentes penales pueda beneficiarse de algún modo por esta nueva ley.[129]

La información sobre antecedentes personales es diferente del registro de conductas penadas por la ley. Por ello, el *habeas data* procede en cualquiera de los supuestos ya citados con el fundamento de resolver el tratamiento de datos automatizados de carácter personal cuando la base o archivo ofrezca una definición de características personales o un perfil individual; no así cuando la información proporcionada refiere a los antecedentes penales de la persona.

En su caso, la autoridad que posea esta base informativa está obligada a cumplir con los preceptos legales, aun cuando pueda, en el ejercicio de sus propias actividades, comunicar a otros las condenas sufridas por los imputados.

---

[129] MENEM, Eduardo, "Una ley que garantiza el derecho al honor y a la intimidad", *Diario La Nación* del 30 de octubre de 2000.

> Un solo ejemplo sirve para ilustrar este punto de manera más que suficiente: en cualquier democracia, la vista de un procedimiento penal en la que se dicta sentencia es publica, pero en todas y cada una de nuestras democracias —afirma Marcel Pinet— los antecedentes penales, que son los archivos de las condenas que se dictaron de manera pública, son uno de los archivos más protegidos y menos accesibles. Esto es un ejemplo de como cuando se recopila información, ésta toma un valor informativo específico. Esta es la razón por la que un fallo del Tribunal Supremo de los Estados Unidos, del 22 de marzo de 1989, denegó la petición de unos periodistas para serles comunicadas las sentencias de varias personas ligadas a la mafia, aunque éstas se habían dictado públicamente. El tribunal precisó que al evaluar los intereses en conflicto, "la infracción del derecho al respeto de la vida privada de un ciudadano, resultante de la difusión de sus antecedentes penales, superaba el interés público que se obtendría del ejercicio de la libertad de prensa".[130]

Cuando el antecedente penal queda en un registro o bancos de datos de información judicial, se advierte la trascendencia del problema a resolver cuando se difunde un dato proveniente de dichas fuentes.

En efecto, los ficheros incorporan decisiones judiciales tomadas respecto a personas físicas y jurídicas; algunas veces, son resoluciones adoptadas en el curso del procedimiento (lo cual supone su provisionalidad) de modo tal que solamente con la sentencia (firme y definitiva) el dato es actual y exacto.

Pero un conflicto habitual en los medios de comunicación es transferir situaciones procesales no firmes como si fueran tales, afectando en consecuencia algunos principios o garantías procesales que se destinan hacia la persona (en la dimensión de sus propias libertadas, como la presunción o estado de inocencia; o la continuidad de la empresa en los procesos fallimentarios) y hacia el órgano judicial (debido proceso, defensa de las personas, imparcialidad del juez, etc.). En estos casos, el dato se obtiene de una fuente judicial fidedigna, es verdad, pues el acceso a la información no está vedada en las actuaciones jurisdiccionales, salvo en situaciones muy especiales. El inconveniente aparece en la forma como se difunde el dato, y en la prohibición de divulgar antecedentes penales o contravencionales por constituir una afrenta a la protección de datos personales, la intimidad y el honor. Esta es la situación que la ley pretende consolidar evitando la transmisión de datos sensibles como los referidos.

337. Datos personales en expedientes judiciales

337.1. Las actuaciones judiciales son públicas aunque los expedientes pueden mantenerse en reserva y confidencialidad en determinadas circunstancias. Las limitaciones siempre se han de resolver analizando particularmente el caso. La decisión, a la luz del proceso en cuestión, ha de considerar circunstancias como: la fase en la que se encuentra; si no ha concluido aún, la legitimación del interés del peticionario,

---

[130] PINET, Marcel, *Datos públicos o datos a los que puede acceder el público y protección de datos personales,* en XX Conferencia Internacional de autoridades de protección de datos (1998), Agencia de Protección de Datos, Madrid, 1999, p. 65.

el alcance objetivo de la consulta, o la finalidad del tratamiento, previo a la ponderación de los valores en conflicto, buscando el necesario equilibrio entre el derecho a un proceso público con todas las garantías, la tutela de los derechos fundamentales inherentes a las personas cuyos datos personales constan incorporados a la documentación judicial y otros valores constitucionalmente protegidos, como el derecho, también fundamental, a recibir y comunicar información.

337.2. La cuestión de la publicidad de las actuaciones judiciales y el problema que en ellos cierne es el tema de este espacio, donde se pueden ver de inmediato dos cuestiones esenciales. La de los datos que un expediente reporta por su sola condición pública, de manera que cualquier persona, tomando como base que el expediente judicial puede acceder al ser una fuente de acceso público; y la privacidad alterada que encuentra quien es parte en la controversia.

El aspecto de modular la accesibilidad a las actuaciones judiciales está en hallar el necesario equilibrio entre el derecho a un proceso público con todas las garantías y la tutela de derechos fundamentales inherentes a las personas cuyos datos personales, precisamente por su relación con el proceso, ya sea como partes procesales, testigos o peritos, han sido incorporados a la documentación judicial.

La experiencia diaria evidencia que tal incorporación potencialmente entraña determinados riegos para determinados bienes jurídicos, sobre todo si no se tiene asegurado el control respecto del tratamiento que posteriormente puedan recibir aquellos datos.

> Ha dicho Gomez Loeches, a quien seguimos en estas apreciaciones, que la dificultad o imposibilidad de asegurar el referido control y la gravedad de los eventuales riesgos o peligros a que se ven sometidos en algunos casos los titulares de tales datos, ha hecho necesaria la articulación de instrumentos normativos, como la Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales, que permitan a la autoridad judicial la aplicación de las medidas legales de protección que considere necesarias, previa ponderación, a la luz del proceso, de los distintos bienes jurídicos constitucionalmente protegidos, de los derechos fundamentales en conflicto y de las circunstancias concurrentes en los testigos y peritos en relación con el proceso de que se trate.[131]

337.3. Otras veces son intereses públicos con relevancia constitucional basados en razones de eficacia en la acción de la justicia los que aconsejan una protección más reforzada que la que brinda el deber de sigilo profesional de quienes intervienen en el tratamiento de tales datos, como son el secreto y la reserva.

La técnica de declarar secretas o reservadas unas actuaciones es habitualmente empleada con la finalidad de excluir de su conocimiento a personas ajenas o no autorizadas, y así evitar los eventuales riesgos derivados de un posterior tratamiento de tales datos en unas condiciones, o con unas finalidades, que su titular no tenga

---

[131] GOMEZ LOECHES, Luis, *El acceso a la documentación de las actuaciones judiciales,* Universidad Alcalá de Henares, Madrid, Centro de Documentación.

obligación jurídica de soportar, o en las cuales no esté garantizada la integridad de los enunciados bienes jurídicos.

La cuestión del acceso afecta a sujetos diferentes. Propone Gomez Loeches la siguiente terminología: *el peticionario* (persona que pretende ejercer el derecho de acceso a la información, puede ser el propio afectado o interesado, o un tercero), *el órgano judicial* (el personal del órgano que intervenga en el tratamiento de la información, sea a título de responsable o de encargado del tratamiento) y *el interesado* (o afectado, es la persona física identificada o identificable concernida por la información, aquella cuyos datos personales forman parte de los antecedentes que obran en las actuaciones).[132]

Si el peticionario es el propio interesado, y se identifica como tal, no tendrá dificultades para acceder a las actuaciones, a menos que le afecte el carácter reservado o secreto que pueda pesar sobre éstas. Tampoco tendrá problema aquel abogado que demande correctamente el acceso por encargo de su cliente, el interesado.

Continúa afirmando Gomez Loeches que:

> en el ámbito penal, el derecho de defensa corresponde a aquellos de los que resulta una imputación en unas diligencias penales o pueden resultar perjudicados por el hecho delictivo (artículo 118 LECr.), quienes tienen la condición de legítimamente interesados, con independencia de que formalmente haya o no comparecido en la causa. Esto es, el que los interesados no se hayan mostrado formalmente parte en el proceso, no restringe su derecho de acceso, pero la falta de personería en la causa por medio de Procurador de los Tribunales en modo alguno exime al Abogado de acreditar el encargo de su cliente, de modo fehaciente y a satisfacción de quien ha de controlar el acceso a las actuaciones, así como que su cliente posee un interés legítimo.

337.4. Claro está que definir o identificar al que toma conocimiento de las actuaciones judiciales no resuelve el problema, o al menos, lo simplifica en el sentido de verificar quien sabe cuánto se desarrolla en el expediente. Vale decir que si éste difunde los datos sin disociar la información, puede quedar expuesto a los principios que reglan la protección de datos personales.

Surgen así otras excusas absolutorias, como son el derecho de acceso a la información y documentos que producen los poderes públicos; y también el potencial derecho a informar aquello que es de interés público (*v. gr.:* pongamos como ejemplo aquellas causas judiciales de relevancia o interés mediático que ponen a los hechos y a las personas en un escenario de especulaciones o imaginerías).

Pero la garantía de publicidad tiene el límite de las situaciones jurídicas subjetivas de los ciudadanos cuya dignidad puede quedar alterada o su vida privada afectada por la información que se transmite de un expediente judicial.

337.5. En Europa la preocupación por la difusión de datos personales que se archivan en los expedientes judiciales, y en particular, a través de las resoluciones jurisdiccionales, han dado espacio a la *Recomendación nº R (95) 11* del Comité de

---

[132] Ver nota anterior.

Ministros (adoptada el 11 de setiembre de 1995), procurando facilitar la información jurisprudencial sin que ella afecte los derechos de las personas involucradas.

Entre sus principales disposiciones se encuentran las siguientes:

- Considerando la Recomendación nº R (83) 3 sobre la protección de los usuarios de los servicios de información jurídica,
- Considerando que el pleno conocimiento de la jurisprudencia de todas las jurisdicciones es una de las condiciones esenciales para la aplicación equitativa de derecho;
- Considerando que la objetividad y la representación de los sistemas automatizados de difusión de la jurisprudencia es una condición indispensable para una buena justicia,
- Constatando que los medios automatizados son utilizados cada vez más frecuentemente para la investigación jurídica, y que el creciente número y la complejidad de las resoluciones judiciales fomentan un recurso cada vez más amplio a estos nuevos métodos,
- Considerando que el público en general y las profesiones jurídicas en particular deben tener acceso a esos nuevos métodos de información,

Recomienda a los gobiernos de los Estados miembros:

1. Poner en conocimiento de las personas encargadas de la creación, de la gestión y de la puesta al día de los sistemas de documentación jurídica automatizados los principios generales y las líneas directrices que se definen a continuación.

2. Tomar las medidas apropiadas para permitir la aplicación de estos principios y de las líneas directrices a los sistemas automatizados de difusión de la jurisprudencia en el sector público, de facilitar su aplicación a la representatividad de los sistemas automatizados de difusión de la jurisprudencia.

3. Tomar las medidas necesarias para garantizar el acceso fácil de todos los usuarios a los sistemas automáticos de documentación jurídica abiertos al público.

Anexo 1 a la Recomendación nº R (95)11
principios generales para los sistemas automatizados de documentación jurídica automatizados relativos a la selección, el tratamiento, la presentación y el archivo de las resoluciones judiciales

I. *Campo de aplicación*

A los efectos de esta Recomendación, los sistemas de difusión de las resoluciones judiciales comprenden:

- los bancos de datos, cualquiera que sea su constitución difusión;
- los nuevos soportes de difusión magnética y óptica (especialmente los CD-Rom que contengan la jurisprudencia).

II. *Objetivos de la jurisprudencia*

Los objetivos de los sistemas automatizados son, especialmente;

- —Facilitar el trabajo a las profesiones jurídicas proporcionándoles datos rápidamente, completos y actualizados, —informar a toda persona interesada en una cuestión de jurisprudencia; —hacer públicas más rápidamente las nuevas resoluciones, particularmente en las materias de derecho en evolución; —hacer público un número más grande de resoluciones que afecten tanto al aspecto normativo como al factual (quántum de las indemnizaciones, de las pensiones de alimentos, de las penas, etc.);

—contribuir a la coherencia de la jurisprudencia (seguridad jurídica"Rechtssicherheit") pero sin introducir rigidez; —permitir al legislador hacer análisis de la aplicación de las leyes, —facilitar los estudios sobre la jurisprudencia;

- En ciertos casos, proporcionar informaciones con fines estadísticos.

III. *Principios generales*

1. *Cobertura*

La jurisprudencia de todos los ámbitos del derecho y del conjunto de las regiones geográficas debe poder ser difundido por uno o varios sistemas automatizados. Los Estados deberían garantizar ellos mismos o promover sistemas para ocuparse de los sectores que no estén ya incluidos en algún sistema (véase la Recomendación nº R(83)3, anexo 1, parte 1, n25, 22 apartado, así como el Anexo 11 más adelante, 11.3).

2. *Exhaustividad - selección*

2.1. Se puede hacer una selección de las resoluciones según las reglas del sistema jurídico o las necesidades del sistema automatizado, se puede hacer una selección de las resoluciones cuando resulte necesario.

2.2. En los sectores en los que se realice una selección, ésta deberá ser objetiva según los criterios previstos en el Anexo II, y las resoluciones seleccionadas deberán ser globalmente representativas de la jurisprudencia del sector.

Ello comprende la selección de una resolución contraria a una tendencia jurisprudencias dominante.

3. *Actualidad y puesta al día*

El sistema automatizado debe ser cargado regularmente en plazos razonables con las resoluciones recientes de las jurisdicciones.

Es deseable que el sistema automatizado permita a los usuarios una información rápida de las resoluciones más recientes introducidas en el sistema.

Los plazos de la puesta al día no deberían superar, en la medida de lo posible, un mes para las resoluciones de los tribunales supremos y tres meses para las resoluciones de las otras jurisdicciones a contar desde el día de su publicación o de la entrega de la copia de la resolución a las partes.

Los métodos de puesta al día deberían aprovechar las técnicas más eficaces, especialmente de la reutilización de textos ya disponibles en formato legible por ordenador. Además, los servicios de informática jurídica deberían esforzarse para garantizar que la información se pusiera en dicho formato de la manera más rápida posible.

4. *Confirmación o revocación de las resoluciones judiciales*

Cuando una resolución seleccionada sea objeto de recurso ante una jurisdicción superior, la existencia de ese recurso deberá señalarse en toda presentación de esa resolución.

En la medida de lo posible, deberá mencionarse la resolución del tribunal superior (confirmación o revocación).

5. *Archivo de las resoluciones*

Los criterios de archivo en los sistemas automatizados de difusión de la jurisprudencia deberían ser claros y simples en la medida de lo posible, y las resoluciones archivadas se deberían memorizar en uno o unos soportes que permanezcan accesibles para los usuarios que lo deseen explícitamente.

Convendría estudiar cómo evitar que se complique la utilización del sistema por la acumulación de una masa creciente de informaciones obsoletas.

Los servicios de información jurídica deberían facilitar la búsqueda documental limitada a resoluciones dictadas después de una fecha fijada.

Anexo a la Recomendación nº R (95) 11
líneas directrices referentes a la selección, el tratamiento, la presentación y el archivo de las resoluciones judiciales en los sistemas de documentación jurídica automatizados

I. *Selección*

1. *Definición*

A los efectos de las líneas directrices reproducidas a continuación, se entenderá por "selección los métodos de elección de las resoluciones judiciales dictadas en un país miembro que se introducirán en los sistemas de bases de datos.

2. *Criterios de selección*

Es deseable que la selección de las resoluciones judiciales se realice respetando los criterios siguientes.

- selección jerárquica: la selección jerárquica consiste en el hecho de seleccionar las resoluciones de una o varias instancias judiciales determinadas en razón de su rango jerárquico dentro del ordenamiento jurídico del país implicado-,
- selección geográfica: la selección geográfica consiste en el hecho de seleccionar las resoluciones de uno o varios tribunales determinados en razón de su situación geográfica,
- selección por la materia del derecho: la selección por la materia del derecho consiste en el hecho de seleccionar las resoluciones judiciales relativas a una o varias materias de derecho- por ejemplo el derecho pena¡, el derecho del medio ambiente, el derecho procesal, el derecho matrimonial, el derecho fiscal, etc.
- selección por el fondo: la selección por el fondo consiste en el hecho de seleccionar las resoluciones judiciales según tengan o no suficiente interés jurídico.

Las líneas directrices siguientes se aplicarán tanto a las resoluciones sobre el fondo como a las resoluciones sobre el procedimiento.

II. *Líneas directrices*

Cuando se realice la selección, se efectuará de modo que se garantice la objetividad y la representatividad de la base de datos.

La selección debería, por una parte, garantizar un acceso amplio y general a la información relativa a las resoluciones judiciales y, por otra parte, evitar la acumulación de informaciones inútiles.

Los criterios de selección definidos anteriormente deberían aplicarse de la manera siguiente:

1. La selección jerárquica es útil para limitar la masa de informaciones susceptibles de búsqueda documental. Este tipo de selección tiene por efecto privilegiar generalmente las decisiones de los tribunales supremos. Sin embargo, hay que tener en cuenta el hecho de que la frecuencia de los recursos puede varias de una materia jurídica a otra y que ciertos tipos de sentencias no son susceptibles de recurso. En consecuencia, no se debería descartar sistemáticamente las decisiones de los tribunales inferiores.

2. Se debería evitar la selección geográfica, a menos que las circunstancias particulares la justifiquen, por ejemplo la existencia de un derecho regional o de jurisdicciones regionales, o en el caso de investigaciones concretas de carácter científico.

3. La selección según la materia de derecho es un medio útil de limitar la masa de informaciones susceptibles de búsqueda documental cuando los sistemas están concebidos para grupos particulares de usuarios. La selección por materias se efectúa normalmente seleccionando las resoluciones que se refieran a una o varias materias de derecho. Un medio de conseguirlo sería almacenar todas las resoluciones dictadas por uno o varios tipos de tribunales especializados - tribunal fiscal, tribunal penal, etc. Los Estados deberían esforzarse en promover la creación de bases de datos relativas a los tipos de informaciones, las materias jurídicas y las jurisdicciones no incluidos ya en otras de datos (*cfr*. Recomendación nº R(83) 3, anexo 1, parte 1, 5.2).

4. La selección por el fondo se debería hacer siempre con una gran circunspección, con el fin de garantizar la objetividad y la representatividad de la selección de las resoluciones. Una resolución presenta un "interés jurídico" cuando expresa un principio de derecho que crea un precedente jurídico, una tendencia de la jurisprudencia en la estimación de los hechos, una nueva práctica procesal, de tal manera que la resolución es o podría ser importante para conocer, de una manera pertinente y detallada, la práctica judicial en la materia jurídica tratada.

Además se deberían tomar en cuenta los elementos específicos siguientes.

Como regla general no se deberían omitir las resoluciones relativas a la evaluación (de la pena, del perjuicio, etc.), así como las resoluciones que traten esencialmente de cuestiones de prueba o de contrato, ya que esos tipos de resoluciones representan, en efecto, elementos importantes dentro de los sistemas jurídicos.

Una resolución que exprese una "jurisprudencia constante" de los tribunales debería representarse con objeto de ilustrar los principios fundamentales de la práctica constante de las jurisdicciones. El almacenamiento de estas resoluciones no debería contribuir a impedir una eventual evolución de la jurisprudencia. En consecuencia, los sistemas de información jurídica deberían almacenar periódicamente las resoluciones conformes u opuestas a una "práctica constante" de los tribunales. Podrían darse las indicaciones apropiadas, por ejemplo, añadiendo anotaciones confirmando o revocando la jurisprudencia.

5. *Criterios de selección suplementarios*

Los criterios de selección pueden ser positivos o negativos. En lo que respecta a los criterios de selección negativos, las resoluciones se pueden descartar:

a. Si los considerandos están redactados según una fórmula formulación que se puede tales como los de un estándar o una cláusula de pura forma, formulación que se puede descubrir con la ayuda de módulos tales como los de un tratamiento de textos,

b. Si las resoluciones que tratan sobre medios o elementos de prueba concuerdan con la jurisprudencia.

Si una selección se revela necesaria en lo que respecta a las resoluciones de las instancias supremas, sería deseable que se utilice el método de selección negativo en todos los ámbitos del derecho.

Se pueden utilizar los siguientes criterios de selección positivos para la elección de las resoluciones:

a. Las resoluciones en las que se explica una noción o un término jurídico, es decir en las que se formula o se modifica una regla de derecho;

b. Las resoluciones en las que el método de interpretación utilizado conduce a una aplicación inusitada de una regla de derecho a un conjunto de hechos;

c. Las resoluciones en las que se expone una argumentación inédita;

d. las resoluciones que tratan de una cuestión relativa a la competencia del tribunal;

e. las resoluciones en las que se expone una opinión concordante o disidente;

f. las resoluciones en las que se pone en cuestión un principio de derecho y/o un conjunto de hechos de interés general.

III. *Puesta en práctica de la selección*

La selección debería efectuarse siempre según las líneas directrices fijadas anteriormente, claramente definidas y fácilmente accesibles para el usuario. Esas líneas directrices se deberían elaborar según los principios indicados en el punto II.

La selección se debería realizar por una o unas personas con cualificación jurídica. La selección por el fondo se debería efectuar recurriendo a una amplia gama de especialistas y garantizando que están representadas opiniones y puntos de vista diferentes. La selección se puede hacer por etapas, por ejemplo, por una preselección.

Esta persona o personas podrían ser jueces, universitarios juristas, fiscales y otros funcionarios. Este grupo de personas podría incluir igualmente a representantes de asociaciones, de revistas jurídicas y de otros servicios de información jurídica.

Si un tribunal de última instancia pide que se introduzca una de sus resoluciones en una base de datos, en principio se la debería incluir.

Es muy deseable la participación de los usuarios en cuanto a la selección y a la elección de los criterios de selección.

IV. *Presentación*

1. *Presentación de las resoluciones (documentos)*

Los documentos se deberán presentar de manera que se garantice una búsqueda segura y rápida.

Las resoluciones judiciales deberían almacenarse, si es posible, bajo la forma de textos originales completos. Además, convendría examinar atentamente las siguientes posibilidades de enriquecer la base de datos:

- cabeceras (head-lines);
- palabras claves (keywords);
- vocabulario controlado (fixed vocabulary);
- abstracts/sumarios (abstracts);
- comentarios: resumen/análisis (*summaryianalysís*)
- anotaciones, por ejemplo referencias a la legislación, a la jurisprudencia, a la doctrina;
- información sobre los recursos y el resultado de los recursos.

2. *Respeto de la vida privada*

Cualquier cuestión de vida privada y de protección de datos personales que se plantee en los sistemas de informática jurídica se debe resolver de acuerdo con el derecho nacional de conformidad con los principios del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio nº 108 de la Serie de Tratados Europeos) y de sus textos subsidiarios.

3. *Acceso*

Se deberían aplicar las líneas directrices de la Recomendación nº R(83)3, anexo, parte 1, puntos 2 y 3, para el acceso de los sistemas de informática jurídica a los textos originales de las resoluciones judiciales, especialmente a los textos existentes en formato legible por ordenador, y para el acceso del usuario a los sistemas de informática jurídica.

338. Datos archivados en sumarios policiales

338.1. Se nominan en esta categoría a los archivos que genera la policía en ejercicio de sus potestades de investigación preliminar. Esta sola característica obliga a ponderar con máxima constricción la posibilidad de almacenamiento y conservación eventual de informaciones personales.

En efecto, el dato personal registrado con fines policiales (por ejemplo, cuando se toman datos de identificación en una "redada") se debe cancelar cuando no sea necesario para las averiguaciones practicadas. En consecuencia, el dato recabado del titular que luego no tiene incidencia para la investigación, debiera quedar suprimido de inmediato; sin embargo es común oír la frase: *está fichado*, expresión que significa haber quedado almacenado en un banco de datos sin especificar.

La ley argentina utiliza una voz inusual en los derechos que concede al afectado. Dice que los datos policiales se *cancelarán*, cuando en realidad debió indicar que deben ser suprimidos porqué el fin que tiene el archivo policial no puede afectar al interesado. También, en su lugar, pudo decir que el dato debiera quedar bajo secreto o en confidencialidad.

338.2. La policía guarda datos sobre origen racial, vida sexual, salud, aficiones, estilo de vida, lengua materna, pertenencia a clubes y asociaciones, así como el código genético de los investigados. Son algunos de otros muchos datos personales que figuran en los ficheros informáticos de la policía de investigación.

En muchos casos, estas informaciones que afectan al ámbito más íntimo de las personas, no se refieren a individuos condenados o procesados, sino a detenidos, investigados, incluidos en atestados, encartados o implicados en hechos delictivos, entre otras expresiones imprecisas.

Estos datos que forman los archivos policiales (que no son de acceso público) tienen carácter temporal; permanecen en las bases mientras dure la investigación. Si es necesario conservar estos u otros datos personales, tiene que registrarlos y estar autorizados por una ley especial, una ley general o la reglamentación precisa para el caso.

En Argentina, el artículo 22 inciso 2 apartado *d)* de la Ley de Protección de Datos Personales, exige la publicación de la estructura básica del archivo, confirmando así la sospecha generalizada de que los bancos de datos policiales contienen información sobre la vida privada de millones de ciudadanos. Con mayor o menor detalle, todos los habitantes de la nación, mayores y algunos menores, como un buen número de extranjeros figuran en al menos uno de los múltiples bancos de datos que utiliza la policía para sus investigaciones y de los que implementa también el Estado nacional a iguales o diferentes fines.

El fichero PERPOL (España) contiene datos personales —incluida la raza, salud y vida sexual— de todas aquellas "personas físicas nacionales y extranjeras que tengan órdenes de búsqueda vigentes o cesadas, que hayan sido detenidas o se haya demostrado su implicación en hechos delictivos o sobre las que haya recaído alguna sentencia judicial por procesos penales". Los ficheros Archivo e Inteligencia —que afectan, respectivamente, a "personas físicas y jurídicas que atentan contra la seguridad pública" y a "investigadas por hechos de tráfico ilícito de drogas"— recogen más de 60 datos personales de cada individuo; entre otros, además de la reiterada alusión a la vida sexual o el origen racial, la "pertenencia a clubes y asociaciones", las "suscripciones a publicaciones y medios de comunicación", los ingresos, rentas, inversiones, hipotecas, seguros, tarjetas de crédito, etc. El fichero ADN incluye el "patrón de bandas ADN"; es decir, el código genético, de todas las personas "implicadas en la comisión de hechos delictivos". En la mayoría de los casos no se explica cómo se han obtenido estos datos, limitándose a señalar que "la información es grabada por los gestores a partir de los hechos investigados". El lugar donde deben indicarse las cesiones de datos previstas a otros organismos aparece casi siempre en blanco, salvo en algunos supuestos, en los que se indica: "A instituciones de carácter oficial con competencia en el ámbito de la seguridad pública" o "A la Agencia, Tributaría".

338.3. Por ello los archivos policiales tienen proyecciones que deben calibrar y equilibrar los derechos en juego: el de seguridad y defensa del Estado, y la protección de la intimidad y el honor de las personas.

Si se opta por la conservación, las medidas de seguridad exigidas deberán ser de nivel alto. Es decir, cuando no se suprimen los datos y simplemente se cancelan para el uso de una investigación (es decir que se pueden conservar entre los antecedentes personales del afectado), la garantía de seguridad técnica deberá ser superior.

Precisamente debido a la naturaleza sensible de los datos personales que se mantienen registrados, se deberán adoptar medidas de seguridad mucho más restrictivas. Por ejemplo, las copias de seguridad deben custodiarse en un lugar distinto al lugar de ubicación de los soportes, y los sistemas informáticos registrar puntualmente todos los accesos. En cuanto al transporte de la información se requerirá autorización firmada del responsable de seguridad y se procederá a la encriptación de los datos para evitar que sean capturados durante el trasiego telemático. Para una correcta implantación de estas medidas de nivel alto será necesaria la implantación de una infraestructura de clave pública en donde se garanticen los principios de intimidad, autenticación y confidencialidad. Siendo por tanto crucial el desarrollo de las autoridades de certificación o terceras partes de confianza, y el de las firmas digitales que influirán de forma positiva al correcto desarrollo de estas medidas de seguridad.

En España se ha firmado un convenio de colaboración de duración indefinida entre el Ministerio del Interior y el Consejo General del Poder Judicial, con el objeto de que los jueces y tribunales puedan disponer directamente de los datos contenidos en la base de la Dirección General de la Policía, sin la tramitación que, hasta ahora, era necesaria para ello. Con esta medida se pretende mayor efectividad a la hora de localizar a personas que estén siendo investigadas judicialmente y se hallen en paradero desconocido, así como mayor rapidez para comunicar a la Policía determinadas situaciones de los encausados tales como órdenes de busca y captura, prohibición de abandonar el territorio nacional,

etc. Lo que se pretende es agilizar un mecanismo ya existente, no modificándose el fondo sino la forma del mismo, por lo que, en principio, no existe vulneración de los derechos constitucionales. Parece una fórmula acertada siempre que no se caiga en abusos que la desvirtúen.

338. 4. En cambio, hay veces que el dato policial deberá ser suprimido como una manifestación clara y puntual del derecho al olvido que tiene toda persona afectada por un pasado al que no puede quedar prisionero.

Como ejemplo de ello señala Pablo Palazzi,[133] el leading case estadounidense *Melvin v. Reid*. Allí, la actora, cuyo nombre original era *Gabriel Darley*, había ejercido la prostitución y había estado involucrada como imputada en un juicio por homicidio. Después de haber sido absuelta logró abandonar la vida licenciosa que llevaba, casarse con un hombre llamado Melvin y con este comenzó a llevar una vida decente y respetable, entablando nuevas amistades con gente que desconocía su pasado. Siete años después se estrenó una película, *The Red Kimono*, donde se narraba la verdadera historia, con su nombre original, lo que reveló su pasado a sus actuales amistades y que en definitiva terminó arruinando su vida. La actora accionó por invasión a la privacidad y el tribunal, basándose en una cláusula constitucional del estado de California que otorgaba a todos los hombre el derecho de "procurar y obtener la felicidad", hizo lugar a la demanda.

El hecho en definitiva consistió en el uso sin autorización del anterior nombre de la actora para hacer una película sobre su vida pasada. El tribunal entendió que se estaba revelando un hecho que era verdadero, pero juzgó que el uso innecesario del nombre de la actora y la revelación de su pasado a sus nuevos amigos y asociados introdujo un elemento que en si mismo era una transgresión a su derecho a la privacidad.

Es decir que se concluyó que el uso y difusión de un dato verdadero puede ser violatorio de la intimidad y reserva de un individuo, cuando éste tiene cierta antigüedad.

En síntesis, las opciones no registran antecedentes en nuestra legislación, pero admiten comparar el hecho con los llamados "*Acuerdos de Schengen"* que tienen por objeto preservar el orden y la seguridad del Estado, controlando la circulación de personas por los países europeos adherentes a este sistema de intercambio informativo. Los ficheros que se implementan, denominados "Europol" se conservan durante el tiempo necesario para el cumplimiento de sus fines, los que se estiman nunca superiores a tres años desde la introducción del dato, salvo que la autoridad de control sugiera su renovación.

Si no se decide la prolongación del dato —explica Gils Carbó— ellos se suprimen automáticamente, pero si un Estado miembro suprime datos en sus ficheros nacionales que hayan sido transmitidos a Europol deberá informarlo para que ésta los suprima, o decida conservarlos si son de interés. Por último, no se procederá a la supresión cuando pueda perjudicar intereses dignos de protección de la persona de que se trate, en cuyo caso, sólo se utilizarán los datos con su consentimiento.[134]

---

[133] PALAZZI, Pablo, *El habeas data en la Constitución Nacional (La protección de la privacidad en la "era de la información")*, en Jurisprudencia Argentina del 20 de diciembre de 1995.

[134] GILS CARBÓ, Alejandra, *Régimen legal de las bases de datos y habeas data*, La Ley, Buenos Aires, 2001, pp. 76 y ss.

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

339. Datos públicos y privados

339.1. La dualidad entre dato público (expuesto) y privado (secreto y/o confidencial) presenta la misma diatriba entre aquello que el público tiene derecho a conocer y lo que el hombre tiene derecho a conservar para sí mismo.

Derecho a la información versus derecho a la privacidad son términos aparentemente contrapuestos en esta presentación.

Por otra parte, la intimidad personal antaño considerada como "el derecho a estar en soledad", permite inferir un término donde las acciones particulares obran determinantes para esa posibilidad de aislamiento, porqué si es la misma persona quien ocasiona la publicidad de sus actitudes y comportamientos, puede existir una provocación a la exposición pública.

339.2. Al menos, la notoriedad, fama, o el reconocimiento general, significa que respecto a ese alguien la gente conoce más, lo cual no autoriza a invadir la esfera de secreto, reserva o intimidad que el hombre público quiera preservar. El problema será si lo puede conseguir.

> Es evidente que hoy —dice Concepción Rodríguez— la intimidad es el bien más amenazado y desprovisto de una enérgica tutela en todas sus facetas. El interceptar conversaciones, el revelar datos personales que constan en determinados registros para unos fines; el captar imágenes con aparatos apropiados, sin que se aperciba de ello la persona fotografiada, etc., es noticia usual. La intimidad debe ser protegida en todas las personas, sin que sea lícito discriminar, en principio, a las que gozan de fama pública o actúan en la vida pública. Sin embargo, hay que atender a la esfera que, por sus propios actos, mantenga la persona reservada.[135]

Pongamos como ejemplo la noticia de la internación de Diego Maradona en Cuba, donde la prensa efectuó un pormenorizado relato de las adicciones padecidas y el tratamiento que se aplicaron. Evidentemente, una demanda eventual contra los medios de comunicación podría ser posible por la intromisión y divulgación de las acciones personales tomadas por el conocido futbolista, pero nunca sería factible por difamación, porqué en los hechos que estudiamos, importa más la exposición abierta

[135] CONCEPCIÓN RODRÍGUEZ, ob. cit., p. 86.

de hechos privados de la persona pública antes que la veracidad de la información ofrecida.

339.3. Ahora bien, este caso es un supuesto de invasión a la privacidad, pero ¿cómo se aplica el principio respecto a datos personales?

Es necesario advertir que la persona pública, *lato sensu*, tiene un historial más conocido que las personas comunes. Se sabe y conocen detalles de su vida, sus actos, circunstancias caracterizadoras, etc. Es probable que cada uno de estos comportamientos se encuentre guardado en un archivo periodístico (que es, en definitiva, una base de datos).

Sobre esta base hipotética ¿qué diferencia existe entre la noticia que versa sobre aspectos clínicos del tratamiento de Maradona, respecto a otro interno por similares adicciones?

Parece claro que la exposición de uno (la fama) trasciende más que la del ignoto, aunque le afectación sea idéntica en el grado de bochorno que produzca la invasión a información tan sensible.

> Cuando el titular del honor lesionado —dice Concepción Rodríguez— resulta ser un *personaje de proyección pública*, existen ciertas particularidades no ya porque su honor sea distinto al de cualquier persona, sino porque la esfera de protección que le dispensa el Derecho es menor, por cuanto, la opinión pública, en aras de la libertad de información, tiene derecho a conocer los datos relativos a aquéllos, facultad que cobra toda su trascendencia con relación al derecho a la intimidad.[136]

339.4 Por eso, sostener que existe un *dato público* cuando la persona *es pública*, compromete seriamente la tutela prevista para el tratamiento de informaciones sobre la vida personal. De igual modo, no se podría afirmar que el *dato es privado* cuando la persona es común y su grado de exposición pública sea mínimo.

En ambos casos, la defensa de la intimidad es la misma, y el derecho a proteger los datos personales no cambia.

> Observado desde otro punto de vista, suele transportarse el problema a la distinción entre información pública e información privada. En efecto, la información pública sería aquella que es de público conocimiento. La privada, por el contrario, es la que permanece constreñida a la intimidad de las personas o al conocimiento de un círculo de personas limitado. El conocimiento de la información podría ser un criterio de delimitación de la información pública, dice Sánchez de Diego, pero a su vez, establecer el grado necesario para que una información sea calificada como pública presenta innumerables dificultades [...]. Se puede variar el enfoque y considerar que no es tan importante los indicadores cuantitativos como cualitativos. En este sentido una información sería pública cuando se tiene conocimiento de ella por personas ajenas al origen de la información o cuando es de fácil adquisición o está a disposición del público. En definitiva, establecer un nivel de conocimiento público que determine con claridad cuando una información es pública es sumamente dificultoso. Lo cierto es que cuando un hecho es de conocimiento público, más que información pública se trata de *información publicada*. Y que, sin lugar a dudas,

[136] CONCEPCIÓN RODRÍGUEZ, ob. cit., p. 87.

> una información puede considerarse publicada cuando ha sido difundida por los medios de comunicación social.[137]

339.5. No obstante, una variable es considerar que existen *datos públicos* cuando la fuente de información es de fácil acceso; y *datos privados* cuando el sondeo tiene carácter confidencial o secreto.

Por ejemplo, el acceso a la información judicial es simple y difundida hacia todos, pero el lamentable archivo de abogados que llevaba la Cámara Federal de apelaciones en lo criminal y correccional (sobre comportamientos procesales que, en su caso, debieran ser considerados por el Colegio profesional) era un registro privado de circulación restringida. En el caso, existe con ese banco de datos una afectación a la esfera de intimidad, porqué los derechos fundamentales de cada uno coexisten con los llamados derechos personalísimos que tienen una protección especial, o al menos, la merecen. Y por tanto, el honor, la privacidad, la imagen personal o el prestigio profesional son un patrimonio de la persona.

339.6. Otra proyección puede darse cuando con los datos privados que se hacen públicos se persigue lograr beneficios económicos especulativos, merced a la exposición de la persona notoria o famosa.

Aun cuando también aquí hay que establecer diferencias, como lo hizo el Superior Tribunal de Justicia de España al tratar la afectación de un funcionario público que se sintió perturbado en su derecho a la propia imagen. Sostuvo el Alto Tribunal que:

> …quien ejerce un cargo público o una profesión de notoriedad o proyección pública tiene derecho a su propia imagen y a su intimidad, cuando elude su presentación en un acto público o en lugares abiertos al mismo, pues si consta el decidido propósito de eludir la exposición al estar en una playa alejada de la gente y alejada de los núcleos de población y que, vestida sólo con una pieza inferior de su traje de baño, es fotografiada con teleobjetivo sin su consentimiento, fotografías que tomadas por un profesional son vendidas a una revista donde son publicadas, debe salvaguardarse su intimidad que tan subrepticiamente fue vulnerada.

Identificar el dato desde la condición pública o privada de la fuente de información es el temperamento de la ley de protección de datos española que divide entre ficheros de titularidad pública y ficheros de titularidad privada. Lo característico, en esta clasificación, es el dominio del dato antes que la identidad de la persona.

Sostiene Sánchez de Diego que:

> este nuevo criterio explica que las informaciones divulgadas por quienes son origen de una información se convierten en informaciones públicas, desde el momento en que difunden y, por tanto, desde que pierden el dominio, la posesión. Este criterio —agrega— es también perfectamente aplicable en los casos de bases de datos, en donde la posesión de la información procede de la titularidad de los medios de almacenaje y recuperación de la misma, esto es, la titularidad de la base de datos. En principio, la titularidad de una

---

[137] GOZAÍNI, *Derecho Procesal Constitucional – Habeas Data (Doctrina y Jurisprudencia),* cit., p. 344.

base de datos por un particular o por una entidad pública determinaría la cualidad de la información, en cuanto pública o privada. Y todo ello con independencia del tipo de información de que se trate: datos personales de un alumno, datos estadísticos, informes de personal, movimiento de cuentas bancarias, test de eficacia de vehículos, diligencias judiciales, etc.[138]

340. Clasificación de los datos

340.1. La información personal que registran los archivos proviene de fuentes *directas* (datos voluntariamente prestados por su titular) o *indirectas* (adquisición de otras bases; interconexión; transferencias, etc.) que determinan el origen o lugar de procedencia.

Esta diferencia es importante para resolver el tema de la notificación de los derechos que tiene la persona al incorporar sus datos a un registro público o privado. Si el dato se otorga de manera directa la comunicación ha de ser inmediata; mientras que en el segundo caso se debe asegurar el conocimiento de los derechos bajo apercibimiento de aplicar el órgano de control las sanciones correspondientes.

340.2. Los datos se pueden clasificar con los siguientes criterios:

Por la identificación del titular del dato, se divide en:

a) *Nominativo:* es el dato de una persona física o jurídica conocida e identificada.

Uicich sostiene que dato nominativo es aquél que está referido a una persona determinada. Y lo divide de acuerdo a como se llegue a identificar a la persona en: *a)* directos: cuando lo identifica sin necesidad de proceso alguno, *b)* indirectos: cuando permite la identificación pero no lo hace en forma directa sino agrupando datos.[139]

El Consejo de Europa en el Convenio emitido en el año 1981 aclaró que la protección de datos personales sólo corresponde a las personas físicas independientemente de que ellos se manipulen por administraciones o empresas; pero que las personas ideales son amparadas con relación a informaciones que vinculen a grupos de personas, asociaciones, fundaciones, sociedades, organizaciones comerciales u otros similares, tengan o no personería jurídica.

Para Velázquez Bautista:

el Convenio se aplica a todo tipo de ficheros que contuvieren datos sobre personas físicas, con independencia de quien los trate, salvo las excepciones establecidas; de esta forma se llega a "el reconocimiento de un derecho individual de acceso a los ficheros de personas jurídicas en el supuesto de que las informaciones registradas fueren utilizadas con miras a adoptar una decisión que pudiere ser invocada en contra de la persona interesada (por ejemplo, denegación de un crédito, de un seguro, etc.).[140]

---

[138] SÁNCHEZ DE DIEGO, ob. cit., p. 34.

[139] UICICH, ob. cit., p. 123.

[140] VELÁZQUEZ BAUTISTA, Rafael *Protección jurídica de datos personales automatizados,* Colex, Madrid, 1993, p. 66.

La identificación más simple o sencilla, supone que del individuo se tengan datos provenientes de su documento o él mismo aporte otros que permitan conocerlo sin ninguna dificultad ni probabilidad de error. En cambio, si para identificar la persona se deben aplicar procesos, el dato compilado seguirá siendo nominativo pero indirecto.

b) *Innominativo o anónimo:* es el dato de uso estadístico o científico que no identifica a persona alguna porque la información archivada no se refiere a él sino a sus actividades.

Es información tomada a un cierto fin y no se puede utilizar ni aplicar para otra cosa incompatible con ella.

Por la confidencialidad de la información pueden ser:

a) *Datos que no afectan la sensibilidad de las personas*: se trata de aquella información irrelevante o anodina que por las características que tiene no permiten herir los sentimientos más íntimos de la persona relevada ni afectar su derecho a la privacidad. Es el dato rutinario, el que se ofrece sin complicaciones o se obtiene de fuentes fácilmente accesibles.

Sin embargo, hay que tener mucho cuidado con afirmar que el dato irrelevante no afecta el derecho a la intimidad, porqué hemos visto como se puede procesar la información y lograr de ella perfiles y costumbres cambiando las reglas de la colección (*v. gr.:* caso de los directorios telefónicos).

> Esto pone de manifiesto —según Orozco Pardo— que un dato es inocuo o sensible, no ya por su contenido, sino por el uso que de él se haga, pues como señala Castell (*La limitación informática*, en Estudios sobre la Constitución Española, editorial Cívitas, Madrid, 1991), "la interconexión de ficheros, la libre utilización de los datos, producen la teoría del mosaico, por el que datos *a priori* irrelevantes, pueden servir para una finalidad diferente y, por lo tanto, proporcionar claves insospechadas sobre una determinada persona". En tal sentido, la postura más lógica, que sostiene la jurisprudencia alemana, es la de no establecer diferencias entre los datos, atendiendo fundamentalmente al contexto y finalidad con que se utiliza. Por ello, una norma eficaz ha de atender, no al contenido en concreto del dato desligado de cualquier otro elemento, sino utilizar criterios flexibles adaptables a los supuestos y contextos concretos del caso.[141]

b) *Datos que afectan la sensibilidad de las personas*: son los que de difundirse ponen en conocimiento de quien los conoce, datos de contenido privado que, salvo manifestación expresa del afectado, socavan la intimidad de las personas.

El dato sensible, como es conocido en la doctrina y legislación que lo aplica, se divide en dos campos: Uno refiere al objeto de protección, propiamente dicho; el otro, a la garantía que tutela estos datos y el nivel de protección que merecen de acuerdo al grado de sensibilidad que se le atribuye.

---

[141] OROZCO PARDO, Guillermo, "Los derechos de las personas en la Lortad", en *Revista Informática y Derecho*, números 6/7, UNED, Mérida, 1994, p. 154.

> Herrán Ortiz diferencia entre datos sensibles de criterios sustantivos o distinguidos por su contenido; de datos sensibles formales que tienen una garantía establecida con relación al nivel mayor o menor de protección que ampara a los mismos. En otras palabras —agrega— frente a los denominados datos especialmente sensibles, referidos a informaciones relacionadas con la libertad de ideología o creencias religiosas y que en su contenido afectan a lo que puede considerarse el "alma o interior mismo" de la persona, se reconoce la existencia de unos datos sensibles, referidos a informaciones de carácter material de la persona, que no por ello dejan de ser privados o personales, pero que afectan al comportamiento o a cuestiones más "externas" de la persona —origen racial, comportamiento sexual o salud— que sin dejar de ser privadas, y por ende sensibles, que con frecuencia se referirán a aspectos de la persona fácilmente perceptibles a los ojos de los demás, y para los cuales el tratamiento automatizado no representa un atentado tan grave a la intimidad de la persona, salvo que además de su conocimiento se proceda al tratamiento automatizado de los mismos, y constituyan elementos decisorios o de simple discernimiento en la adopción de decisiones que afectan a la persona.[142]

El dato sensible se refiere a la salud, la condición racial y social, los pensamientos, hábitos y costumbres de la persona. Suelen establecerse categorías entre ellos con el fin de adecuar la protección al nivel de divulgación o exposición que puedan tener.

Un primer grupo se refiere a los *datos sobre ideología, religión o creencias,* que se consideran "especialmente sensibles"; ellos que no pueden hacerse públicos salvo expresa autorización del afectado. Inclusive, aun siendo obligatoria la prestación de datos, esta información está excluida por el carácter particularmente íntimo que tienen.

El segundo grupo se vincula con los *datos sobre el origen racial, la salud y la vida sexual*, que como en el caso anterior no se pueden registrar salvo que el individuo lo permita.

El tercero se relaciona con la historia personal de la persona en su vida social, destacando los *datos sobre infracciones administrativas o antecedentes penales* que tienen reglamentos especiales como veremos de inmediato (*v. gr.:* Registro de antecedentes personales; Registro o fichero de morosos; deudores fiscales, etc.).

En conjunto estos datos constituyen el objeto material a proteger, pero la garantía suele variar por la naturaleza del perjuicio, obligando, en consecuencia, a una labor de interpretación del órgano —judicial o administrativo— encargado de aplicar el reglamento establecido.

> Toniatti hace una distinción partiendo de unos "datos personales irrelevantes o de rutina", sustraídos a éste régimen normativo especial. Posteriormente, desde un punto de vista material entiende por *datos sensibles* "aquellos que más directamente se refieren sea a la esfera personal e íntima, sea a la titularidad de los derechos fundamentales de la libertad", en tal sentido, cabe citar e las creencias religiosas, opiniones políticas, salud, antecedentes

---

[142] HERRÁN ORTIZ, ob. cit., p. 88.

penales, origen racial, vida sexual, etc. Por último, habla de unos *datos supersensibles o sensibilísimos*, para atender a una categoría especial en la que el ordenamiento excluye incluso al propio interesado y el ejercicio de sus medios de control para el acceso, corrección, etc. Se trata esencialmente de datos personales clasificables desde el punto de vista material como ordinarios y sensibles que se cualifican ulteriormente por su presencia en archivos destinados a finalidades de orden particular y de valor preeminente, entre los que destacan, en primer lugar, la protección del orden público y de la seguridad nacional y, en segundo lugar, la intimidad en materia sanitaria.[143]

Por la mayor o menor complejidad para lograr el dato se clasifican en:

a) *Datos públicos o fácilmente conocidos*

La información personal que se encuentra disponible para cualquier interesado por encontrarse en registros o lugares de fácil acceso al público, no tiene derecho al reclamo de protección a través de la ley reglamentaria o del proceso constitucional específico (*habeas data*).

La limitación se da cuando estos datos no sufren restricción alguna para su conocimiento y difusión, por ejemplo, resultados de censos, anuarios, bases de datos de registros oficiales, repertorios de jurisprudencia, archivos de prensa, directorio de teléfonos, y todo otro dato de similar registro.

Sin embargo la afirmación no puede ser rotunda, porqué existe información contenida en esos archivos que aun siendo expuestas y como tales divulgadas, necesitan mantener la actualidad del archivo y la proporcionalidad de sus fines.

Es decir, cualquier afectado puede reclamar la puesta al día de esa información si ella le produce un menoscabo en sus derechos subjetivos; los que deberá probar para acceder a la sentencia favorable.

Mientras que otros registros similares por su carácter público, pero restringidos por el fin al que se crean, no pueden tener la exclusión dicha con anterioridad.

En efecto, los ficheros profesionales, por ejemplo, se pueden dar a publicidad en el marco de necesidad que justifique la petición, pero nunca difundirse con fines publicitarios, por ejemplo.

> En otras palabras, dice Herrán Ortiz, la relación de miembros de grupos profesionales admite su publicación con fines y objetivos concretos propios del grupo, pero no con el propósito de utilizarlos en forma indiscriminada por terceros, fuera del ámbito profesional de que se trate.
>
> Así el dato accesible al público lo será cuando la fuente sea pública con carácter general, pero no cuando la misma tenga como fundamento un fin predeterminado y establecido entre quienes consienten la publicidad de dichos actos, ya que dicho consentimiento obedece a un interés de la propia persona de darse a conocer dentro del grupo profesional y a esos solos efectos.[144]

---

[143] TONIATTI, Roberto, "Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada", en R.V.A.P., nº 29, 1991, pp. 65 y ss.

[144] HERRAN ORTIZ, ob. cit., p. 158.

b) *Datos privados, secretos y confidenciales*

La distancia entre el dato público y el privado es la misma que suele efectuarse con las relaciones humanas, es decir, los comportamientos son públicos o privados no en sí mismos, sino en atención al espacio en que se desenvuelven.

Dato privado sería aquél que la persona quiere conservar en la reserva de su intimidad. Es el dato oculto, aquél que sólo conoce la persona y que será secreto únicamente mientras esté en el reducto de lo personal, exento de toda curiosidad.

Es este un dato imposible de filtrar y por ello no cuenta en el problema de protección o defensa que merece.

El motivo es obvio. Si el dato se revela a otro, sale de la esfera de intimidad para ocupar a alguien más quien participa de la confidencialidad. Comienza así una proyección del dato privado, que es el *dato secreto* que debe custodiarse en la medida que el deber de secreto constituye una de las manifestaciones del derecho a la intimidad.

Dice Herrán Ortiz que:

> el secreto se caracteriza, además de por el deber de ocultamiento, por constituir un concepto fundado en las relaciones intersubjetivas. El secreto implica ocultación de "algo", pero la misma se ha de efectuar en relación a un grupo de personas, si bien éste será generalmente reducido. Por ello, no se puede conceptuar ni constituir el secreto en relación con la propia persona, ni nace de la interioridad del sujeto, más bien, se traduce en la existencia de una comunicación que se pretende preservar.[145]

Dato confidencial es el que por su alta sensibilidad no se puede divulgar ni transmitir a terceros. Cuando el dato está en un banco o archivo la reserva es una obligación que convierte en responsable directo a quien produce la revelación.

La línea entre las tres clases de datos es muy fina, pero queda esclarecido el ámbito de protección con el derecho a la privacidad, el cual interesa al honor, la imagen, la intimidad más recóndita y aquellos sectores de la vida que sin resultar secretas, merecen sin embargo, el respeto de todos, porque el derecho que cada uno tiene a que se respete su esfera privada garantiza la inviolabilidad de la vida particular.

Por la subjetividad o pertenencia del dato se clasifican en:

a) *Datos personales existenciales*

Se denomina así a los datos que se relacionan con definidores de la personalidad tales como el natalicio, lugar de origen, estado civil, domicilio actual y profesional, entre otros.

Heredero Higueras es el autor de esta clasificación. Para él:

> *dato existencial* es el nacimiento, fallecimiento, matrimonio, divorcio, domicilio, actividad profesional, patrimonio, afiliación política o sindical, confesión religiosa, desplazamientos, enfermedades o encarcelamiento. Estos constituyen una "masa de datos" que no tienen carácter personal cuando no puedan ser asociados a personas determinadas o determi-

[145] HERRAN ORTIZ, ob. cit., p. 160.

nables. Asimismo es dato personal *no existencial* las informaciones referidas a condiciones personales o materiales relacionadas con cosas o bienes de las personas.[146]

b) *Datos personales no existenciales*

Son aquellos vinculados con el patrimonio económico y con la pertenencia de cosas que identifican. La ley alemana hace esta distinción al referir a "condiciones personales y materiales" de la persona.

Por el secreto que guardan

Los datos secretos y/o confidenciales conservan una categoría propia observada en relación con alguien que debe preservar el deber de ocultación.

El dato secreto puede ser *profesional*, al estar asentado en una base de datos que supervisa y ordena quien a recibido la información como consecuencia de su desempeño en una profesión determinada.

El caso de abogado que registra cada etapa del procedimiento que involucra a una persona o personas, anotando cuestiones que le fueron dadas en confidencia; o del médico que elabora la historia clínica; o del psicólogo que anota detalles de la personalidad del individuo, son manifestaciones del secreto profesional que no se pueden revelar.

En esta materia, el tratamiento de datos obliga a conservar el secreto a quienes hayan trabajado en las bases de datos y, por ello, tomado conocimiento de la información personal archivada.

El *dato militar* es secreto cuando pone en riesgo operaciones de logística o compromete la seguridad del Estado al hacer público el armamento disponible, la campaña diseñada, el planeamiento estratégico, la adquisición de material, etc.

La nueva ley de tratamiento de datos española establece en el artículo 22 sobre *Ficheros de las Fuerzas y Cuerpos de Seguridad*.

> 1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley. 2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad. 3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales. 4. Los datos personales registrados con fines policiales se cancelarán

[146] HEREDERO HIGUERAS, ob. cit., p. 79.

cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

El dato secreto puede estar en documentos oficiales, los que quedan restringidos del derecho de acceso con la excepción que se otorgue específicamente para ello.

Sección 5ª ⋮ Los archivos de datos personales

341. Evolución y desarrollo de los archivos de datos personales

341.1. En la historia del mundo la recopilación de información concerniente a las personas ha sido una práctica constante vinculada con políticas demográficas, culturales y de todo tipo. Poco ha cambiado aquél sentido solo que ahora se aplica a una diversidad de situaciones que penetran el tejido de aquello que una persona quiere o consiente transmitir.

En la evolución de los archivos se verifica un cambio importante que proviene del desarrollo tecnológico y de las ciencias de la información.

Perez Luño dice que:

> en otros períodos históricos el progreso de la ciencia y de la técnica venía entendido, las más de las veces, como aportación al desarrollo de la humanidad en términos cuantitativos y, por ello, independiente respecto a los valores. Por el contrario, el signo distintivo de nuestra época es que en ella el progreso tecnológico se halla inescindiblemente ligado a elecciones o valoraciones éticas y políticas. Ello obliga a someter cada innovación tecnológica al correspondiente *technology assesment,* esto es, a una tasación crítica de sus consecuencias. A esta exigencia son especialmente sensibles las sociedades más desarrolladas. En ellas se teme el coste que, para el disfrute de los derechos fundamentales, puedan representar determinados progresos tecnológicos e, incluso, se ha llegado a aludir, en algunos sectores de la teoría social anglosajona, al peligro de una contaminación de las libertades en el seno de las sociedades tecnológicamente avanzadas.[147]

341.2. El derecho a la intimidad está ahora acosado por la transformación y el progreso de las herramientas técnicas. Inclusive, la información sobre las personas constituye un dato relevante y revelador de las fuentes de conocimiento sobre el desarrollo de la sociedad.

La posibilidad de aislamiento, otrora posible, está afectada por la intromisión permanente de los medios en el hogar, los que son inevitables y paradójicamente imprescindibles.

El dilema no es la perturbación en sí misma, tampoco la invasión en el reducto privado del ambiente familiar. El problema es que cuando se obtiene un dato y se lo asocia a otro, comienza a elaborarse un perfil de la persona, o del grupo al que pertenece, o también, interesando la sociedad donde está inserto.

---

[147] Pérez Luño, Antonio, *Ensayos de informática jurídica*, Fontamara, México, 1996, p. 11.

En definitiva, se ha producido un tratamiento (procesamiento) de los datos que posteriormente se recopilan, se compendian y archivan para darles un destino del cual, esas personas quizás jamás tengan conocimiento.

> Es cierto —recuerda Estadella Yuste— que antes de la era del ordenador ya se utilizaron archivos manuales con información personal, los cuales fueron usados por ciertas autoridades nacionales para repetidos intentos de aniquilación de un sector de la sociedad, por ejemplo, en Alemania por Hitler, Por esta razón, la automatización de ficheros de datos personales es vista, muy a menudo, con cierto recelo.[148]

341.3. El avance tecnológico le permite al hombre común que disponga de interés para conseguirlo, la posibilidad de tomar fotografías desde puntos tan lejanos que serían imposibles de captar desde el objetivo; se pueden escuchar conversaciones a distancia; se testimonian hechos por la reconstrucción computarizada; y, entre tantas más, se levantan datos y registros de personas con la finalidad de formar archivos que dan las características generales de la sociedad donde se vive.

Muchas veces estas actividades no tienen el consentimiento o el sometimiento voluntario de las personas a quienes se afecta. Aparece así la manipulación y la introducción de la técnica en la vida íntima de los hombres, agrediendo en consecuencia, la esfera de sus libertades individuales.

Algunos afirman que es recién en los años sesenta del siglo XX cuando se advirtió la amenaza que la intimidad personal sufría por las nuevas tecnologías, comenzando un proceso de legislación internacional, regional y local que sigue hasta nuestros días.

> Los derechos humanos han sido objeto, a lo largo de la historia, de una serie de mutaciones que les permiten ser clasificados por generaciones. Tal como Perez Luño ha puesto de manifiesto, la primera generación correspondería a los derechos humanos considerados como derechos de defensa de las libertades del individuo, es decir, los que exigen la no injerencia de los poderes públicos en el ámbito privado; la segunda generación corresponde a los derechos económicos, sociales y culturales, los cuales requieren una política activa de los poderes públicos para garantizar tales derechos; y en la tercera generación se encontrarían los derechos humanos que complementan las libertades individuales y los derechos sociales, es decir, son los que se presentan como una respuesta al fenómeno de la contaminación de las libertades; dentro de esta categoría se destacarían el derecho a la libertad informática o protección de datos, derechos de los consumidores, etc.[149]

341.4. El desarrollo normativo, no obstante, ha debido equilibrar la importancia que tiene la acumulación informativa a los fines de la organización política (por ejemplo, planificación estratégica, política fiscal, economía social, estadística, etc.) con la protección del hombre en su derecho a la privacidad, que constituye, por estos tiempos, un avance moderno de la libertad de intimidad.

---

[148] ESTADELLA YUSTE, *La protección de la intimidad frente a la transmisión internacional de datos personales,* cit., p. 73.

[149] PEREZ LUÑO, ob. cit., p. 17.

342. Regulación y legislación

342.1. La elaboración de un conjunto de leyes que se haga cargo del problema enfrentado con las bases de datos, puede clasificarse a grandes rasgos, en tres sistemas:

a) El sistema internacional
b) El sistema regional
c) El derecho interno (constitucional, legislativo y jurisprudencial)

El primero de ellos es una proyección sobre la inteligencia que cabe asignar a las cláusulas que tienen, sobre el tema del derecho a la intimidad, las convenciones internacionales.

Tomemos por ejemplo el caso de la "*Declaración Universal de Derechos Humanos*" (1948) que declara su fe en los derechos fundamentales del hombre, en la dignidad y el valor de la persona humana y en la igualdad de derechos de hombres y mujeres, expresando la resolución de la comunidad universal de elevar el nivel de vida dentro de un concepto más amplio de libertad.

La Resolución 217 A (III) del 10 de diciembre de 1948 consagró el derecho de todo individuo a la libertad de opinión y expresión, incluyendo en esa garantía, el derecho a no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, el de difundirlas sin limitación de fronteras por cualquier medio de expresión.

342.2. Sin embargo, entre libertad de información y derecho a la intimidad hubo roces inevitables, los que sólo pueden remediarse a través de una lectura inteligente de las cláusulas. Ese fue el paso que dieron los sistemas regionales.

En el seno del Consejo de Europa, en 1967, se creó una comisión consultiva para estudiar el impacto de la tecnología informativa en los derechos de las personas, dando lugar la investigación a la Resolución 509 sobre "*los derechos humanos y los nuevos logros científicos y técnicos*". A partir de esta decisión el Comité de Ministros elaboró una serie de reglas relativas a la protección de la vida privada de las personas físicas respecto a los bancos de datos electrónicos en el sector privado y otra similar pero referida a los bancos de datos del sector público. En ambos casos, se debía armonizar entre el derecho a ser informado y a tener una vida privada, a cuyos efectos se dieron las pautas siguientes:

- La información debe ser exacta, mantenida al día, apropiada para el fin para el que fue almacenada y obtenida por medios legales.
- Todo ciudadano tiene derecho a conocer la información archivada sobre sí mismo.
- Las personas que deben operar sobre las bases de datos tienen que estar bajo severas normas de conducta para el mantenimiento del secreto y para poder prevenir el mal uso de los datos.
- La seguridad debe ser extremada al máximo para impedir el acceso a las bases de datos a personas no autorizadas o para evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos.

- Si la información va a ser utilizada con fines estadísticos se revelará de tal forma que sea totalmente imposible relacionarla con ninguna persona en particular.

342.3. Tiempo después de da el "*Convenio para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal*" (Estrasburgo, 1981) conocido como Convenio 108, el cual fue largamente demorado en su ratificación por los estados partes.

El mismo ordenó que, una vez que se pusiera en vigor el Convenio, se constituiría un Comité Consultivo. Cada Parte tendría un representante y un suplente en dicho Comité. Cualquier Estado miembro del Consejo de Europa que no sea Parte del Convenio poseía el derecho de hacerse representar en el Comité por un observador.

La aprobación del Convenio 108 fue una reacción por parte del Consejo de Europa al creciente volumen de procesamiento automático de datos personales como consecuencia de los avances en la tecnología de la información y los medios de mantenimiento y tratamiento de la misma en forma digital.

Los principios establecidos se refieren, en particular a la distribución justa y legal la recogida y el tratamiento de los datos personales, la recolección de los datos personales únicamente con objetivo específico y fines legítimos, que excluye el tratamiento de los datos para otros fines, incompatibles con aquellas para las que la datos han sido recolectados, la limitación del tiempo para el tratamiento de los datos después de lograr los fines estipulados, etc. El objetivo del Convenio 108 fue fortalecer la protección de datos personales relativos a personas específicas.

Después de 1970 los países europeos comenzaron a adoptar normas legales para la protección de los derechos fundamentales de las personas y, en particular, se preocupó por la tutela del derecho a la intimidad, incluida la defensa contra desproporcionados de recolección y tratamiento de datos personales. En 1970 el estado de Hessen (Alemania) aprobó la primera ley sobre la protección de datos personales en el mundo. Fue seguida por Suecia (1973), Alemania (Ley Federal, 1977), Francia (1978) y otros países. Cinco años después de la publicación de la Resolución 74 (29), una serie de países habían adoptado legislación para la protección de datos personales (además de los nombrados anteriormente que incluyen Alemania, Austria, Dinamarca, Luxemburgo y Noruega). Tres países incluyen la protección de los datos de sus derechos constitucionalmente garantizados (Portugal, España y Austria). Algunos estados han centrado sus actividades legislativas sólo en los datos procesados por computadoras. Otros se acercaron a este problema en un contexto más amplio; la ampliación de la protección al tratamiento de datos personales por cualquier medio técnico.

La experiencia internacional, sin embargo, poco a poco demostró que la protección de los datos personales no podía ser dirigida exclusivamente a nivel nacional solamente. El creciente volumen de las transferencias de datos personales entre los países, la creación de bancos de datos nacionales, el aumento progresivo de circulación de personas independientemente de las fronteras estatales, el engrandecimiento de la cooperación internacional con respecto a la ciencia y la investigación, puso

nuevos requisitos sobre la coordinación internacional con el fin de proteger los datos personales.

Fue necesario, entonces, unificar los principios de protección de datos personales y definir de manera uniforme los riesgos que se derivan de su libre transferencia. Estas necesidades son también los motivos que tiene la Organización para la Cooperación y Desarrollo Económicos (OCDE, que elaboró en 1969 un estudio sobre la transferencia de datos a través de las fronteras estatales para atender a las necesidades del sector público). El 23 de septiembre de 1980 la organización emitió las Directrices de Administración la Protección de la Privacidad y Flujos Transfronterizos de Datos Personales.

OCDE cooperó en la preparación de este documento con el Consejo de Europa, que en ese momento ya había elaborado un proyecto de convención sobre la privacidad. Este documento por primera vez define los términos que después se utilizaron en todas las normas jurídicas.

Hay varios instrumentos del Consejo de Europa para la aplicación principios de protección de datos en la práctica diaria (por ejemplo, recomendaciones, informes, dictámenes).

342.4. En Estados Unidos de América, en 1974, se sanciona la "*Privacy Act*" que reza en su exposición de motivos:

> El Congreso estima que la privacidad de un individuo es afectada directamente por la captación, conservación, uso y difusión de información personal por entes y órganos federales…, el creciente uso de ordenadores y de una tecnología compleja de la información, si bien es esencial para el funcionamiento eficiente de las administraciones públicas, ha aumentado sensiblemente el detrimento que para la privacidad individual puede derivarse de cualquier captación, conservación, uso y difusión de información personal.

Algunos autores observan en este desarrollo normativo una relación con la evolución de los derechos.

> Una primera generación —dice Fappiano— de leyes sobre protección de datos personales (*Datenschultz*, del Land de Hesse de 1973, *Landesdatenschutgesetz* de Renania-Palatino, 1977, *Data Sueca* de 1973, etc.) tiene como objetivo garantizar los derechos individuales estableciendo determinados límites al empleo de la informática. Se interpretó que la eficacia de la protección reposaba en la autorización previa del banco de datos y en el posterior control de su gestión mediante órganos específicos de vigilancia. Era la época de las computadores escasas y de hardware voluminosos y, por consiguiente, localizables con facilidad.
>
> Las leyes de segunda generación (*Privacy Act* de 1974, *Informatique aux fichiers et aux libertes* francesa de 1978, Constitución de Postugal y España) centran su inquietud en asegurar el derecho de acceso de las personas a las informaciones que les conciernen, mostrando especial atención por la ´calidad de los datos´ y no del hardware que los memoriza, mediante cláusulas específicas de protección de las informaciones consideradas sensibles por su directa incidencia sobre la vida privada o sobre el ejercicio de las libertades.

> En tanto que la tercera *generación* (Convenio Europeo de 1981; *Data Protection Act* inglesa de 1984) e hace cargo de los cambios en la tecnología provocados por la revolución microinformática y, también, de la necesidad de conciliar la defensa de los datos personales con las exigencias de una sociedad en la que la transmisión de informaciones constituye un compromiso social, económico, político y cultural ineludible. Es la época de los "personal computers".[150]

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

Esta orden ocasiona espinosos problemas desde el punto de vista de la protección de datos personales. Estados Unidos no reconoce con carácter general el derecho fundamental a la protección de datos personales, pese a que la privacidad se menciona en la Cuarta Enmienda a la Constitución norteamericana. Lo hace básicamente cuando existe un riesgo de abuso gubernamental en el trato de la información personal y, de este modo, la ley federal interviene sólo frente a él ("P*rivacy Act*" de diciembre de 1974) o cuando se trata de negocios que almacenan información personal sensible (*v. gr.:* datos médicos, financieros o sobre el alquiler de determinadas películas de vídeo). En el resto de casos, si se disciplina, se hace por medio de disposiciones de carácter autorregulatorio.

Además, en el concreto ámbito al que se alude, no existe tutela alguna respecto de los datos de pasajeros que no son ciudadanos de los Estados Unidos (o residentes legales) ni tampoco recurso judicial contra eventuales abusos en la aplicación de dichas medidas. Acceder al PNR significaba realizar una transferencia internacional ilegal según los cánones de la Directiva 95/46/CE; por ello, entre junio de 2002 y mayo de 2004 se desarrolló un complejo proceso de negociación para paliar tal contradicción. Dicho proceso culminó con la autorización de las transferencias a través de la Decisión del 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de Estados

---

[150] FAPPIANO, Oscar Luján, "*Habeas data*: Una aproximación a su problemática y a su posible solución normativa", en *"Liber Amicorum" Héctor Fix Zamudio*, volumen 1, Secretaría de la Corte Interamericana de Derechos Humanos, San José, Costa Rica, 1998, pp. 322 y ss.

Unidos ("*Bureau of Customs and Border Protection*") y la Decisión 2004/496/CE del Consejo, de 17 de mayo, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos.

No obstante, vistos los términos del acuerdo, el acceso al PNR seguía sin respetar el contenido y la finalidad de la Directiva 95/46/CE, por lo que ambos textos fueron recurridos por el Parlamento Europeo ante TJCE el 25 de junio de 2004. El Tribunal de Justicia de la Unión Europea, en un fallo de su Gran Sala, de fecha 30 de mayo de 2006, resolvió anular el mencionado Acuerdo.[151]

342.5. El tercer tiempo fue de los Estados en particular; cada uno diseñó una estrategia para llevar a buen puerto la defensa de la intimidad frente a la agresión informática.

Algunos han optado por la incorporación expresa en el texto constitucional (como es el caso del *Habeas data* de Brasil); otros lo proyectan entre sus garantías constitucionales (por ejemplo, el caso de Argentina que lo trasciende desde el derecho de amparo); algunos prefieren establecer con claridad el derecho a tutelar (intimidad, privacidad, control sobre los datos, etc.) y dejar abierto el tipo procesal (por ejemplo, Perú).

La opción reglamentaria no está ausente y para ello se crean diversidad de textos legales que explicitan el derecho constitucional (Costa Rica); mientras que la preferencia jurisprudencial es reticente, quizás por la desconfianza reinante en las instituciones judiciales.

342.6. La Directiva 95/46 que hemos referido anteriormente, fue seguida en su diligencia y grado de satisfacción que produjo. La Comisión formada indicó en el año 2007 que la aplicación mejoró y que todos los Estados miembros habían transpuesto la Directiva, aconsejando por ello que no se practicaran modificaciones.

El informe da cuenta entre otras cosas de los resultados de las consultas realizadas por la Comisión sobre la evaluación de la Directiva entre los gobiernos, las instituciones, las empresas, las asociaciones de consumidores y los ciudadanos. Los resultados mostraron que pocos participantes abogaron por la modificación de la Directiva.

En suma, lo que se advierte es que pese a los retrasos y lagunas en la aplicación, la Directiva ha cumplido su principal objetivo, a saber, eliminar los obstáculos a la libre circulación de datos personales entre los Estados miembros.

No obstante, otros objetivos de la política de mercado interior no se han satisfecho. La legislación sobre protección de datos sigue mostrando grandes divergencias entre los Estados miembros. Ahora bien, esas disparidades impiden a las organizaciones multinacionales desarrollar políticas paneuropeas sobre protección de datos.

---

[151] MOLINA QUIROGA, *cfr*. tesis doctoral antes citada.

En cuanto al nivel general de conformidad de la legislación sobre protección de datos en la UE, se pueden destacar tres dificultades: *a)* recursos insuficientes en cuanto a la aplicación; *b)* conformidad muy irregular por parte de los responsables del tratamiento de datos; *c)* conocimiento al parecer escaso por parte de los interesados acerca de sus derechos, que puede ser el origen del fenómeno anterior.

342.7. También en Europa la evolución genera nuevas directivas sobre privacidad y formación de archivos en orden a:

a) Comunicaciones electrónicas (Directiva 2002/58 CE)

b) Cláusulas contractuales tipo para la transferencia de datos personales a terceros países (Decisión 2004/915/CE, y Decisión 2001/497/CE)

c) Protección de datos por las instituciones y organismos de la Comunidad (Reglamento 45/2001/CE relativo a la protección de las personas físicas),

342.8. En Argentina, a nivel de legislación local, presenta la siguiente evolución:

Comienza con la reforma constitucional de 1994, cuyo art. 43 introduce en el tercer párrafo la protección de datos personales que provoquen cualquier tipo de discriminación.

Se reglamenta en la Ley 25.326 de Protección de los Datos Personales, que se reforma parcialmente con la n° 26.343 que incorpora el art. 47 (llamada "blanqueo de morosos").

La Ley 26.388 reforma del Código Penal en materia de Delitos Informáticos. Deroga y modifica algunos incisos introducidas por el art. 32 de la Ley 25.326 al Código Penal.

En materia reglamentaria, el decreto 995/2000 veta parcialmente y promulga la ley 25.326. El decreto 1.558/2001 reglamenta la ley de protección de datos y establece principios generales, derechos de los titulares de los datos, usuarios y responsables de archivos, registros y bancos de datos; para finalmente disponer sobre el control y sanciones.

Con el decreto 1898/2002 se procede a la designación del Director Nacional de Protección de Datos Personales, con carácter de excepción a lo previsto por el art. 19 de la Ley 25.565. Y el decreto 1.104/2003 designa en forma transitoria al subdirector.

En el año 2010, se dicta el decreto 1160 que modifica el Art. 31 inc. 3 del decreto 1558/2001 (Decreto Reglamentario de la Ley N° 25326) que desarrolla y amplía las facultades de la Dirección Nacional de Protección de Datos Personales (DNPDP) para la investigación de presuntas infracciones a la ley

Varias disposiciones locales se agregan informativamente:

Disposición n° 1/2003 (Derogada por Disposición N° 7/2005). Apruébanse la "Clasificación de Infracciones" y la "Graduación de las Sanciones" a aplicar ante las faltas que se comprueben.

Disposición n° 2/2003 Registro Nacional de Bases de Datos. Habilítase el mencionado Registro y dispónese la realización del Primer Censo Nacional de Bases de Datos.

Disposición n° 1/2004 Impleméntase, con carácter obligatorio, el Primer Censo Nacional de Archivos, Registros, Bases o Bancos de Datos Privados.

Disposición n° 3/2004 Prorrógase el Primer Censo Nacional de Archivos, Registros, Bases o Bancos de Datos Privados.

Disposición n° 4/2004 Homológase el Código de Etica de la Asociación de Marketing Directo e Interactivo de Argentina (AMDIA).

Disposición n° 2/2005 Implementación del Registro Nacional de Bases de Datos Privadas alcanzadas por la Ley N° 25.326. Formularios de inscripción.

Disposición n° 3/2005 Apruébanse los formularios, instructivos y normas de procedimiento que utilizará la Dirección Nacional de Protección de Datos Personales, en relación con la implementación del Registro Nacional de Bases de Datos Privadas.

Disposición n° 4/2005 Prorrógase la fecha de implementación del mencionado Registro, establecida por la Disposición N° 2/2005.

Disposición n° 6/2005 Apruébase el diseño del isologotipo que identificará a los responsables de bases de datos personales inscriptos en el Registro Nacional de Bases de Datos.

Disposición n° 7/2005 Apruébanse la "Clasificación de Infracciones" y la "Graduación de las Sanciones" a aplicar ante violaciones a las normas de la Ley N° 25.326 y de las reglamentaciones dictadas en su consecuencia. Derógase la Disposición N° 1/2003.

Disposición n° 1/2006 Prorrógase el plazo de vencimiento para la inscripción en el Registro Nacional de Bases de Datos.

Disposición n° 2/2006 Impleméntase el Relevamiento Integral de Bases de Datos Personales del Estado Nacional.

Disposición n° 5/2006 Impleméntase el Registro Nacional de Bases de Datos a los fines de la inscripción de los archivos, registros, bancos o bases de datos públicos.

Disposición n° 6/2006 Prorrógase el plazo de vencimiento para la inscripción en el Registro Nacional de Bases de Datos.

Disposición n° 8/2006 Ordénase la publicación de los dictámenes de la Dirección Nacional de Protección de Datos Personales en la página web de la dependencia.

Disposición n° 9/2006 Registro Nacional de Bases de Datos. Apruébanse los Formularios de Modificación y Baja del Registro.

Disposición n° 10/2006 Registro Nacional de Bases de Datos. Incorpórase la inscripción de archivos, registros, bases o bancos de datos públicos pertenecientes a los entes públicos estatales no incluidos en la Disposición N° 2/2006 y entes públicos no estatales, que se encuentren interconectados en redes de alcance interjurisdiccional, nacional o internacional.

Disposición n° 11/2006 Apruébanse las "Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados".

Disposición n° 1/2008 Apruébase el diseño de los isologotipos que identificarán a los responsables de bases de datos inscriptos en el mencionado Registro, que haya efectuado las renovaciones correspondientes a los años 2007 y 2008.

Disposición n° 2/2008 Créase el Repertorio de Jurisprudencia sobre *Habeas Data*.

Disposición n° 3/2008 Créase el Centro de Jurisprudencia, Investigación y Promoción de la Protección de los Datos Personales.

Disposición n° 5/2008 Apruébase las Normas de Inspección y Control de la Dirección Nacional de Protección de Datos Personales.

Disposición n° 6/2008 Control de ejecución de formularios de consentimiento informado.

Disposición n° 7/2008 Apruébanse la "Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público" y el texto modelo de "Convenio de Confidencialidad".

Disposición n° 9/2008 Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales contenidos en Archivos, Registro, Bancos y Bases de Datos Públicos No Estatales y Privados. Prorrógase el plazo establecido por la Disposición Nº 11/2006.

Disposición n° 10/2008 Establécese que los Responsables y Usuarios de Bancos de Datos Públicos o Privados, deberán incluir en su página web y en toda comunicación o publicidad, en particular, en los formularios utilizados para la recolección de datos personales, información al respecto.

Disposición n° 12/2008 Apruébase el diseño de los isologotipos que identificarán a los responsables de bases de datos inscriptos en el mencionado Registro durante el año 2009.

Disposición n° 4/2009 Establécese que la opción para el ejercicio del derecho de retiro o bloqueo contemplada en el artículo 27, inciso 3 de la Ley 25.326 deberá aparecer en toda comunicación que se efectúe con fines publicitarios, junto con el mecanismo previsto para su ejercicio.

Disposición n° 7/2009 Apruébase el diseño del isologotipo que identificará a los responsables de bases de datos personales.

Disposición n° 7/2010 Créase el Centro de Asistencia a las Víctimas de Robo de Identidad.

Disposición n° 12/2010 Tratamientos de Datos Personales Destinados a Difusión Pública.

Disposición n° 17/2010 Establécese el sistema informativo denominativo "Base Informática para la Comunicación Electrónica Interjurisdiccional sobre Datos Personales en Información Crediticia".

343. Creación de archivos

343.1. La base o banco de datos se constituye para un fin determinado; circunstancia que la diferencia de una fuente de información que puede estar en las cosas o lugares.

Es común que las legislaciones especifiquen o interpreten que se entiende por archivos de datos personales. Algunos son más precisos que otros, dando lugar a desencuentros que en adelante mostramos.

La ley argentina dice en el artículo 2 que "archivo, registro, base o banco de datos" [...] "*indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso*".

Informa Uicich la Resolución del Consejo de Ministros de la Organización de Cooperación y Desarrollo Económico (OCDE) europea del 23 de setiembre de 1980 que en el artículo primero de su Directiva define a las bases de datos como:

> Toda colección de obras o materiales ordenados, almacenados y accesibles mediante medios electrónicos, así como el material electrónico necesario para el funcionamiento de la misma, por ejemplo: su diccionario, índice o sistema de interrogación o presentación de información, no quedarán comprendidos en la definición de los programas del ordenador utilizados en la realización o el funcionamiento de las bases de datos.[152]

Un ejemplo testimonia con facilidad la distinción: si alguien necesita conocer la solvencia económica de una persona, recurre a un *registro* bancario o a una oficina comercial creada para estos efectos; en cambio, si lo buscado es un dato aislado, por el caso: fecha de nacimiento o de deceso; la fuente de información llega desde el lugar donde fue la persona sepultada, o del archivo documental que emite la partida de nacimiento o el certificado de defunción.

Esto significa que la cantidad de información almacenada sirve para diferenciar un archivo de un registro, o de una base de datos; pero todas en general están alcanzadas por la protección especial que confiere el derecho a la autodeterminación informativa.

343.2. Cabe destacar que un gran número de datos se encuentra fácilmente disponible para quien los necesite. Desde aquellos que se toman de la simple información cotidiana como de otros que están al servicio de la sociedad para fines diversos. Por eso el problema no es la disponibilidad de la información que concierne a una persona, sino de los datos que éste admite que sean públicos o que pretenda estén reservados o absolutamente confidenciales.

Los archivos existen desde tiempos inmemoriales; ellos han dejado constancia de los nacimientos, las defunciones, los matrimonios, las enfermedades, entre tanta información recopilada y guardada con fines históricos o para ensayar comparaciones científicas.

El cambio operado se produjo con la aparición de la tecnología, que desvanece el límite antes fijado por el espacio y el tiempo. La crónica anterior fue suplida por la telemática (que supone hacer posible la consulta de una base de datos desde cualquier distancia) y el tratamiento de la información permitió generar otras deduc-

---

[152] UICICH, ob. cit., p. 75.

ciones, y lo que fue más importante, dejó de estar en sólo un lugar para instalarse en un sistema de acceso mundial con la sola pulsación de una tecla (Internet).

> En el ámbito de las telecomunicaciones es bien conocido el ejemplo de los directorios inversos: se crean con los mismos datos que se utilizan para los directorios públicos de los abonados telefónicos, pero se invierte el criterio de búsqueda; en vez de utilizar un nombre y una dirección conocidos para encontrar un número de teléfono, se usa ese número para averiguar el nombre y la dirección del abonado.

343.3. De esta manera allí donde ya existía un archivo, un registro, una copia de datos o un respaldo documental, con la aparición de la informática surge una abundancia informativa que hace necesaria la clasificación, la comparación, la sistematización y la recuperación de la misma, convirtiendo la simple reunión informativa en un grandioso archivo de perfiles, de preferencias, de gustos, de estructuras económicas, etc., etc.

Este cambio, evidentemente, provocó la dispersión de los datos y la pérdida del control sobre ellos. Las redes informáticas difundieron en escala dichas fuentes de información, y la tecnificación (digitalización, escaneo documentario, recuperación de textos, etc.) han multiplicado al infinito las posibilidades de búsqueda y de organización.

> La estructura abierta de la red Internet se fomentó para evitar que los datos fuesen conservados en un solo lugar. Para el Pentágono —afirma Marcel Pinet— se trataba de la máxima medida de seguridad: la dispersión de los datos estratégicos permitía esconderlos de las fuerzas enemigas a la vez que permitía conservar la posibilidad técnica de una recuperación instantánea. Esta es la característica que ha abierto nuevas posibilidades: primero para las Universidades y ahora para las empresas comerciales.
>
> Ahora, los datos nominativos se esparcen por la red por varias razones: para facilitar la cooperación científica existen directorios de investigadores; publicaciones de organigramas que describen la organización de la administración o de empresas privadas, en los que se incluyen anotaciones biográficas de las personas que ostentan los cargos de responsabilidad; transmisión de directorios preexistentes, como los de los abonados telefónicos, anuncios por palabras, etc.[153]

La antigua privacidad de los archivos, habitualmente conservados en registros manuales escritos, rápidamente se transformó en unos pocos *bits* almacenados en la memoria de una computadora que, desde la generalización de las redes virtuales como Internet, facilitan la transmisión. De suyo, los datos antes reservados y ciertamente confidenciales pasaron a ser públicos y disponibles para cualquiera.

343.4. Es preciso aclarar que algunas legislaciones prefieren no hablar de "archivos" optando, por ejemplo, por "ficheros", quizás influenciados por el significado que el primero tiene en el sentido informático, como conjunto de datos que ocupan un espacio en el disco (duro o flexible), a los que se asigna un nombre y tienen un

---

[153] PINET, ob. cit., p. 25.

autor determinado. Su característica es similar a la de un libro, solo que la extensión se mide en *bites (binary digit* o dígito binario) y tiene un atributo determinado.

Nosotros utilizamos la noción de "archivo, registro o banco de datos" que tienen en nuestro vocabulario mayor comprensión que las voces usadas en Europa.

> La interacción entre las disposiciones que afectan a los registros públicos y la legislación en materia de protección de la intimidad puede ser compleja, afirma Bruce Slane. La utilización de la libertad de información en este contexto puede, innecesariamente, agravar aún más la situación. En mi opinión —agrega—, la libertad de información no encaja fácilmente con la institución de los registros públicos y, sin embargo, se utiliza en Nueva Zelanda para exigir la publicación de datos en masa. Este tipo de aplicación de la legislación sobre libertad de información es demasiado estricta y no sirve ni para el cumplimiento de la función encomendada a los registros ni para la propia libertad de información.[154]

De esta manera, la creación de los archivos ha debido respetar ciertas reglas y principios, pero al mismo tiempo, reconocen derechos al individuo afectado (concernido) por el registro, y también, al titular de la base de datos. Se establecieron procesos y procedimientos para el almacenamiento, la conservación, la seguridad interna del archivo, y las fases para el tratamiento (circulación y venta de la información).

343.5. Para hacer referencia a los sistemas de documentación informática se utilizan las expresiones banco de datos (*data bank*) y base de datos (*data base*). En ocasiones —dice Pérez Luño— se ha tratado de establecer diferencias entre ambos términos. Así, por ejemplo, se ha indicado que mientras las bases de datos se refieren a sistemas de documentación que operan con títulos o referencias, los bancos de datos almacenan textos o documentos. Otras veces, se ha considerado que la expresión base de datos es propia del lenguaje técnico informático y hace referencia al conjunto de programas dirigidos a organizar la documentación, mientras que los bancos de datos sería la expresión propia del lenguaje de las ciencias sociales y del derecho que aludiría al conjunto de informaciones pertenecientes a estos campos del saber y que se hallarían organizadas en una o varias bases de datos.[155]

El hecho de que en inglés la abreviatura BD sirva para aludir a *data banks* y *data bases*, indistintamente, ha determinado un uso indiferenciado entre ambas expresiones. Por tanto, parece ocioso tratar de establecer contrastes, más o menos sutiles, cuando las diferencias entre ambos términos han sido abolidas por la práctica.

La realidad de los registros evidencia que no todos tienen finalidades informativas, es decir, que sean transmisibles a terceros. Esta característica, en consecuencia, lleva a resolver cuál es la protección que la persona ostenta: si lo es para evitar que el archivo ingrese sus datos y con esa incorporación afecte, probablemente, la

---

[154] SLANE, Bruce, *Publicación masiva de registros públicos: una perspectiva Neozelandesa,* en "XX Conferencia Internacional de autoridades de protección de datos" (1998), Agencia de Protección de Datos, Madrid, 1999.

[155] PÉREZ LUÑO, ob. cit., p. 166.

privacidad; o en su caso, si la tutela se vincula a la reserva y confidencialidad (y eventual supresión) que los datos deben conservar, evitando que se concrete una hipotética transferencia que violente la intimidad de la persona al hacer públicas sus características.

En los hechos, ambas son las actitudes defensivas que tiene un individuo. Sólo que una vía se concreta desde la ley de protección de datos; y la otra, a través del *habeas data* y sus posibilidades concretas de demanda (*v. gr.:* acceso, actualización, rectificación, confidencialidad, reserva, o cancelación).

344. La formación de archivos públicos y privados

344.1. A los fines de la protección de datos personales, se ha visto establecer diferencias según quien los capture sea con finalidades públicas (*v. gr.:* estadística, censo poblacional, registros de propiedad, inscripciones matrimoniales, etc.) o privadas (*v. gr.:* información comercial; marketing directo; publicidad; etc.). La distinción es necesaria pues mientras uno se refiere al gestor que desarrolla la base, propiamente dicha, el restante diferencia la calidad reservada o disponible de la información. Es decir, mientras un archivo público puede ser propio y natural para la gestión social y económica del Estado, el dato que allí se encuentra puede ser público por su disponibilidad como fuente de conocimiento para todos. En cambio un archivo privado puede tener finalidades diversas (*e-commerce*; confianza crediticia; perfiles para la venta potencial, etc.) y el dato allí contenido suele ser confidencial por la naturaleza del banco de datos, aunque la circulación de ellos sea producto de la propia actividad desarrollada.

> De todos modos, conviene anticipar que algunos autores suelen distinguir entre datos reservados y datos públicos y hacen diferencias en cuanto a los alcances de la protección que debe asignárseles a uno y otro. Los típicos datos reservados —sostienen Beltramone y Zabale— son aquellos que contienen algún tipo de información de la calificada como "sensible" y que atañe a cuestiones íntimas de las personas (religión, raza, conducta sexual, opinión política, etc.). Los datos denominados "públicos" serían, entonces, para esa doctrina, aquellos de menor importancia o que pueden ser obtenidos fácilmente (como un número telefónico o una dirección, por ejemplo). De modo que los primeros, y dado precisamente su carácter de "reservados", merecen una mayor salvaguarda que los segundos.[156]

344.2. La división entre "tipos" de archivos posibles, permitiría una clasificación más extendida. Por ejemplo, archivos de datos personales; de información crediticia; de movimientos comerciales; de antecedentes penales; de inversiones; y en definitiva, de cuanta actividad se disponga a almacenar en un banco informático.

Sin embargo, la pregunta inmediata es ¿para qué sirve tal clasificación? La respuesta puede ser totalmente inesperada: "para nada", salvo que exista un tratamiento

---

[156] BELTRAMONE, Guillermo, ZABALE, Ezequiel, *El Derecho en la era digital —Derecho informático a fin de siglo—*, Juris, Rosario (Argentina), 1997, p. 54.

diferencial entre archivos públicos y privados. Pero como bien afirma la doctrina, el problema no está en la condición del archivo, sino en la calidad del dato, y aun así, hay que reconocer que ello es una diferencia contingente.

Afirma Bianchi[157] que:

> no hay datos públicos o privados sino situaciones concretas que los califican como tales. Agregando Beltramone y Zabale que las creencias religiosas o las prácticas sexuales, son normalmente un dato reservado, pero también puede serlo el domicilio de una persona o su número telefónico, en el caso de que exista una amenaza de un atentado contra ella. Por otra parte, un dato insignificante puede carecer de importancia, pero la suma de ellos puede llegar a desnudar la intimidad de las personas.[158]

344.3. En Argentina, el artículo 43 de la Constitución, y su ley reglamentaria los iguala. Los archivos pueden ser *públicos o privados* y, a los fines del *habeas data*, deben estar *destinados a proveer informes*. Por registros o bancos de datos públicos debemos entender los existentes en los organismos del Estado, de cualquier naturaleza, ya que la ley sólo establece las siguientes excepciones:

> ART. 23 (Supuestos especiales):
>
> 1. Quedaran sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia: y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.
>
> 2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad publica o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categoría, en función de su grado de fiabilidad.
>
> 3. Los datos personales registrados con fines policiales se cancelaran cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Esto incluye no sólo a las reparticiones de la Administración Pública nacional centralizada, sino también a los entes descentralizados, autárquicos, empresas públicas y sociedades estatales, así como dependencias provinciales y municipales.

Para Sagüés:

> la expresión *registros o bancos de datos públicos* no debe ser interpretada en el sentido de registros públicos, por oposición a registros reservados o secretos, ya que la norma se

---

[157] BIANCHI, Alberto, *Habeas Data y derecho a la privacidad,* ED, 161-868 y ss.

[158] BELTRAMONE, ZABALE, ob. cit., p. 59.

refiere a los titulares u operadores de los registros o bancos de datos. La redacción del texto abona esta interpretación ya que armoniza con la referencia a '*los privados destinados a proveer informes*'.[159]

Han sido incorporados como sujetos pasivos de la acción de *habeas data*, los registros o bancos de datos privados '*destinados a proveer informes*', que son, básicamente, los operados por las empresas o personas individuales dedicadas a recolectar información personal para suministrarla a sus clientes. Es el caso de las empresas de informes comerciales o financieros, que proveen a bancos, financieras, comercios y a quienes conceden crédito en general, información sobre situación patrimonial, reclamos pecuniarios judiciales o extrajudiciales, etc.

344.4. Sin embargo, la legislación comparada advierte que esta es una corriente sesgada. Sostener que solo están alcanzados los archivos cuyo destino es proporcionar información a terceros, puede dejar al descubierto un sinfín de problemas.

Por ello, otros como *Paraguay*, prefieren ocuparse solamente de los archivos públicos dando permiso a toda persona a recolectar, almacenar y procesar datos personales para uso estrictamente privado. Pero cuando son de aquel carácter la fuente pública de información es libre para todos. "Toda persona tiene derecho al acceso a los datos que se encuentren asentados en los registros públicos [...]" (art. 2, ley 1682).

La línea se comparte en *Perú*, cuyo inciso 3° del art. 200 de la Constitución Política del Estado, modificado por la ley de reforma constitucional n° 26.470, incorpora el *habeas data* como proceso destinado a controlar el acceso a la información pública, archivada en registros públicos y privados. El derecho otorga la posibilidad de solicitar, sin expresión de causa, la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo á Ley y siempre que se refieran al caso investigado.

En cambio *México*, en la ley Federal de protección de datos personales, decide dejar fuera de control a los *archivos públicos*, aplicando en todo el país la regla por la cual se protegen datos personales en *posesión de particulares,* con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

ART. 2.—Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:

---

[159] SAGÜÉS, Néstor Pedro, *Derecho Procesal Constitucional —Acción de Amparo—*, Astrea, Buenos Aires, 1995, p. 367.

I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y

II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Colombia, con la ley estatutaria 1266 incluye disposiciones generales del *habeas data* y regula el manejo de la información contenida en las bases de datos personales, en especial las bases financieras, crediticias, comerciales, de servicios y las provenientes de otros países. La norma define claramente su objeto: desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales así como el derecho a la información establecido constitucionalmente, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

El alcance de la norma es tanto en bases de *datos públicas* como *privadas,* exceptuándose las que tienen por finalidad producir la Inteligencia de Estado por parte del Departamento Administrativo de Seguridad (DAS), y de la Fuerza Pública para garantizar la seguridad nacional interna y externa. Los registros públicos a cargo de las cámaras de comercio se rigen exclusivamente por las normas y principios consagrados en las normas especiales que las regulan y también quedan excluidos aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y los que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales.

También *Ecuador,* en el art. 94 de la Constitución dice que:

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.

344.5. En resumen, el alcance de la protección a los datos personales no se acuerda por el solo hecho de estar en una base de datos, archivo, registro o banco de datos (después veremos que cada uno de estos es una categoría, aunque legislativamente se los considere con igualdad). La defensa depende del uso que se destine a la información, por lo que se simplifica la dimensión en las posibilidades siguientes:

a) *Archivos públicos* (todos aquellos que tengan información personal). En este espacio se ubican todos los registros de datos personales que están encuadrados dentro

del derecho de acceso a la información pública que solo se puede negar informar cuando se altera el derecho de terceros, o se invade la intimidad del concernido.

Por tanto algunas leyes prefieren especificar que el alcance de la protección es para los [...]:

*a.*1) Archivos públicos que reporten información a terceros o difunda datos de contenido personal.

*a.*2) Se excluyen los archivos de defensa; seguridad; orden público; cuando la información afecte a terceros; cuando se obstaculice una actuación judicial o administrativa en curso que investigue sobre el cumplimiento de obligaciones tributarias o previsionales; cuando impida el desarrollo de actividades de control de la salud; cuando obstaculice el control del medio ambiente; cuando impida o genere dificultades en la investigación de delitos penales; cuando impida o genere dificultades en la verificación de infracciones administrativas.

Otras excepciones a los derechos de los afectados las tiene la Ley 15/1999 del 13 de diciembre, española, que ha sido declarado inconstitucional[160] por el fallo citado en nota. Allí se indica que:

> 1) Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas. 2) Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

b) Otros restringen la protección a los *archivos privados* que compilen información personal, con las particularidades que siguen [...]:

---

[160] El Tribunal Constitucional español ha declarado la inconstitucionalidad de este precepto incluido en la ley 15/1999. Ha dicho: "Como en otra ocasión hemos aseverado, los motivos de limitación adolecen de tal grado de indeterminación que deja excesivo campo de maniobra a la discrecionalidad administrativa, incompatible con las exigencias de la reserva legal en cuanto constituye una cesión en blanco del poder normativo que defrauda la reserva de ley. Además, al no hacer referencia alguna a los presupuestos y condiciones de la restricción, resulta insuficiente para determinar si la decisión administrativa es o no el fruto previsible de la razonable aplicación de lo dispuesto por el legislador (SSTC 101/1991, FJ 3 y 49/1999, FJ 4). De suerte que la misma falta evidente de certeza y previsibilidad del límite que el art. 24.2 LOPD impone al derecho fundamental a la protección de los datos personales (art. 18.4 CE), y la circunstancia de que, además, se trate de un límite cuya fijación y aplicación no viene precisada en la LOPD, sino que se abandona a la entera discreción de la Administración Pública responsable del fichero en cuestión, aboca a la estimación en este punto del recurso interpuesto por el Defensor del Pueblo al resultar vulnerados los arts. 18.4 y 53.1 CE".

Se excluyen:

*b.*1) Los ficheros de uso personal, interno o doméstico, porque no están destinados a dar informes

*b.*2) Las bases de datos y las fuentes de información periodística.

*b.*3) Los archivos de datos recopilados con fines estadísticos, encuestas de opinión, mediciones, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, siempre que la recolección de datos se practique en forma anónima o la información se disocie de la identidad del titular mediante un procedimiento técnico (art. 28, ley 25.326 de Argentina)

Se incluyen solamente aquellos destinados a:

*b.*4) Dar información de solvencia patrimonial y de cumplimiento de obligaciones.

*b.*5) Bases de datos destinados a venta telefónica directa

En estos casos, las bases son de particulares que toman información personal para transmitirla a otros o para aprovecharla en su beneficio. Por ello, esta categoría no trata de establecer una excepción a las reglas generales que suele tener las leyes de protección de datos personales, sino de imponer obligaciones adicionales como el plazo para la conservación de los datos, el derecho de *opt out*, o el deber de disociación o anonimato de la persona concernida.

En el caso de los archivos de datos con fines de publicidad las particularidades son referidas a los temas del *consentimiento* para la obtención y uso de información personal (sea para determinar perfiles o establecer hábitos de consumo), el derecho de *acceso gratuito* permanente, y la *calidad de los datos* que se pueden trabajar en marketing.

> No es ocioso señalar que la actividad de estas bases de datos constituye uno de los desarrollos más importantes en el mercado mundial. El comercio electrónico está creciendo con gran rapidez y alcanzó casi 200.000 millones de euros en el año 2000. A finales de 1996, 86 millones de personas estaban conectadas a internet en todo el mundo y se proyectó que en el año 2000 habría 250 millones. Tal impacto llevo a la CEE a realizar una propuesta de Directiva encaminada a establecer un marco jurídico coherente para el desarrollo del comercio electrónico en el mercado único, que permitirá que los servicios de la sociedad de la información se beneficien de los principios de mercado único, de libre circulación de servicios y de libertad de establecimiento y puedan proporcionar sus servicios en la Unión si cumplen con la ley en su país de origen. Para que el enorme potencial que el comercio electrónico representa se materialice, es esencial generar seguridad y confianza en las transacciones *on line*. Consciente de ello la Unión Europea publicó el 13 de mayo de 1998, una Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica. El propósito de esta propuesta es facilitar la manifestación de voluntad por vía electrónica en redes abiertas, eliminando las diferencias del reconocimiento legal de la firma electrónica entre los países miembros de la Unión.
>
> El tema de la validez de la firma electrónica debe mantenerse íntimamente vinculado al tema de la contratación electrónica, que es la que ha generado la necesidad de aquélla y del reconocimiento de su fuerza ejecutiva y probatoria.

La propuesta establece normas armonizadas específicas sólo en aquellos ámbitos estrictamente necesarios para garantizar que las empresas y los ciudadanos puedan suministrar y recibir, respectivamente, servicios de la sociedad de la información en todo el ámbito de la U.E. Se abarca de este modo tanto los servicios entre empresas, como los servicios de las empresas a los consumidores, incluso los servicios proporcionados gratuitamente financiados con ingresos publicitarios o patrocinio, o servicios que permiten transacciones económicas interactivas por televisión.

Los sectores afectados por esta futura regulación serán:

- Las bases de datos en línea.
- Los periódicos en línea.
- Los servicios financieros y profesionales en línea
- Los servicios de ocio
- Los servicios que proporcionan acceso a la Web

Las características de estas bases de datos llevan a decisiones significativamente diferentes en países que han regulado al sector respecto a quienes continúan elaborando respuestas a partir de criterios tradicionales del derecho común.

Queremos expresar con ello que el uso de datos personales en archivos de marketing pueden o no estar alcanzados por una ley de protección de información personal, dependiendo muchas veces del temperamento legal o de la interpretación jurisprudencial que analice si estamos ante un problema de usos generalizados de datos que no identifican a nadie en particular, o si en realidad, con el tratamiento se provocan perturbaciones individuales que merecen una singular tutela. Mientras el primer caso, puede llevar a autorizaciones globales por resultar, en definitiva, un servicio más que se pone a disposición de las personas; en el segundo supuesto, se piensa que la formación de perfiles, la determinación de hábitos de consumo, o la oferta individualizada provoca intromisiones en la vida privada de las personas que sólo ellas pueden autorizar.

344.6. La aplicación práctica de una la ley de protección de datos personales depende del modelo que se adopte. En España, se inscriben ficheros de titularidad pública y privada, mientras que en Argentina, los archivos privados que no estén destinados a dar información, no tienen que registrarse y menos aun, cuando sean de uso exclusivamente personal.

En términos coincidentes la reglamentación dispone que no será obligatoria la inscripción cuando el archivo esté constituido, dentro de un mismo grupo económico, con el fin de proporcionarle información.

No obstante, algunos opinan que el concepto "destinado a proveer informes" puede entenderse en dos sentidos: *a)* uno *restringido*, referido a los registros privados que se dedican a proveer informes a terceros, que son los que deberían inscribirse en el Registro de Archivo de Datos para cumplir el deber de información impuesto. Y *b)* uno *amplio*, que califica como tales a los que exceden el uso personal, en el sentido de que, son los que recopilan datos personales que tienen relevancia para el goce o protección de los derechos de sus titulares (de los datos), sin que necesariamente tengan la función específica de emitir informes hacia terceros.

345. Los archivos de uso personal

345.1. *Archivo de uso personal*, básicamente, es el banco de información que tiene para uso profesional o doméstico una determinada persona física o jurídica. Esos datos que almacena, pueden haberse obtenido directamente del cliente o del concernido (titular de los datos), o lograrlos mediante procedimientos indirectos, o de fuentes accesibles al público; pero en todos los casos, con la obligación de mantenerlos en reserva y confidencialidad debido al carácter secreto que tiene su propio registro.

Esta calidad surge de la propia aplicación que tiene la base de datos personal y exclusiva, toda vez que la información almacenada no se puede ceder ni transferir. Además, un registro de esta naturaleza puede o no estar alcanzado por la ley, pero cuando lo está, hay que aplicarle los principios de proporcionalidad (tener sólo los datos necesarios para la actividad o el uso específico de carácter exclusivo), y de calidad de los datos en general.

345.2. Si el archivo personal revierte y se decide dar a esa base informativa otro destino, y en particular cederlos a terceros, queda encuadrado en el marco de protección de datos, necesitando las operaciones realizadas, expreso consentimiento de las personas.

El caso es más habitual que inesperado y sucede, por ejemplo, cuando desde un correo electrónico se envía una información genérica a varios destinatarios, uno de los cuales copia las direcciones formando una base que debe ser informada a cada persona concernida, cuando el destino que se quiere darle es de información a terceros.

345.3. Esta sutil diferencia que tiene solamente en cuenta el agente que origina el banco de datos (público o privado) no es suficiente para controlar la invasión a la intimidad. Basta confrontar un hecho cotidiano para advertir la indefensión de la persona para detener llamados telefónicos o cartas que llegan a su nombre ofreciendo cosas, lugares o servicios. Esa injerencia permanente es una intromisión indeseable en un reducto propio y contamina la privacidad.

> Una investigación publicada en el año 1996 calculaba que en Estados Unidos una persona generaba 150 registros electrónicos diarios. Porque cuando se completan formularios, cupones, encuestas, por ejemplo, o en la simple utilización de la tarjeta de crédito, o al depositar un cheque en la sucursal bancaria, esa información se carga en una computadora que la guarda o distribuye donde debe. Luego, esa información privada y reservada es la que conforman las bases de datos. Tan necesarias para el trabajo de unos y tan valiosas para los negocios de otros; pero que al mismo tiempo, provocaron un mercado ilegal que, en el mejor de los casos, se utilizan con fines comerciales o de promoción política.
>
> Un ejemplo más muestra porqué no es útil la diferencia entre el archivo que se origina desde el Estado y aquél que resulta creado por un particular con fines comerciales. El Estado tiene en sus bases de datos, por ejemplo de la ANSES (Administración Nacional de la Seguridad Social) una fuente de información grandiosa al contar con una variable

> de registros que van desde los habituales identificadores hasta el de profesiones e ingresos promedios anuales. En cierta ocasión fue descubierta una operación de compra de esos datos por una cifra muy significativa de parte de una empresa comercial que pretendía con ello obtener un perfil de clientes a quienes seducir con sus productos. Asimismo, hay bases de datos creados por personas que buscan compradores tradicionales (por ejemplo, empresas de telemarketing, que venden sus productos a través del teléfono o del correo), lo cual supone una actividad perfectamente lícita. Sin embargo, alguna vez un banco oficial (del Estado) con la idea de vender más tarjetas de créditos, persiguió adquirir estos archivos que tenían identificadas y clasificadas a las personas por su nivel de ingresos, solvencia económica, ingresos anuales, deudas hipotecarias pendientes, juicios civiles o penales en su contra, etc., informaciones —todas ellas— de carácter confidencial, que se vendían a razón de un valor ínfimo por dato, pero que en la suma llegaba a un múltiplo verdaderamente sorprendente.[161]

En *España* la ley de tratamiento de datos divide los ficheros según la titularidad sea pública o privada, pero en ambos casos, se tiene en cuenta la finalidad prevista para el archivo, las formas como se efectuará el almacenamiento de información, la descripción de los datos que se pretende relevar, las cesiones o transferencias que se prevean, los órganos que son responsables del fichero y los servicios que se presten a las personas identificadas cuando ellas pretendan ingresar al banco de datos y ejercer actos de control sobre el mismo.

El principio, en ambos casos, es que la persona debe prestar consentimiento para estar en las bases de información. Ha de quedar en claro que, esta pretensión, si bien ideal, constituye muchas veces una utopía (mucho más cuando se advierte que la toma de registros, a veces, se produce desde Internet y resulta imposible conocer las probables interconexiones de datos).

345.4. Frente a tanta diversidad en el almacenamiento de datos resulta necesario elaborar una clasificación de los archivos (ficheros, en el nomenclador que utiliza España), teniendo presente que algunas veces los datos son fácilmente conocidos, y otras que, aun siendo de personas fallecidas, conserva gran interés conocer el antecedente para sistematizarlos.

Con esta tendencia la ley argentina incorpora un régimen para los archivos, registros o bancos de datos públicos y privados destinados a proveer informes, por el cual, además del dato personal que se categoriza genéricamente, se establecen singularidades para los datos sensibles; los hábitos personales o preferencias de consumo; los antecedentes penales y contravencionales y los datos relativos a la salud.

Expresa Pinet que:

> cuando un legislador estipula que una determinada información sea accesible al público no quiere decir necesariamente que esa información tenga la consideración de *res nullius*. Del mismo modo, cuando una persona decide hacer públicos unos datos, bajo ciertas condiciones, no quiere decir que dicha persona pretende renunciar a todos sus derechos.[162]

---

[161] *Cfr.* Gozaíni, *Derecho Procesal Constitucional – Habeas Data (Doctrina y jurisprudencia),* cit., p. 138.

[162] Pinet, ob. cit., p. 73.

345.5. Con otra perspectiva, *Paraguay* dispone el derecho de toda persona a recolectar, almacenar y procesar datos personales para uso estrictamente privado. El uso de los datos que se toman de fuentes públicas de información son libres para todos, de manera que a los fines antes dichos, no hay limitación a la formación de archivos particulares.

Igual derecho tienen aquellos que apliquen la información a fines científicos, estadísticos, encuestas y sondeos de la opinión pública o para estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas. Pero se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables.

Como se aprecia, al confrontar las legislaciones, el radio de cobertura para los archivos es distinto siendo conveniente clasificarlos.

346. Diferencias entre archivos, registros, bases y banco de datos

346.1. En la práctica no suelen clasificarse los tipos de archivos (manuales o informáticos), porque se pretende resolver la aplicación de los principios fundamentales de la denominada "libertad informática" sobre la calidad del dato que se guarda o transmite. A partir de allí se deriva su relación con el derecho a la intimidad y otras reglas y principios que se aplican a quienes trabajan sobre datos de las personas físicas y jurídicas.

No obstante la idea común es proteger la información que se resguarda en documentos informáticos, que pueden ser compilados en archivos, registros, bases o banco de datos. Las leyes suelen dar sinonimia a los conceptos, pero ellos son diferentes.

346.2. *Archivar* es guardar papeles o documentos en un archivo; y *archivo* significa el lugar donde se resguardan cosas importantes o curiosas. En otro sentido, pero vinculado, se dice de quien conserva secretos o intimidades que se le confían.

> Actualmente, en lenguaje informático, archivar es registrar un conjunto de información que tiene similar estructura. El archivo puede ser *lógico* y estar referido a un sistema de ingreso y búsqueda; o ser *físico* y permanecer en un lugar establecido.
>
> Toda base de datos contiene información para el usuario y, una vez dentro del sistema, cada dato abre nuevas variables. Estas suelen clasificarse en *características (data dictionary),* y *relaciones (relationships),* que vinculan los archivos a través de una tabla (que es la que almacena por segmento o grupo) o por documentos (*file*) que establece campos de búsqueda e interxconexión.
>
> Los archivos se denominan "*maestros*" cuando contiene los registros de la base de datos, donde cada cual tiene un conjunto de longitud variable que se identifica con un número o nombre.
>
> Son archivos "*invertidos*" aquellos que contienen términos que pueden usarse como puertos de acceso para la recuperación de información, pero desde una pauta diferente a la tradicional. Por ejemplo, si se busca información de alguien, en lugar de buscar su nombre y apellido, se localizan sus rasgos físicos u otros.

Se denominan "*archivos Any*" los que permiten agrupar términos asociados y lograr un perfil por disociación. Por ejemplo, cuando se quiere saber cuál es el gasto anual de una persona que pertenece a un grupo profesional. Estos asimismo se vinculan con los llamados "*Archivos cruzados*" que facilitan la interconexión y el tratamiento de los datos.

Un archivo es la base general (*v. gr.:* Archivo Histórico de la Nación), que puede abrir archivos menores que suelen registrar información clasificada.

346.3. *Registrar* es transcribir en los libros de un registro público las resoluciones de la autoridad o los actos jurídicos de los particulares. Se registra cuando se dejan señales de identificación de un lugar, cosa o personas.

Un *registro* es el libro en donde se apuntan datos o noticias, y tiene una diversidad de manifestaciones (*v. gr.:* Registro Civil; Registro de la propiedad inmobiliaria; Registro de la propiedad intelectual; Registro de la propiedad industrial; entre otros). También constituyen *registros* las anotaciones informáticas que se incluyen en un soporte mecánico, y son las piezas que fundan los bancos de datos.

Un registro puede formar parte de un archivo e integrar en su compilado, observaciones o anotaciones puntuales.

346.4. Las *bases y bancos de datos* son el conjunto organizado de informaciones que han sido objeto de "tratamiento" o "*data mining"* que permite realizar entrecruzamientos y prospecciones para interpretar los datos almacenados.

Estos son fragmentaciones de los registros y partes inferiores de un archivo. Por ejemplo: el mencionado Archivo Histórico puede tener "registros" por años, y bases que informan lo hecho por cada prócer dentro del período que se investiga.

346.5. Los *bancos de datos* son fuentes de información independiente. A ellos se recurre cuando se quiere comenzar a formar el archivo. Por ejemplo, si deseo implementar el Archivo Histórico se recurre a los bancos de información sobre hechos, personas, acontecimientos, etc., que pueden estar en uno o varios bancos; y en solo un lugar o en varios, locales o transfronterizos.

346.6. Finalmente, se denomina como "*tratamiento"* las operaciones y procedimientos técnicos, de carácter automatizado o no, que permiten almacenar, grabar, elaborar, modificar, resguardar, disociar y eliminar datos de carácter personal, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

El artículo 2º de la ley argentina nº 25.326, aclara que es **"**Tratamiento de datos": *Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias*.

346.7. Se puede observar que cuando se habla de protección de los datos, inmediatamente aparece la necesidad de dar seguridad a las personas que están con-

tenidas en cualquiera de esas modalidades de anotación, con el fin de evitar invasiones en la intimidad de ellas.

Sostiene Gils Carbó que:

> el tratamiento de los datos almacenados no admite clasificaciones pues todo dato puede tornarse "sensible" en la medida en que la sumatoria de datos no sensibles, que permitan hacer un seguimiento en la vida de las personas, también puede representar una afrenta a la privacidad.[163]

La defensa de la privacidad tiende a instalar reglas y principios en la formación de los bancos de datos. Asimismo, se restringe la interconexión de registros, con el fin de anular la manipulación informativa que no tiene el consentimiento anterior del afectado.

346.7. La realidad de los registros evidencia que no todos tienen finalidades informativas, es decir, que sean transmisibles a terceros. Esta característica, en consecuencia, lleva a resolver cuál es la protección que la persona ostenta: si lo es para evitar que el archivo ingrese sus datos y con esa incorporación afecte, probablemente, la privacidad; o en su caso, si la tutela se vincula a la reserva y confidencialidad (y eventual supresión) que los datos deben conservar, evitando que se concrete una hipotética transferencia que violente la intimidad de la persona al hacer públicas sus características.

En los hechos, ambas son las actitudes defensivas que tiene un individuo. Sólo que una vía se concreta desde la ley de protección de datos; y la otra, a través del *habeas data* y sus posibilidades concretas de demanda (*v. gr.:* acceso, actualización, rectificación, confidencialidad, reserva, o cancelación).

347. Clasificación de los archivos

347.1. Siguiendo la pauta establecida en el punto anterior, se pueden señalar archivos que se forman para especiales funciones que, por ello, quedan excluidas de la injerencia que el *habeas data* establece.

Los principios de la protección deben aplicarse a cualquier información relativa a una persona identificada o identificable. Para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona. Los principios de la protección no se aplican a aquellos datos hechos anónimos de manera tal que no sea posible identificar al interesado.

Pero, al mismo tiempo, la legislación y sus inevitables variables, obliga a clasificar los archivos para resolver cuáles de ellos están alcanzados por la ley y sus principios; y cuáles quedan fuera de la órbita.

347.2. El principio general de una ley de protección de datos personales es la tutela de las personas (físicas o jurídicas) *determinables*, por eso cuando está asegu-

---

[163] GILS CARBÓ, ob. cit., p. 112.

rado el anonimato o la disociación del individuo, afectado por el uso de sus propios datos personales, el archivo, registro o banco de datos que almacena dicha información no tiene el deber de registrarse aunque tiene que cumplir los imperativos legales de secreto, confidencialidad y elusión de cualquier uso abusivo que exceda la finalidad de sus registros.

El deber de secreto (o anonimato) básicamente se instala desde el primer momento que comienzan a tratarse datos personales, esto es, desde el proceso de recolección, y se mantiene hasta el tramo final cuando la información se transfiere o se emiten los resultados del trabajo (*v. gr.:* mediciones de la encuesta; conclusiones estadísticas; etc.).

347.3. La ley 25.326 de Argentina enuncia (de manera que la lista es meramente indicativa) los siguientes tipos de archivos que quedan fuera del deber de vigilancia y control: *a)* encuestas de opinión; *b)* mediciones; *c)* estadísticas; *d)* prospección de mercados; *e)* investigaciones científicas; *f)* investigaciones médicas y *g)* otras actividades análogas.

En cada caso se exige que los datos recogidos *no puedan atribuirse a persona determinada o determinable.*

a) Las *encuestas de opinión* que la ley se ocupa, son aquéllas donde se pidan datos personales que se vuelquen al documento; dejando fuera las opiniones vertidas en ocasiones circunstanciales que sirven únicamente como dato sobre un aspecto general. Sin embargo, puede ocurrir que una opinión (por ejemplo, de contenido político) se relacione con la persona que la emite y, a partir de esa vinculación, se produzca un tratamiento discriminatorio.

En este caso puntual ¿procede el *habeas data*? ¿Cómo se protegen los datos personales?

Creemos que no es este un problema emergente del uso de datos, sino de otras situaciones normadas como sería en el aspecto reseñado la ley que persigue evitar los tratamientos discriminatorios. Ahora bien, un reclamo sobre la base de datos sería posible en razón que se toma conocimiento de la opinión de alguien, porqué el archivo no ha mantenido reservado o secreta la identidad del individuo; es decir, ha violado el deber de disociación o anonimato.

b) Las *mediciones* son resultados concretos de un proceso que se almacenan en un archivo. Estas son conclusiones que pueden provenir de servicios estadísticos oficiales como de cualquier otro tipo de consultora pública o privada. Por eso, no hay diferencias entre mediciones de carácter administrativo y datos estadísticos.

> Aunque habitualmente los datos estadísticos —dice Velázquez Bautista— se distinguen por su carácter de anónimos, en el momento de la recogida suele solicitarse el nombre y apellido, domicilio, etc., de aquél al que conciernen los datos, hecho que supone encontrarnos con una serie de datos gracias al nombre y apellidos que se pueden relacionar con una persona concreta.[164]

[164] VELÁSQUEZ BAUTISTA, ob. cit., p. 79.

c) Las *estadísticas* y los datos obtenidos de ellas, no pueden identificar a la persona que los aporta, ni aplicar esa información para otras finalidades (*v. gr.:* fiscales, policiales, etc.). Tampoco se pueden requerir datos sensibles, y de hacerlo, la persona se puede negar amparado por los principios de protección a dichos datos especiales.

Antes de procesar datos estadísticos se deben disociar los datos personales, de manera que sea imposible la identificación individual. Ante la eventualidad de vulnerar este derecho al anonimato, la información recolectada se debe destruir sin más trámite.

El secreto estadístico es una figura propia del derecho administrativo, y consiste en la obligación de preservar el anonimato de los datos individuales, obtenidos en la realización de las actividades estadísticas para los servicios estadísticos de las administraciones públicas, a fin de proteger el bien jurídico que constituye la intimidad de las personas, entendido en el sentido más amplio de aquello que hoy se denomina privacidad.[165]

> El secreto estadístico constituye un deber jurídico por mandato imperativo de la ley que obliga a todo el personal estadístico y también a las personas físicas y jurídicas que tengan conocimiento de la información estadística individualizada y a los órganos de la administración titulares de la función pública estadística, a no difundir ni directa ni indirectamente datos individuales o individualizables de los suministradores de la información...La aplicación del principio del secreto estadístico comporta también la prohibición de actuar sobre los datos personales, de utilizarlos para otras finalidades no estadísticas o ilegítimas y de posibilitar el cruce con datos de diversos ficheros. En definitiva, existe un vínculo obligacional en el contenido jurídico del secreto estadístico: por una parte la obligación legal de declarar los datos para la realización de actividades estadísticas; de otra, el imperativo legal de mantenimiento del secreto estadístico y también la obligación legal de difusión pública de los resultados estadísticos.[166]

d) Las actividades de *prospección de mercados* llevan el mismo sesgo que los comentarios anteriores: no se puede permitir -ni tolerar- que se asocien datos personales con los resultados del estudio, porqué de ese modo se vulnera la garantía que la ley de protección de datos personales tiene hacia la intimidad y el honor de las personas.

e) Las *investigaciones científicas*, como las *investigaciones médicas*, a las que ya nos hemos referido, señalan muchos de los problemas que ocupan a los archivos, registros o bancos de datos médicos, y en particular, los que se relacionan con la investigación (*cfr*. arts. 5 inciso 2 apartado d, 7 inciso 2, 11 inciso 3 apartado d, y 12 inciso 2 apartado b).

Los datos médicos son datos sensibles, y por ello la lógica preocupación del legislador por conservar y mantener la legalidad de las bases de datos, sin perjuicio del alcance punitivo que oportunamente señalamos.

---

[165] BACARIA MARTRUS, Jordi, *El secreto estadístico (contenido jurídico),* Informática y Derecho nº 6/7, UNED, Mérida, 1994.

[166] BACARIA MARTRUS, cit., *passim*.

Se ha dicho que la reglamentación de los bancos de datos, usados con fines de salud pública, administración de servicios médicos, y de salud, o para el progreso de la ciencia médica debe tener en cuenta la preeminencia de los derechos y libertades individuales.

347.4. En adelante hemos de clasificar los archivos tomando como guía provisional la división en dos grandes sectores (públicos y privados) que, posteriormente, se van segmentando para centrar su principal actividad.

Pérez Luño establece tres modelos de bases de datos:

> *a)* bases de datos *jerárquicas,* en las que los datos están organizados por relaciones de jerarquía que pueden representarse de forma arborescente a partir de una raíz común; *b)* bases de datos *reticulares*, en las que las distintas informaciones se organizan a través de una pluralidad de puntos de acceso; *c)* bases de datos *relacionales*, en las que los datos se estructuran sistemáticamente en relaciones homogéneas que permiten al usuario seleccionarlas y adaptarlas a sus necesidades operativas.[167]

a) *Archivos públicos* y *privados*

Públicos son los registros que tiene el Estado para el almacenamiento de datos relativos a una actividad que, por seguridad jurídica, se debe mantener custodiada y con un respaldo documental. Pueden transferirse a terceros, y por lo general, son informaciones que están disponibles a cualquiera sin más requisitos que la solicitud fundamentada.

Privados son los archivos que se conservan por personas físicas o jurídicas con una finalidad determinada. Si resultan para una simple información personal (*v. gr.:* base de datos científica; archivos con perfiles sociales; etc.) no afectan la intimidad mientras no se logre identificar a persona alguna en particular (en cuyo caso, el afectado podría requerir el acceso a la base y requerir explicaciones sobre la finalidad del registro).

b) *Archivos manuales* e *informáticos*

La protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual.

Los archivos manuales constituyen una parte de la historia del mundo, como lo acreditan las leyes *Aelia Sentia* y *Papia Poppaea* de la Roma del emperador Augusto en el año 9 a.C.; fueron la modalidad habitual desde la creación de la imprenta y uno de los grandes poderes de la iglesia con sus actas de fe. En los últimos siglos los registros constituyeron el testimonio manifiesto del derecho de propiedad.

La informática, como hemos dicho largamente, modificó sustancialmente el espacio y el tiempo para conservar la información. Por todo ello el alcance de la protección no debe depender de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión.

---

[167] PÉREZ LUÑO, *Ensayos de informática jurídica,* cit., p. 37.

> La Comunidad Económica Europea a través de la Directiva sobre Tratamiento de datos señala, en cuanto respecta al tratamiento manual, que sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas. En particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva.

c) *Archivos de Seguridad del Estado*

En Europa, tanto el Convenio 108 del Consejo emitido en el año 1981, como la Directiva 95/46 y las legislaciones locales que ratificaron el criterio allí mentado, han sostenido que existen datos cuya protección es manifiesta (ordinaria) y otros que merecen una defensa especial al implicar un riesgo mayor para la intimidad de las personas, en cuanto son los que revelan ideología, creencias religiosas, afiliación sindical, origen racial, salud y vida sexual (datos sensibles).

Los archivos de seguridad, generalmente están excluidos de la injerencia del *habeas data*, lo cual no obsta a que se pueda efectuar un control directo sobre las bases de datos, toda vez que, siendo bancos de información del Estado, la reserva y confidencialidad queda limitada por el conocimiento y admisión expresa que el afectado pueda tener sobre el registro.

El caso *Urteaga* que falló la Corte Suprema de Justicia de la Nación Argentina, fue paradigmático por esta razón. Sostiene en una de sus partes que_

> …dado que el *habeas data* se orienta a la protección de la intimidad, el giro ´datos a ella referidos´ debe ser entendido como el reaseguro del derecho básico protegido por la norma, como medio de garantizar que sea el titular de los datos el que pueda obtener el desarme informativo del Estado, o de quien fuere, para poder decidir acerca del destino y contenido de dichos datos. Pero, además, en tanto el texto constitucional permite ejercer un control activo sobre los datos, a fin de supervisar no sólo el contenido de la información en sí, sino también aquello que atañe a su finalidad, es evidente que se trata, a la vez, de un instrumento de control. Por lo tanto, no es posible derivar de la citada expresión un permiso genérico para que el Estado se exima de su "deber de información", pues ello significa divertir su sentido fundamental (C.S., 15 de octubre de 1998, "*Urteaga, Facundo Rául c/ Estado Nacional – Estado Mayor Conjunto de las Fuerzas Armadas s/ amparo –ley 16.986*").

Los registros de datos de personas físicas solamente pueden quedar intangibles cuando la causa del secreto justifique la reserva, al punto que si la pretensión de difusión o conocimiento que reclama el presunto afectado, pueda vulnerar la razón de Estado que autoriza la confidencialidad estricta.

En España, la Ley establece en el artículo 22 sobre "*Ficheros de las Fuerzas y Cuerpos de Seguridad"* lo siguiente:

1) Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley. 2) La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad. 3) La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales. 4) Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

La decisión, obviamente, es jurisdiccional, porqué sólo los jueces están en el punto de equilibrio exacto que la resolución merece.

El artículo 23 inciso 2º de la ley 25.326 (Argentina) establece que:

El tratamiento de datos personales con fines de defensa nacional o seguridad publica por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categorías de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad publica o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categoría, en función de su grado de fiabilidad.

En suma, todos los datos personales contenidos en bancos de datos han de sufrir mínimas limitaciones en el acceso a la información y consecuencias que de ella deriven.

Si se toleran excepciones, como las que menciona el artículo 17 de la ley argentina referida; ellas deben ser fundadas y obliga a categorizar la calidad de los archivos; cuestión que se ha delegado en el Poder Ejecutivo de la Nación.

ART. 17 (*Excepciones*):

1. Los responsables de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión de datos de carácter personal en función de la protección de la defensa de la Nación, o de la protección de los derechos e intereses de terceros.

2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de

control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

d) *Archivos históricos*

Un ejemplo lo presta el "Archivo General de la Nación Argentina" creado en 1821 donde conviven las historias públicas y privadas de quienes nos precedieron, con sus proyectos, sus esperanzas y también sus fracasos, porqué la historia —tal como se presenta al Archivo en su página web— se construye con la totalidad de los acontecimientos y de sus protagonistas.

El archivo histórico contiene intimidades de héroes y personajes de la vida y tradición de los pueblos, que se exponen al conocimiento público como una muestra de sus personalidades.

En principio, podría afirmarse que la historia se cuenta por experiencias de investigación y análisis, y lo que se transmite es producto de esa labor; sin embargo, ¿puede un dato histórico ser eliminado por afectar la intimidad de un prócer? Si fuera afirmado que tal o cual personaje era adicto a tal estupefaciente; o, eventualmente, que era afecto a inclinaciones sexuales morbosas o diferentes, ¿puede el historiador, un familiar, una línea de descendencia, provocar la rectificación del dato o la supresión del mismo?

Evidentemente, son exposiciones de características muy personales de nuestros antecesores, y la probable justificación de ser hombres públicos, aparentemente, no sería causa bastante para fundamentar el dato publicado. Por ello, la afectación a la intimidad sería evidente, e hipotéticamente, procedería el *habeas data*.

Sin embargo la afirmación no puede ser rotunda ni perentoria toda vez que el archivo histórico conserva una información periodística, o un documento oficial o privado del cual surge el dato, o el producto de una investigación, o bien un libro que cuenta esa parte de la historia personal, y como tales son fuentes que hipotéticamente no pueden revertirse por el *habeas data*, sino a través de una nueva investigación, o del derecho a réplica cuando el archivo es reciente y el afectado puede entablar la acción reparatoria.

La trascendencia de un Archivo Histórico se puede encontrar en la memoria que representa para un pueblo tener documentados los hechos y sus personajes. En la legislación especial encontramos que el artículo 4° del decreto ley 19414, ley de defensa, conservación e incremento del patrimonio documental del Perú, que permanece vigente, exceptúa a los organismos de la defensa nacional (Ministerios de Guerra, Marina, Aeronáutica, hoy de Defensa, el del Interior, y Relaciones Exteriores) a transferir la documentación que cumple 30 años al Archivo General de la Nación (AGN), que han sido calificados como "Confidencial", "Secreto", o "Estrictamente Secreto" y sólo pueden transferirse cuando hayan perdido dichas clasificaciones. En la práctica nunca se procedió a evaluar los documentos que podían superar la clasificación y entró en está categoría toda la documentación de las mencionadas instituciones. El reglamento del decreto ley, decreto supremo

022-75-ED en el artículo 6° además agrega que los documentos perderán dichas clasificaciones previa autorización del Titular del Sector. En el año 1992 se logró avanzar algo, al introducirse una norma en el D.S. 008-92-JUS Reglamento de la ley 25323 del Sistema Nacional de Archivos, el artículo 37 que ratifica que son documentos confidenciales, secretos y estrictamente secretos los que tienen que ver con la defensa y seguridad nacional, pero agrega que cada entidad debe establecer sin excepción sus respectivas tablas de clasificación hasta por un período no mayor de 30 años para su conocimiento público. La legislación peruana según el artículo 4° primer párrafo, del decreto ley 19414, Ley de defensa, conservación e incremento del Patrimonio Documental, exige que las entidades públicas transfieran su documentación mayor de 30 años al Archivo General de la Nación, y aunque no establece categóricamente que luego esta documentación se pondrá al servicio de la investigación por calificarse como de valor histórico, interpretamos que es el plazo fijado para definir esta categoría poniéndose al libre acceso de la investigación por considerarse de valor histórico.

La ley 25323 del Sistema Nacional de Archivos del Perú, de conformidad con el artículo 5°, inciso e) faculta al AGN a normar el acceso a toda clase de documentos estableciendo los términos y modalidades de uso en concordancia con los dispositivos legales pertinentes, y el Decreto Supremo 008-92-JUS, su Reglamento en el Capítulo IX De la accesibilidad a la información en sus artículos 34 a 39 legisla sobre el tema entendiéndose por accesibilidad a la disponibilidad de los documentos para la consulta mediante el servicio que debe ofrecer todo archivo, de todos los documentos que conforman el Patrimonio Documental de la Nación sean públicos o privados, y taxativamente comprende a todos los archivos que integran el Sistema Nacional de Archivos exceptuando aquellos que puedan atentar contra los intereses y la seguridad nacional y a la privacidad o intimidad personal. Respecto de los archivos privados señala que en los respectivos convenios que celebren con el AGN se establecerán los términos de accesibilidad a la información de sus documentos.[168]

e) *Archivos penales*

La información sobre antecedentes personales es diferente del registro de conductas penadas por la ley. Por ello, el *habeas data* procede en cualquiera de los supuestos ya citados con el fundamento de resolver el tratamiento de datos automatizados de carácter personal cuando la base o archivo ofrezca una definición de características personales o un perfil individual; no así cuando la información proporcionada refiere a los antecedentes penales de la persona.

El artículo 7 inciso 4º de la ley argentina nº 25.326 establece que: *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*.

Un solo ejemplo sirve para ilustrar este punto de manera más que suficiente: en cualquier democracia, la vista de un procedimiento penal en la que se dicta sentencia es publica,

---

[168] MENDOZA NAVARRO, Aída Luz, *Base legal sobre el acceso a la información y a los archivos en el Perú,* Comunicación presentada en el "Seminario Internacional de Archivos de Tradición Ibérica, Río de Janeiro-Brasil", 3 al 7 de abril del 2000, *passim*.

> pero en todas y cada una de nuestras democracias —afirma Marcel Pinet— los antecedentes penales, que son los archivos de las condenas que se dictaron de manera pública, son uno de los archivos más protegidos y menos accesibles. Esto es un ejemplo de como cuando se recopila información, ésta toma un valor informativo específico. Esta es la razón por la que un fallo del Tribunal Supremo de los Estados Unidos, del 22 de marzo de 1989, denegó la petición de unos periodistas para serles comunicadas las sentencias de varias personas ligadas a la mafia, aunque éstas se habían dictado públicamente. El tribunal precisó que al evaluar los intereses en conflicto, "la infracción del derecho al respeto de la vida privada de un ciudadano, resultante de la difusión de sus antecedentes penales, superaba el interés público que se obtendría del ejercicio de la libertad de prensa".[169]

El antecedente penal, puede incorporarse entre los registros o bancos de dato de información judicial, y en este grupo se advierte la trascendencia del problema a resolver cuando se difunde un dato proveniente de dichas fuentes.

En efecto, las bases de datos incorporan decisiones judiciales tomadas respecto a personas físicas y jurídicas; algunas veces, son resoluciones adoptadas en el curso del procedimiento (lo cual supone su provisoriedad) de modo tal que solamente con la sentencia (firme y definitiva) el dato es actual y exacto.

Pero un conflicto habitual en los medios de comunicación es transferir situaciones procesales no firmes como si fueran tales, afectando en consecuencia algunos principios o garantías procesales que se destinan hacia la persona (en la dimensión de sus propias libertadas, como la presunción o estado de inocencia; o la continuidad de la empresa en los procesos fallimentarios) y hacia el órgano judicial (debido proceso, defensa de las personas, imparcialidad del juez, etc.). En estos casos, el dato se obtiene de una fuente judicial fidedigna, es verdad, pues el acceso a la información no está vedada en las actuaciones jurisdiccionales, salvo en situaciones muy especiales. El inconveniente aparece en la forma como se difunde el dato.

> Estas informaciones en las que puede aparecer nuestro nombre y apellido, se reflejan periódicamente en los medios de comunicación como fruto del ejercicio del derecho a la información, y por lo que a este punto se refiere —sostiene Velázquez Bautista— "sentencias", su difusión responde también al principio de publicidad de la actuación judicial. También se tratan informáticamente por personas que no forman parte o son colaboradores de la administración de justicia, constituyendo así, bases de datos que se utilizan con finalidades diversas.[170]

Creemos que el *habeas data* no es la vía idónea para impedir la difusión del dato penal (o judicial), en la medida que las actuaciones judiciales no son bases o bancos, ni archivos o registros, y aún a pesar de la existencia del registro de sentencias.

La situación debiera entender dos problemas diferentes. El que transmite la información debiera reservar en la difusión sólo el dato consistente en la situación procesal, y nada más. Es imprescindible resguardar la reserva y confidencialidad de otros datos que surgen del relevamiento jurídico efectuado en las etapas sumariales

---

[169] PINET, ob. cit., p. 75.

[170] VELÁZQUEZ BAUTISTA, ob. cit., p. 188.

donde necesariamente se investigan aspectos de la personalidad que no son parte de la información a comunicar.

> La manipulación y la posibilidad de conocerse al momento de celebrar un contrato u otorgar un crédito por una institución financiera también deben ser limitadas, al menos en el tiempo, porque las personas tienen derecho a ser perdonadas. A esta situación aludía el *artículo 22 del Título III (proyecto* para Chile), que intentando terminar con los registros o boletines llamados "históricos", se preocupa de fijar plazos para proveer o suministrar información a terceros (lo que no hace propiamente un acreedor sino más bien empresas comerciales que lucran —y "Abusan del Derecho"— prestando servicios de solvencia patrimonial). Según el proyecto no puede hacerse pasados 3 años desde que la obligación se canceló o transcurridos 10 años desde que la obligación se extinga por cualquier causa legal.
>
> Agrega Jijena Leiva que, los datos patrimoniales "positivos" tales como monto de ingresos, de acciones que se poseen, de participaciones en sociedades, de depósitos bancarios, de bienes muebles e inmuebles, etc., no deben por regla general o en principio ser procesados y menos perfilados o cruzados con otros.[171]

Por ello, en 1997 la Comisión de Bélgica afirmaba que:

> la posibilidad de usar bases de datos centralizadas o integrales para buscar los antecedentes penales de una persona crea riesgos para la protección de datos que son totalmente desproporcionados respecto a los medios tradicionales de acceso o publicación de los casos judiciales…La evolución tecnológica debe ir acompañada de una mayor discreción respecto a la revelación de la identidad de las partes que se encuentran en los archivos de los casos judiciales.

El otro aspecto del tema es qué puede hacer el afectado cuando se transmite información sensible además de aquella que se vincula con sus antecedentes penales.

En estos casos el registro de antecedentes penales, o el de sentencias, o toda información que surja de un expediente judicial, debe permitir al interesado el derecho de exigir que la información que se transmita sea únicamente respecto a la decisión final adoptada sin agregados. Por ejemplo, si la sentencia decide la exclusión del hogar de una persona y el embargo de sus bienes, no se podría complementar la información indicando cuales son los inmuebles o valores afectados ni el lugar del que se lo excluye.

El Consejo de Europa ha recomendado la eliminación inmediata de todo dato personal que no sea necesario para el sumario policial, a cuyo fin se establecieron tres categorías de actuaciones de investigación: en *primer lugar* las dirigidas a prevenir o, en su caso, reprimir amenazas graves e inminentes para la defensa del Estado, orden y seguridad pública, siempre que sean cometidas por bandas o grupos organizados; en *segundo lugar*, las previstas para prevenir otros peligros reales para

---

[171] JIJENA LEIVA, Manuel, *Carta…,* publicada en *Boletín Hispanoamericano de Informática y Derecho*, año I, nro. 5, octubre-noviembre, 1998.

la seguridad pública, distintos de los anteriores; y en tercer lugar, las que reprimen infracciones penales que requieran la utilización de datos personales, sean o no especialmente protegidos.

Los criterios para la cancelación de oficio de los datos personales son diferentes en cada categoría de actuaciones, de suerte que los datos personales registrados para investigaciones relacionadas con la primera categoría de actuaciones policiales estarán sujeta para su cancelación a los regímenes procesales locales; los datos recabados para las investigaciones relativas a la segunda categoría de actuaciones se cancelarán en el plazo de cinco años a contar desde el momento en que no se incorporen nuevos datos a la investigación concreta de que se trate; y finalmente, en relación con los datos recabados para las investigaciones a que se vincula la tercera categoría, se cancelarán en el plazo de cinco años siempre que recaiga sentencia condenatoria; el plazo comenzará a contar desde que se cumpliere la misma o desde el indulto o remisión de la pena. Asimismo procederá la cancelación inmediata de los datos cuando recaiga sentencia firme absolutoria o auto de sobreseimiento libre por no ser los hechos constitutivos de delito.

> Otro aspecto al que se debe prestar atención, es la transmisión del dato penal requerido por otro Juez interviniente, pues si lo que se pretende es mantener la confidencialidad, no debiera en caso alguno solicitarse por el Juez civil o penal o de cualquier otra jurisdicción, más datos de los que son absolutamente necesarios. También, es preciso garantizar la reserva del trámite, de modo tal que en el mismo intervengan solamente aquellos que pueden ver la información. Inclusive, para las partes el alcance del secreto debiera extenderse impidiendo la extracción de copias del expediente donde figure la información sensible.

f) *Archivos científicos o de investigación*

Las bases de datos que, generalmente, se constituyen con fines de investigación están excluidas del ámbito donde actúa el *habeas data*. No interesa que la información sea transmitida a otros o se negocie con el almacenamiento logrado.

El art. 8º de la ley argentina dispone (Datos relativos a la salud): "Los establecimientos sanitarios públicos o privados y los profesionales vinculados a la ciencia de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando los principios del secreto profesional".

La única excepción resulta cuando en el archivo, o en la cesión, se mencionan expresamente personas físicas a las que se da un perfil determinado, una vez efectuado el tratamiento de los datos que le conciernen.

Por ejemplo, en la investigación científica sobre una enfermedad (*v. gr.:* SIDA, Diabetes, Cáncer, etc.) suelen tomarse casos testigos que, ineludiblemente, vinculan a personas determinadas que padecen el mal. Estas son identificadas, caracterizadas, seguidas permanentemente hasta en mínimos detalles, y todo ello se registra y archiva en el banco de datos.

Esta información personal que divulga a otros un dato sensible, no obstante ser un archivo con finalidades científicas, necesita protegerse a sí mismo para lograr

mayor seguridad, evitando transferir datos que afectan la intimidad de los seres investigados.

> Debe considerarse —afirma Herrán Ortiz— que el almacenamiento de determinadas informaciones relacionadas con la salud conlleva un peligro añadido, en otras palabras, no será preciso para conocer la enfermedad de un paciente registrar ésta explícitamente, porqué a través de la información relativa a determinados fármacos, puede deducirse fácilmente la enfermedad que padece la persona.[172]

La recomendación nº 81 del 23 de enero de 1981 del Consejo de Europa sostuvo entre sus fundamentos que era imprescindible considerar la relevancia del tratamiento automatizado de los datos médicos de una persona pues éstos forman parte de la esfera más íntima de las personas y *la divulgación injustificada de los datos personales de carácter médico puede ser luego el origen de diferentes tipos de discriminaciones y también de violaciones de derechos fundamentales.*

> La actual recomendación sobre datos médicos R.97/5 se detiene especialmente en tratar el problema de la investigación científica y los datos médicos, estableciendo el principio general del tratamiento anónimo de los datos médicos con dicha finalidad, si bien cuando no sea posible no impedirá de forma absoluta la realización de las investigaciones.[173]

Un desvío potencial es la adquisición de la base informativa por parte de laboratorios que pretenden anticipar resultados con la producción de fármacos; o desde otra perspectiva, la segregación laboral de personas que padecen una determinada enfermedad (lo cual, quizás tampoco sea materia del *habeas data* —pues el dato es preciso aun siendo sensible— aunque permita una acción de amparo por segregación).

> En Francia, las personas portadoras del virus del SIDA deben incorporarse inmediatamente a una base de datos a cuyo fin el médico está obligado a dar la información (Decreto del 31/10/82). Luego, informa Herrán Ortiz, pensando en las investigaciones epidemiológicas y estadísticas de la enfermedad, se ha adoptado una disposición que trata de garantizar los derechos de la persona seropositiva, imponiendo la necesidad de la autorización expresa del afectado con anterioridad al registro de la información y al empleo de un proceso criptográfico de archivación, logrando que la información permanezca disociada incluso para el profesional que interviene en el procedimiento.[174]

g) *Los servicios estadísticos*

El relevamiento estadístico se realiza respetando los principios de reserva y confidencialidad, porqué el resultado que se obtiene de la actividad no es aplicable a una persona en particular sino a la sociedad toda a través de medidas específicas que al efecto se resuelven.

---

[172] HERRÁN ORTIZ, ob. cit., p. 233.

[173] BACARIA MARTRUS, *El secreto estadístico (contenido jurídico),* cit., Informática y Derecho nº 6/7.

[174] HERRÁN ORTIZ, ob. cit., p. 236.

> En el secreto estadístico —afirma Bacaria Martrus— existe un doble vínculo obligacional: por una parte la obligación legal de declarar los datos para la realización de actividades estadísticas; de otra, el imperativo legal de mantenimiento del secreto estadístico y también la obligación legal de difusión pública de los resultados alcanzados.

Idéntica conclusión se aplica a los servicios estadísticos efectuados por empresas o particulares. Un ejemplo de actividad estadística es el censo poblacional que se concreta cada diez años, para el cual cada individuo debe prestar su colaboración.

A los fines de precisar la injerencia del *habeas data* sobre estos bancos de información es preciso conocer que la estadística, antes que una base de datos, es una actividad que tiene por objeto la comparación de datos y su interrelación para la medición de diversos programas (para algunos, es la ciencia que aplica las leyes de la cantidad y de su representación gráfica para condensar los hechos sociales y medir su intensidad, deducir las leyes que los rigen y hacer una predicción próxima).

> El secreto estadístico se puede considerar —a criterio de Bacaria Martrus— como secreto profesional. Es fundamentalmente, una obligación específica de un colectivo concreto y se aplica al personal de los órganos estadísticos y al de otros servicios estadísticos de las administraciones públicas como un elemento de su régimen jurídico, a la vez que se hace extensiva a cualquier otra persona física o jurídica que entre en contacto o tenga acceso a los datos estadísticos individuales o individualizados, por razón de su participación en operaciones estadísticas.[175]

El Consejo de Europa establece en el Convenio 81 (art. 5º) que estos servicios *registrarán finalidades determinadas y legítimas y no se utilizarán de una forma incompatible con dichas finalidades;* además, *serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado.*

> En España la ley 12/89 de la Función Estadística Pública considera como datos estadísticos, tanto los que se obtienen para los servicios estadísticos, como a aquellos recolectados por otros órganos de tipo administrativo. Datos que son útiles a efectos estadísticos, por lo que se facilitan a estos servicios, diluyéndose así —dice Velázquez Bautista— en este caso, la tradicional separación entre datos de carácter administrativo y servicios estadísticos.

La confidencialidad y reserva del trabajo estadístico, unido al carácter de la actividad, lo exime como sujeto pasivo del *habeas data*, aunque se puede exigir al banco de datos que ellos realizan, la aplicación de los principios que imperan para el tratamiento de datos en general.

En España, la Ley 12/1989 de la Función Estadística Pública sostiene:

> 1. Cuando los servicios estadísticos soliciten datos, deberán proporcionar a los interesados información suficiente sobre la naturaleza, características y finalidad de la estadística, advirtiéndoseles, además, de si es o no obligatoria la colaboración, de la protección que les dispensa el secreto estadístico, y de las sanciones en que, en su caso, puedan incurrir por no colaborar o por facilitar datos falsos, inexactos, incompletos o fuera de plazo.

---

[175] BACARIA MARTRUS, *El secreto estadístico (contenido jurídico),* cit., Informática y Derecho nº 6/7.

> 2. En todo caso, serán de aportación estrictamente voluntaria y, en consecuencia, sólo podrán recogerse previo consentimiento expreso de los interesados los datos susceptibles de revelar el origen étnico, las opiniones políticas, las convicciones religiosas o ideológicas y, en general, cuantas circunstancias puedan afectar a la intimidad personal o familiar.

La denuncia de los peligros que reporta la cesión de los datos logrados desde un censo poblacional, se puede evitar disociando la información, esto es, procesando los datos de manera que no se pueda establecer vínculo alguno entre el titular de los datos y la información que se obtiene.

Según Herrán Ortiz:

> así lo ha entendido el legislador español, que ha prohibido cualquier información particularizada sobre los datos personales contenidos en el censo electoral, garantizando a la persona el respeto a su intimidad personal y familiar, ya que de otro modo podría vulnerarse el derecho a la libertad individual al obtener un completo retrato de la persona a través de los datos personales que se encuentran registrados en el censo electoral.[176]

Asimismo, los funcionarios que por razón de sus cargos u oficios tomen conocimiento de datos estadísticos o censales, están obligados a guardar sobre ellos absoluta reserva.

La ley argentina sostiene en el artículo 28 que: (Archivos, registros o bancos de datos relativos a encuestas):

> 1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a la ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable; 2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.

h) *Los bancos de datos genéticos y los bancos de órganos*

Los bancos de datos genéticos contienen información que permite estudiar enfermedades y otras características de la persona humana a partir de su estructura genética.

Informa Uicich que:

> en Islandia se ha permitido a una empresa manejar la información genética y las historias clínicas de los habitantes de ese país. La ley sancionada en 1998 le otorgó por 12 años el estudio de los factores genéticos que inciden en las enfermedades de los habitantes de la nación isleña, quienes han conservado su genealogía desde 1915 y no muestran rasgos de mezcla genética hasta la segunda guerra mundial (lo cual los constituye con una genética propia). Según la empresa, esta base de datos tiene por objetivo comprender los factores genéticos que inciden en las enfermedades, generar una medicina predictiva y mejorar el resto de la administración de salud.[177]

---

[176] HERRÁN ORTIZ, ob. cit., p. 237.

[177] Uicich, ob. cit., p. 98.

Más allá de los beneficios indudables que reporta el estudio de los cromosomas para determinar fisonomías clínicas y resolver causas y tratamiento para los padecimientos de salud, lo cierto es que el tratamiento de estos datos por inescrupulosos (*v. gr.:* guerras químicas que destruyen a los hombres manteniendo la arquitectura de las ciudades) provoca un riesgo que es preferible no correr.

Estos datos pueden identificar al ser humano en detalles que hasta para él mismo podrían ser desconocidos, circunstancia que demuestra la penetración de la intimidad y la necesidad de lograr un punto de equilibrio entre los derechos potenciales que se enfrentan.

Lo mismo sucede con los bancos de órganos que cumplen una función informativa esencial para la vida de las personas a quienes concierne. Estos archivos informáticos localizan órganos humanos de donantes que voluntariamente asumen el transplante a otro quien sufre por la pérdida o afectación del mismo órgano vital.

Son fuentes de datos médicos, evidentemente, pero la acumulación de informaciones sobre la persona del donante y del destinatario es tan variada que podría comprometer la intimidad de ellas.

En nuestro parecer, estos bancos de datos se encuentran en las mismas condiciones que los bancos científicos, por lo cual las conclusiones de ellos les alcanzan.

i) *Las empresas de venta de información crediticia*

Informar sobre la solvencia económica de alguien, tiene en las operaciones financieras una importancia trascendente porque disminuye el riesgo y facilita la toma de decisiones en la asignación de créditos.

Los bancos de datos que se ocupan del tema tienen como objetivo informar a quien lo requiere y paga por ese servicio, sobre el comportamiento comercial y crediticio de una persona o empresa.

Las actividades de estas entidades son básicamente dos: la información sobre la solvencia económica, y la relativa al cumplimiento y morosidad de obligaciones dinerarias. Mientras la primera se refiere a la capacidad económica de una persona, permitiendo al interesado tener una visión sobre la confiabilidad patrimonial; la restante amplía el historial al comportamiento adoptado para responder por los créditos tomados.

A veces, como ocurre en Argentina, para el supuesto de la "*solvencia económica y crédito*" se tiene facilidad para obtener la información o el consentimiento libremente prestado para el archivo; en el caso del "*cumplimiento de las obligaciones"* se toma en cuenta la legalidad del registro cuando éste informa sobre deudas ciertas, vencidas y exigibles que hayan sido previamente intimadas de pago. De este modo, aun sin tener sentencia firme (condenatoria o absolutoria) el archivo puede informar sobre la verdad que constata, sin infringir intimidad comercial alguna.

La información ofrecida se recaba de las operaciones financieras efectuadas (*v. gr.:* compraventa de inmuebles o muebles registrables; cumplimiento en transacciones menores como la adquisición de electrodomésticos a plazos; gastos realizados con tarjetas de crédito, etc.), y de resultar moroso en los pagos o demandado en li-

tigios por cobro de sumas de dinero, se da noticia sobre juicios en trámite, sentencias condenatorias, inhibiciones y embargos, entre otra información disponible.

Por lo general estos informes de solvencia y confiabilidad se reportan como confidenciales, prohibiendo su exhibición o divulgación a terceros, especificando que en caso alguno los datos implican abrir juicios de valor sobre las personas concernidas.

¿Cuál es el problema en torno de estos archivos?

En su inmensa mayoría los procesos de amparo que contra ellos se deducen argumentan que la producción de informes personales violenta el derecho a la intimidad, además de provocar un daño inmediato al privar de crédito y apoyo económico a las actividades que se pretenden realizar.

La respuesta suele fundamentarse en que los datos informados son de fácil acceso para cualquiera por ser públicos y registrados, y que no se afecta la intimidad de persona alguna al permitir el acceso a las fuentes de información y facilitar a los concernidos las quejas que contra los datos tuvieren.

Asimismo, hay que tener en cuenta que, si la función del banco de datos es *informar* objetivamente sin emitir juicios de valor, el suministro del archivo personal responde al fin para el que fue creado y no podría, en principio, catalogarse como ilegítima esa actividad.

> Desde un aspecto subjetivo, se plantean dudas sobre si son aplicables las garantías de la protección de la privacidad a quienes operan en una actividad empresarial como ejecutivos individuales, esto es, si es o no aplicable el régimen de protección de la intimidad a la parte empresarial de la vida particular de un individuo.
>
> El desarrollo jurisprudencial en nuestro país tiene el mismo sesgo restriccionista, porqué sólo procede el proceso constitucional cuando la información proporcionada es falsa o discriminatoria. Por ejemplo, se ha dicho que "*corresponde rechazar la acción de habeas data intentada si los actores no manifiestan que la información proporcionada sea falsa, ni que revista características de discriminatoria (*en el caso se solicitaba la intimación al banco de datos demandado para que cesara de informar sobre circunstancias y hechos precluidos y comunicara a las instituciones bancarias que los actores no registraban antecedentes).[178]

La dualidad entre derecho a la información y derecho a la privacidad aparece, una vez más, en juego. Aunque en este caso, el límite se puede encontrar en las posibilidades reales que encuentre el afectado para acceder y controlar los datos que de él se ocupan.

El artículo 26 de la ley argentina sostiene: "(Prestación de servicios de información crediticia):

> 1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

---

[178] CNCom., Sala E, 1994/12/13, "*Molina, Alberto V. y otros c/ Organización Veraz S.A.*", La Ley Online.

2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.

3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.

4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico- financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho.

5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

j) *Archivos de entidades financieras*

La incorporación a una entidad bancaria o financiera comienza con el llenado de fichas informativas de datos personales, habitualmente muy exhaustivas, que persiguen formar un perfil del nuevo cliente.

Esta base debiera ser confidencial y reservada, y aplicarse para la toma de decisiones respecto a la relación bancaria específica. Sin embargo, es frecuente el intercambio de información en el sistema financiero nacional.

El negocio de la circulación de datos no es necesariamente ilegal. No siempre que se llena un cupón en un comercio se envía información a una boca de lobo delincuencial. Pero a quienes se preocupan por mantener sus empresas dentro de la ley, casos como los ocurridos en Argentina como la venta del banco de datos del sistema de seguridad social o del padrón electoral, les causan más que un dolor de cabeza. No obstante, es sabido que entre las entidades financieras existe una suerte de cooperación, con un centro informativo en el Banco Central, que les permite conocer al cliente a través de las experiencias tenidas entre las sedes y sucursales del sistema financiero.

Considerando que el *habeas data* local se encuentra previsto para controlar todo registro o banco de datos, público o privado esté o no *destinado a proveer informes (*caso de Argentina), cabe la duda respecto a determinar si la cooperación informativa puede ser controlada por este mecanismo constitucional.

La respuesta debe ser afirmativa, porqué la información voluntariamente suministrada, como requisito ineludible para acceder al sistema (igualmente sucede cuando nos alojamos en un hotel; o al completar un formulario para un sorteo; o para suscribir una editorial, etc.) se ingresa como parte de un convenio, donde la confidencia integra el conjunto. Es evidente que la ausencia de control y la falta de recursos o herramientas en manos de los particulares para poder defenderse ante una real desviación de poder en el uso de los datos revelados, puede significar no solamente perjuicio material, sino, además, una honda lesión a los derechos de la personalidad humana.

No obstante, este derecho a exigir confidencialidad no se extiende al comportamiento financiero que el interesado muestra en sus actos, pues la reserva se aplica a los datos denominados sensibles o esenciales.[179]

De todas maneras, no hay que confundir la posibilidad de transferir la conducta del cliente en las operaciones de crédito y cumplimiento de sus obligaciones, con el *secreto financiero*, que supone el deber de la entidad de mantener con discreción y sigilo los datos y bienes sobre los cuales obtiene información a raíz del contrato entre ellos suscripto.

Precisamente, toda entidad bancaria puede —sin violar el secreto bancario— ofrecer información acerca de los datos identificatorios de su cliente; no así respecto de las operaciones por éste realizadas por cuanto ella es reservada, ya que desde el momento en que el cliente circula cheques o cualquier documentación de pago, debe aceptar que los portadores de éstos están habilitados para indagar respecto de la identidad e identificación del librador.

En Argentina, el secreto bancario establecido por la ley 21.526, en su art. 39, alcanza a las informaciones que los clientes brindan a las entidades financieras a raíz de las operaciones que éstos realicen en el marco de dicha ley. Por ello, la declaración de bienes efectuada por el demandado en oportunidad de la apertura de la cuenta corriente en la entidad bancaria, se encuentra amparada por dicha norma. Asimismo, la ley 24.244 ha limitado el deber de secreto a las operaciones pasivas, beneficiando al público en general toda vez que ahora se puede conocer quiénes son los deudores de la entidad financiera donde se piensan colocar los fondos y, por consiguiente, se pueden evaluar los riesgos a asumir si efectivamente son depositados.

Así lo afirma Vázquez Arzaguet, agregando que:

> pese a ello, esta modificación no adquiere la entidad que, *prima facie*, podría pensarse que tiene. Opino que en virtud de nuestra legislación actual, puede ser revelada en sí misma toda operación de activos o de servicios, según sea el caso, pero no sucede lo mismo con los informes que se brindaron al banco para concretar la operación. Lo contrario, importaría violación al derecho de propiedad y al deber de secreto, el que no se encuentra específicamente relevado en este aspecto.[180]

k) *Los archivos fiscales*

Los bancos de datos en materia fiscal se forman esencialmente con las declaraciones juradas que efectúan los contribuyentes amparados por el secreto y confidencialidad del sistema.

---

[179] El derecho de exigir la confidencialidad de datos no se extiende a aquella información de alcance comercial o financiero. Ello es así pues tal información (cierre de una cuenta corriente por haber producido el tercer rechazo de cheques sin provisión de fondos), por su carácter, está destinada a divulgarse entre todas las entidades financieras del país tal como lo prevé la circular OPASI 2 del Banco Central (CNContenciosoadministrativa, Sala IV, 1995/09/05, Jurisprudencia Argentina, 1995-IV, 350)

[180] VÁZQUEZ ARZAGUET, Gabriel A., MIGHETTI, Carlos M., *Secreto financiero*, Depalma, Buenos Aires, 1999, pp. 66 y ss.

En la clasificación antes vista, son archivos públicos que se conservan con la finalidad de controlar el cumplimiento de las cargas públicas; y no tienen otro destino que ese, por lo cual, son personales y afectan la relación entre Estado y ciudadano. Es decir, este tipo de datos no se puede transferir a terceros.

Sostiene Christensen que:

> la Constitución en lo que hace a los registros públicos no fija el requisito que si contempla para los privados, de que los datos estén destinados a ser informados a terceros. En el caso de los registros o bancos de datos públicos no existe tal condicionamiento, por lo que torna procedente a pedido de persona interesada, la acción de *habeas data* contra la Administración Federal de Ingresos Públicos; ya que la clasificación de públicos y privados está dada sobre la base de la persona que es titular de los registros o bases de datos, no a quien accede o pueda acceder a la información de los mismos.[181]

Sin embargo, es manifiesta la intención de los organismos recaudadores –algunas veces concretada- de informar los sumarios o investigaciones que se practican a quienes pueden haber violado el deber de decir verdad en las declaraciones de impuestos. La exposición como vergüenza pública afecta la intimidad, sin perjuicio de otros intereses afectados.

Entra dentro del análisis que se efectúa, las comunicaciones que realiza el Fisco al Banco Central sobre supuestas deudas, que aun sin estar firmes por ser litigiosas, se comunican como si fueran tales; así como los potenciales incumplimientos de la seguridad social. Hace un tiempo —agrega Christensen— el Fisco remitía una nota a los bancos con los que operaba el contribuyente o responsable en los términos del artículo 12 de la Ley 14.449 y de la Circular 1703 del BCRA, a los fines de inhabilitarlo para conseguir créditos de parte de la institución bancaria.[182]

La publicidad de las presuntas infracciones (que son de este carácter al no tener sentencia que las declare e imponga las condenas pertinentes, en el caso de verificarse la violación al principio de buena fe), se convierten en un sutil mecanismo de provocación a un acto espontáneo —aunque sea obligatorio— que viola la privacidad de quien los realiza.

> El presidente de la Agencia de Protección de Datos de España, contaba en oportunidad de visitar Argentina en el año 1999 que con las cuentas bancarias de contribuyentes había surgido un problema que llevó a sostener que el conocimiento de las cuentas bancarias era necesario para proteger el bien constitucionalmente protegido, que es la distribución equitativa del sometimiento de los gastos públicos. El tema que se planteaba era si la informatización por parte de la Hacienda Pública, al pedir datos a los bancos para averiguar si las declaraciones de impuestos se habían efectuado correctamente, vulneraba o no el principio de la intimidad de las personas: y dice que no; porque hay otros valores protegidos. A la vez un pronunciamiento del propio Tribunal de 1986 sostuvo que "no

---

[181] CHRISTENSEN, Eduardo Alberto, *El habeas data como tutela en el derecho tributario,* en "Libro de Ponencias" del XX Congreso Nacional de Derecho Procesal, celebrado en la ciudad de San Martín de los Andes del 5 al 9 de octubre de 1999.

[182] CHRISTENSEN, Eduardo Alberto, ob. cit., *passim*.

> hay derechos ilimitados, por lo cual, si no hay duda de que en principio los datos relativos a la situación económica de una persona y entre ella los que tienen su reflejo en las distintas operaciones bancarias en las que figura como titular entran dentro de la intimidad constitucionalmente protegida, no puede haberla tampoco en que la administración está habilitada también desde el plano constitucional, para exigir determinados datos relativos a la situación económica de los contribuyentes".

De todos modos, el problema que presentamos (violación del secreto y confidencialidad) es diferente del que trae el sistema de registro o archivo de los datos vinculados con la actividad comercial o profesional de una persona.

En la actualidad, el derecho y la gestión comparada, muestra que para la recepción de pagos y de datos contenidos en declaraciones juradas se aplican soportes magnéticos. El objetivo tenido en consideración es el de optimizar el ingreso de datos y pagos mediante un proceso que, en forma paulatina, lleve a la supresión del papel como soporte de datos, para recibir la información declarada.

Para alcanzar esta meta es conveniente establecer un régimen de transferencia electrónica de datos, para la recepción de la información contenida en las declaraciones juradas de obligaciones tributarias que se presenten en las entidades bancarias. Este nuevo régimen se instrumenta mediante la firma de un contrato de adhesión depositado en el banco receptor habilitado, la elección por el usuario de una clave de seguridad e identificación personal y la presentación de las declaraciones juradas mediante su transmisión electrónica remota.

> La aceptación voluntaria de las reglas para presentar las declaraciones juradas, no debe suponer manifestación expresa de voluntad para que la administración ceda información aunque lo sea en miras a dar mayor eficacia al sistema de ingresos públicos. El punto debiera enfocarse en dos posiciones: en primer lugar, la información que adquiere la dirección de impuestos debe reconocerse como necesaria para el desarrollo de sus actividades; y en segundo lugar, que sólo esa información puede aplicarse para el ejercicio de sus propias competencias. Se configura así, un límite a los límites, ya que si la actividad de la administración dentro de los cauces legales constituye una valla para el ejercicio del derecho fundamental al control sobre las bases de datos que le conciernen, en tanto le impone el deber de facilitar información y le impide el acceso a la misma, no debe llevar a que, fundamentado en el cumplimiento de sus competencias, abuse de esas atribuciones legales cual tuviera un cheque en blanco para vulnerar las garantías de la libertad de intimidad y el derecho al secreto de las informaciones fiscales.

La seguridad de la base de datos (que pasa a ser eminentemente informática) se resuelve por un conjunto de mecanismos compuesto por reglas de filtrado en los ruteadores, listas de control de accesos, paredes de fuego (*firewall*), y mecanismos de encriptar por equipo (hardware) las claves de seguridad e identificación personal de los usuarios y los algoritmos de encripción.

La comunicación que se establezca entre el contribuyente y el servidor estará encriptada en tiempo real.

Las claves de seguridad e identificación personal se resguardan en un equipo con estrictas medidas de seguridad física y lógica. Ante cualquier violación, mecanismos de seguridad lógicos deberán impedir la recuperación de los datos allí almacenados.

l) *El registro electoral y las fichas de los partidos políticos*

El padrón electoral es una típica base de datos con información elemental para autorizar la emisión del voto en los sufragios de elección de representantes y autoridades.

Si bien la consulta a estas bases es accesible en tiempos preelectorales, se mantiene en reserva cuando no lo son, aunque se permite conocer los datos si la petición se realiza con patrocinio de abogado y se paga un arancel.

El carácter de archivo público unido a la función que tiene, impide considerar al *habeas data* como vía procesal idónea para acceder y solicitar algunas de las pretensiones propias del sistema de protección de datos personales, toda vez que las correcciones que se debieran hacer por actualización o rectificación deben tramitar ante la justicia electoral.

Es diferente la situación de los padrones de afiliados a partidos políticos.

> Los ficheros a que nos referimos —dice Velázquez Bautista— son para los partidos políticos como los ficheros de clientes para una sociedad mercantil. Por ello, elemento esencial en la vida de los partidos, los cuales sin una militancia cohesionada y participativa, registrada en un fichero, perdería gran parte de su potencial convirtiéndose, al menos durante un tiempo, en una fuerza testimonial. Y en función de los recursos y la aceptación del electorado, en un producto presente en la sociedad a través de un gabinete de prensa y relaciones públicas pero con un futuro incierto.[183]

Una ficha de afiliación partidaria suele requerir datos históricos de la persona. Quizá el más importante, más allá de la expresión abierta hacia un dogma, sea el domicilio y no otros como la ocupación u oficio.

La cuestión que se presenta con estos registros es la disponibilidad a terceros de una manifestación que no siempre se pretende hacer pública. Por eso, la cesión del dato a través del potencial informe necesita el consentimiento del afectado. En el sistema tuitivo que se analiza, el dato de filiación y creencia política se considera sensible, de allí el problema.

En España el dato ideológico se considera sensible pues de acuerdo con el Artículo 7 de la ley, son datos especialmente protegidos:

> 1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo. 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3. Los datos de carácter personal

[183] VELAZQUEZ BAUTISTA, ob. cit., p. 266.

que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. 4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

Evidentemente, el archivo partidario es público y no debiera ser objeto de cesión o informes a terceros, precisamente por la disponibilidad de los datos. Por tanto, el acceso al mismo es irrestricto, y las pretensiones de actualización, corrección y supresión de datos (sensibles) tramitan por el *habeas data*. No así la exclusión del archivo, porqué esa manifestación supone desafiliarse lo cual tiene su carril pertinente.

En Argentina, ni la ley 25.326, ni su decreto reglamentario definen qué es un dato sensible, solamente indica la primera en el art. 7º que ninguna persona puede ser obligada a proporcionar datos sensibles (inciso 1º); y que estos 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 (inciso 2º). Por eso, queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles…" (inciso 3º). Finalmente, la norma autoriza a la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales para que puedan llevar un registro de sus miembros.

En otra oportunidad[184] nos referimos a esta cuestión, opinando que la afinidad con un partido político o la pertenencia a un sector gremial (en el sentido de orientaciones del pensamiento) eran datos sensibles cuando esa información divulgada ponía en riesgo a la persona. Esa fue, en sus orígenes, el motivo que dieron las legislaciones que, mayoritariamente, los comprenden como datos de protección especial. Pero actualmente, la sensibilidad de esta información es relativa. En primer lugar porqué los ideales políticos pueden ser manifiestos en los casos de afiliación partidaria (que son bancos de fácil acceso) o sindical (en España para considerar dato sensible se agrega el requisito de la agremiación).

En segundo término, porqué nos parece suficiente la defensa constitucional que parte del artículo 43 cuando otorga derecho de amparo contra "*cualquier forma de discriminación*".[185] Luego, porqué en un estado democrático no se puede pensar con la sospecha incorporada en cada acto, sino todo lo contrario, hay que obrar con

---

[184] GOZAÍNI, Osvaldo Alfredo, *La afiliación partidaria como dato sensible que no se puede difundir*. La Ley, 2002-F, 1437 y ss. (diario del 14 de noviembre de 2002).

[185] En Argentina, la justicia ha dicho que las tristes experiencias de persecución ideológica vividas justifican plenamente —a través del *habeas data*— la tutela de la información relativa a la filiación política, las creencias religiosas, la militancia gremial, o el desempeño en el ámbito laboral o académico, entre muchos otros datos referidos a la persona titular del derecho, que no corresponde que se encuentren a disposición del público o de ser utilizados por órganos públicos o entes privados, sin derecho alguno que sustente su uso (CNCiv., Sala H, mayo 19/995, in re Rossetti Serra, Salvador c/ Dun & Brandstreet S.R.L., en Jurisprudencia Argentina, 1995-E, 294).

lealtad y buena fe, creyendo que la ideología no puede ser motivo de diferencias o causa de privaciones.

En todo caso, si el dato ideológico es reservado (y permanece en el banco de datos como confidencial), el deber de mantenerlo en secreto es de la base respectiva antes que de la característica intrínseca del dato. Lo mismo podríamos decir respecto a las creencias religiosas o cultos de fe, y sus antípodas, es decir, la ausencia de convicciones y el agnosticismo.

La filosofía moral puede ser notoria en actos que se manifiestan públicos, pese a que el reducto donde se lo practique (por ejemplo, la presencia en una misa supone pertenecer al culto católico y genera una presunción) pueda ser público o privado.

En otra variable, si la persona es famosa, o puede considerarse "pública" por su nivel de exposición, el dato que surge de sus actos cotidianos le otorga un perfil difícil de ocultar, y si a ello se suma la relevancia pública de los hechos (como la asistencia a un templo; el solicitar la bendición; confesarse; etc.), la calidad de dato sensible parece inadecuado para requerir el nivel de secreto perseguido.

A veces el interrogante se plantea en ambientes distintos. Mientras la *participación directa* (cargos públicos) siempre es un hecho de carácter público que está fuera del derecho a la intimidad, desde que la trascendencia y exposición del funcionario torna imposible resguardar el secreto de su adhesión al partido político; otro podría ser el caso cuando el resguardo se vincula con la *participación indirecta* (militancia o afinidad ideológica), es decir, al pretender mantener en confidencia (entre quien se afilia y la entidad que lo recibe) el ingreso a las filas de la asociación.

Sin embargo, es ésta una diferencia intangible.

En efecto, poder establecer dicha distancia para dar lugar al proceso de *habeas data* en uno u otro caso, parece por demás conflictivo. Ocurre que el derecho a mantener en secreto la afiliación es un contrasentido, porque justamente se trata de incluir a la persona en las actividades públicas directas (designaciones eventuales en cargos públicos) o indirectas (militancia o acompañamiento sin actividad) del partido político, cuyo carácter público es evidente (*cfr*. art. 27 de la Ley argentina nº 23.298).

El derecho a mantener en secreto la ideología es diferente cuando no se trata de afiliación expresa. Se parece a la reserva personal sobre hechos y pasiones que la persona conserva para sí; pero excede la privacidad determinada por uno cuando esos aspectos llegan a ser conocido por otros a través de acciones voluntarias (por ejemplo, exponer una conferencia; dar una opinión escrita; etc.). En estos casos, aunque el dato ideológico no se quiere transferir, el pensamiento hecho público impide o anula el motivo de expreso ocultamiento.

m) *Los registros sociales y culturales*

Los archivos o registros de entidades sociales, culturales o deportivas, son de uso estrictamente interno para resolver el acceso a la institución, y posteriormente, mantener informado al adherente sobre actividades y obligaciones emergentes de la asociación.

La calidad de fichero privado que no está destinado a proveer informes, en principio, lo desplaza de la injerencia del *habeas data*.

> Se ha dicho que, si el objeto de la acción de *habeas data* es tener acceso a la información relativa al peticionante, el retiro de la credencial que lo autorizaba a ingresar al casino militar no es un hecho sobre el que haya que emitir opinión jurisdiccional. Por ello, la denegatoria a la admisión como socio de un club, no se halla incluida dentro de los presupuestos de admisibilidad del *habeas data*, *salvo que para tal negativa se haya tenido en cuenta algún dato descalificante o discriminatorio que conste en sus propios archivos*, pero no alcanzan esta categoría ni el listado de socios ni el registro de pago de cuotas.[186]

n) *Los archivos profesionales y ocupacionales*

Las fuentes de información no necesariamente están ordenadas en bancos o archivos específicos, a veces, el simple ordenamiento de los papeles privados que se reúnen con motivo o en ocasión del trabajo, forman un archivo de datos que, posiblemente, contengan información íntima de las personas a quienes se atiende.

El abogado, el médico, el periodista, entre tantas profesiones y ocupaciones conservan materiales de uso particular que involucra a otros a quienes se debe reserva y confidencialidad.

Probablemente, la sofisticación de estas bases de datos y la penetración de otras fuentes de información mediante sistemas informáticos, termine considerando a estos archivos o ficheros, como "bancos de datos privados", tal como acontece en legislaciones demasiado proteccionistas.

En Argentina, la ley 25.326 en el art. 24 de la ley sostiene: (Archivos, registros o bancos de datos privados): *Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21*.

Sin embargo, el problema no es la formación del archivo sino la transmisión del dato sin el consentimiento de la persona.

Por tanto, la cuestión tiene una dimensión vinculada con la privacidad del fichero personal, que por su calidad se debe incluir en el concepto de "papeles privados" de protección constitucional; y otra vertiente que refiere a la responsabilidad del profesional que conoce el dato y lo cede a otros sin el consentimiento del concernido.

Dalla Vía y Basterra opinan que:

> los registros o bancos personales para uso privado no están comprendidos dentro de los registros con posibilidades de acceso; sí estarían comprendidos aquellos bancos de datos de profesionales que puedan tener uso público, y si bien una ley reglamentaria determinará los casos en que es posible el acceso, en definitiva los jueces decidirán en cada caso concreto si es procedente o no la acción.[187]

---

[186] C. Fed. Bahía Blanca, Sala 1ª, 1995/01/18, La Ley, 1996-A, 316.

[187] DALLA VÍA, Alberto R., BASTERRA, Marcela Izascum, *Habeas data y otras garantías constitucionales,* Némesis, Buenos Aires, 1999, p. 38. Ver también, BASTERRA, Marcela I., *Protección de datos personales,* Ediar-Instituto de Investigaciones Jurídicas de la UNAM, Buenos Aires, 2008, pp. 38 y ss.

Sección 6ª El control sobre los archivos que contienen datos personales

347. Límites y alcances de la protección constitucional

347.1. El fenómeno actual del *tratamiento de datos* debe ser analizado en consonancia con el tiempo en que transcurre y avizorando el futuro que nos llega, pues el derecho comparado que en nuestros días se dispone, probablemente, está adecuado a circunstancias y necesidades de cada lugar, y proyectadas, puede ocasionar en otras sociedades una modificación o una interpretación distinta a sus reglas y valores.

En este sentido, es evidente que la era de las comunicaciones que se avecina y constituye hoy una realidad palpable, transforma algunos conceptos y derechos fundamentales. Por ejemplo, la noción de privacidad que tanto espacio dedicamos en los capítulos precedentes, donde la idea de estar solos afinca el derecho individual, personalista y de profundo contenido singular (como derecho de propiedad), es evidente que torna hacia otra inteligencia, por la cual, ese mismo derecho a la soledad se refiere al libre desenvolvimiento de la persona en sus esferas privadas (propia y familiar) y públicas (actuación social y profesional).

Es el cambio que obliga a adecuar las normas y principios fundamentales. No para variar su finalidad, sino para darles posibilidad de eficacia evitando declamaciones que no puedan ser realidades.

Para Herrán Ortiz:

> el estudio de los procedimientos idóneos para la defensa de la persona frente a las prácticas abusivas, significa tener que adecuar las esferas de los derechos y libertades fundamentales, como son la intimidad, el honor, la imagen, la libertad de conciencia, entre otros, al fenómeno del tratamiento automatizado de datos personales, que viene a introducir una penetración diferente a la conocida en el reducto de la privacidad.[188]

347.2. En consecuencia, pensar que se podrá evitar la inmiscusión informática en el ámbito de lo personal, cuando la práctica cotidiana nos lleva a vivir una sociedad plenamente informatizada, parece una utopía, lo que no impide que se formulen reglas y principios que lleven a la convivencia armónica entre la persona y los medios, y en definitiva, a obrar con sentido preventivo antes que reparador.

---

[188] Herrán Ortiz, ob. cit., p. 269.

Nos parece que la regulación constitucional del *habeas data* tiene dicho sentido garantista que actúa *ex post facto*, cuando la sensación de seguridad debe partir antes de que el conflicto suceda; razón por la cual, la garantía procesal necesita de una ley de protección de datos que tenga en cuenta lo trabajado en convenciones y tratados internacionales y las idiosincrasias particulares.

Por ahora, la interpretación constitucional necesita obrar con elasticidad evitando el aislacionismo tradicional de la jurisprudencia, que continúa atrapada en el concepto de derechos subjetivos, propios e intangibles, que eluden el compromiso con la sociedad donde está inserta.

347.3. En esta materia, la tutela de la intimidad amenazada o violada por el uso de datos personales, no tiene en las normas constitucionales respuestas suficientes.

En Argentina con la creación del derecho de amparo (antes que como juicio específico, como garantía de un proceso rápido y expedito), se genera un marco procesal que evita el reduccionismo que aleja la idea de ponderar con preferencia al proceso ordinario; al consagrar una vía rápida de tipo sumarísima que facilita con holgura actuar en los términos como se la emplaza.

Antes la tutela se acotaba a los papeles privados y la correspondencia particular; hoy, en cambio, los tratados y convenciones internacionales que se incorporan a las Constituciones, señalan el rumbo para una defensa efectiva de los derechos humanos.

En suma, la supremacía de los derechos y garantías que de la Constitución emanan, lleva a fundamentar una serie de reglas y otra de principios sobre los cuales se desenvuelva el uso de los datos personales.

La ley francesa (nº 78 del 6 de enero de 1978) establece en el artículo 1º que:

> La informática debe estar al servicio de cada ciudadano. Su desarrollo debe desenvolverse en el marco de la cooperación internacional. No debe afectar la identidad humana ni los derechos humanos, ni la vida privada, ni las libertades individuales o públicas.
>
> Ninguna decisión judicial, que implicara apreciación en cuanto al comportamiento humano, podrá tener por fundamento la definición del perfil o de la personalidad del interesado dada por un sistema automatizado de informaciones… (art. 2º, aplicado con idéntico sentido a las decisiones administrativas y privadas)

347.4. La dignidad humana puede instalarse como punto de partida, para ocupar derechos como la identidad, el honor, la imagen, la reputación personal, y el derecho a que la vida privada no sea alterada por invasiones informáticas no queridas.

Cuando el consentimiento para el uso de los datos no sea manifiesto, el principio a rescatar será el denominado por otras legislaciones como "autodeterminación informativa", base del proceso de *habeas data* que facilita el acceso al banco de datos y permite formular las pretensiones consecuentes.

Explica Casallo López que:

> el consentimiento o "autodeterminación informativa" debe considerarse como un principio general, ya que toda norma tiene excepciones. Esto significa que el titular del dato es el que debe dar su consentimiento para que el mismo pueda ser recogido y transferido a

> un tercero: sin el consentimiento expreso del interesado ninguno de sus datos personales puede ser tocado. Más aún, para que ese consentimiento sea válidamente emitido tiene que ser libre y, fundamentalmente, suficientemente informado por el titular, porque si carece de la necesaria información el sujeto puede estar consintiendo algo que desconoce y automáticamente nos hallaríamos ante un consentimiento nulo, o viciado de nulidad.[189]

Con esta plataforma, ensanchada por la tutela amplia al derecho de intimidad, la persona ha de promover sus derechos a la información (a saber si está en la base de datos y para qué fines fue almacenado); a la privacidad (persiguiendo la eliminación de fastidios directos o indirectos a su vida familiar y personal); a exigir que los datos consignados sean fehacientes y veraces; y a ejercer un control activo sobre los archivos que le conciernen.

347.5. Los principios se basan, en consecuencia, en la libre determinación de las personas para resolver por sí mismas el estar en una base de datos y autorizar el uso de esa información a terceros.

Ahora bien, como es fácil suponer, en un mundo sin fronteras como representa la globalidad informática, resulta prácticamente imposible saber cuándo, dónde y cómo se archivan y colectan nuestros datos, problemas que se deben arreglar sobre la base de reglas que los bancos o archivos han de cumplimentar, bajo estrictas y severas penas por su incumplimiento.

De igual manera, el derecho a ejercer una industria lícita, como es el relevamiento informático de datos, y comerciar con ellos no puede observarse como una actividad a contrarrestar, teniendo en cuenta que la misma reporta múltiples utilidades, bien conocidas en la sociedad de la información.

Por eso, Herrán Ortiz dice que:

> no habría ningún obstáculo jurídico que pueda imponerse al establecimiento o constitución de empresas cuyo objeto o fin social se encuentre en la explotación mercantil o utilización de bases de datos. Por tanto, se alza en límite para el desarrollo y regulación legal del derecho a la autodeterminación informativa el derecho a la libertad de empresa, en tanto que no le estaría permitido al legislador restringir el uso de la informática hasta el punto de prohibir o impedir la constitución de empresas cuyo fin consista en la creación y explotación de bases de datos personales.[190]

348. Límites y alcances de la protección legal

348.1. La implementación de bancos de datos con archivos personales es un fenómeno difícil de impedir, de modo tal que, al menos, deben fijarse límites legales para su operatividad.

El primer aspecto a considerar es la creación del archivo, y el potencial control que sobre él se puede ejercer.

---

[189] CASALLO LÓPEZ, Juan Martín, "Protección de datos", en *Temas de Interés*, nº 3, Escuela Nacional de Inteligencia (Argentina), Buenos Aires, 1999.

[190] HERRÁN ORTIZ, ob. cit., p. 288.

El segundo, ha de establecer las reglas para autorizar su funcionamiento y fijar los derechos que tengan las personas para acceder y conocer las finalidades que tiene el almacenamiento de sus datos.

El tercer problema se refiere a los principios que debe respetar el banco de datos para la guarda, recuperación, conservación, secreto y seguridad de la información que contiene.

> La Lortad (reformada a fines del año 1999) agrupa en dos grandes apartados los principios fundamentales para la protección de los datos. El primero de ellos —expone López Muñiz— es el grupo de derechos que corresponden al sujeto de datos y que son los siguientes: *a)* el del consentimiento, previo a la incorporación a un fichero de los datos personales; *b)* el derecho de información, que corresponde al conocimiento de lo que realmente existe o se ha incorporado al fichero; *c)* el derecho de acceso, o comprobación por el interesado, de una forma periódica, de lo que se mantiene en el fichero; *d)* el derecho de rectificación, para que los datos incorporados a un fichero sean exactos; *e)* el derecho a la veracidad de los datos, es decir, que los de carácter personal incorporados a un fichero deben actualizarse para que permanezcan acordes con la realidad; *f)* el derecho de indemnización de los perjuicios que pueden ocasionarse por el uso indebido de la informática.
>
> El segundo grupo es el conjunto de principios relacionados con el propio fichero que contiene los datos personales. Aquí podemos considerar: *a)* el principio de legalidad en la captación de los datos; *b)* el principio de unicidad, o la necesidad de que los datos captados respondan a la finalidad del fichero, sin que puedan difundirse o tratarse fuera de esa finalidad; *c)* el principio de la adecuación, según el cual los datos recogidos, serán los pertinentes y no excesivos, teniendo en cuenta la finalidad del archivo; *d)* el principio de caducidad, que exige que los datos incorporados a un fichero no se conservarán en el mismo más tiempo que el necesario para cumplir su finalidad; *e)* el principio de seguridad, tanto informática como general, para garantizar la conservación de los datos y la no revelación de los mismos salvo dentro de la finalidad del fichero.[191]

Cada ordenamiento legal (nosotros nos ocuparemos en particular de Argentina, Colombia, Ecuador y México) tiene definiciones y preferencias sobre la interpretación de cuáles son los principios especiales que debe tener una ley de protección de datos; pero todos coinciden en señalarlos con el rótulo general de "principio de calidad" al que más adelante nos referimos.

348.2. Asimismo cualquiera sea el archivo, debe cumplimentar que los datos almacenados sean exactos y veraces; que tengan el consentimiento de la persona concernida y que sea ésta suficientemente informada de cuánto significa encontrarse en esa base.

Cuando se trata de los llamados datos sensibles, se ha de resguardar una protección especial y segura; mientras que la transmisión de datos hacia terceros, en el orden local o transfronterizo, debe encontrar modalidades aplicables.

A todo ello nos referimos seguidamente.

---

[191] López-Muñiz Goñi, Miguel, "La Ley de regulación del Tratamiento automatizado de los datos de carácter personal", en revista *Informática y Derecho*, números 6/7, editorial UNED, Mérida (España), 1994.

349. Quién puede crear archivos con datos personales

349.1. Tanto la Resolución de la Asamblea General de la ONU adoptada en la sesión 45ª sobre "*Directivas para la regulación de ficheros automáticos de datos personales"* (Doc. A/Res.45/95 del 29.1.91), como las instrucciones del Parlamento Europeo y del Consejo de la Comunidad Económica que dieron lugar, el 25 de octubre de 1995, a la "*Directiva 95/46/CE*", se preocupan por establecer una suerte de reglas para la creación de archivos que contendrán datos de carácter personal.

En líneas muy generales, se parte de considerar, antes que la autorización para funcionar, los principios que cada fichero debe cumplir para actuar con legitimación suficiente.

349.2. Para que sea legal el acopio de información personal, se establecen exigencias propias en cada etapa que tiene el tratamiento de los datos, es decir: *a)* la recolección o toma de información personal; *b)* el intercambio de datos que supone, tanto la transmisión a terceros, como la interrelación o "*data mining*"; *c)* la cesión propiamente dicha, y *d)* el control interno y externo del archivo.

> Todas las leyes de protección de datos que tiene Estados Unidos de América como las desarrolladas por los Estados miembros de la Unión Europea, recogen la idea del Convenio 108 del Consejo de Europa, por el cual se crean principios básicos para la protección de la persona a quien se concierne con la recolección y tratamiento de sus datos; dejando que el archivo o fichero se origine sin demasiadas reglas mientras respete dichos principios.
>
> Estos, al decir de Davara Rodríguez, se pueden resumir en los de legalidad y lealtad al recabar los datos, al tratarlos, al utilizar el resultado de su tratamiento y al, en su caso, cederlos a terceros, y los de pertinencia y adecuación al fin y secreto del responsable, complementados con los derechos de información, acceso, rectificación y cancelación, que se constituyen en una constante en el articulado de las diferentes normas.[192]

De alguna manera, es una decisión prudente que no ha soslayado la notoria dificultad de establecer reglas para la creación de archivos que se originan constantemente con finalidades diversas.

Por ejemplo, Internet moviliza un flujo constante de información entre millones de usuarios por día, que acceden a bases de datos diferentes que no tienen control directo ni frontera reconocida. Obviamente, el sitio se origina como un producto y la página informa con reglas similares a las de la tradicional compraventa (*v. gr.:* comercio electrónico).

> La naturaleza sin fronteras de Internet —según Manganelli— contrasta claramente con el enfoque proteccionista o localista adoptado, por la mayoría de los países, en la pertinente normativa. Existen barreras legales que se derivan tanto de los diferentes códigos comerciales (como la responsabilidad de las partes interesadas) y de las leyes de protección de la intimidad, de propiedad intelectual y de censura. Debido a la ausencia de reglas inter-

---

[192] DAVARA RODRÍGUEZ, Miguel Ángel, *La protección de datos en Europa*, Universidad Pontificia Comillas, Madrid, 1998, pp. 13 y ss.

> nacionales, se han implantado con frecuencia "criterios de jurisdicción local" —reglas, criterios y conceptos legales— que por estar muy relacionados con el mundo real no encuadran adecuadamente al entorno virtual de la red.[193]

349.3. Precisamente, la diversidad normativa, la imposibilidad concreta de establecer reglas comunes para un sistema enlazado mundialmente, y las diferencias notables entre continentes para ocuparse en armonía del complejo tema de los bancos de datos, lleva a un problema interno que no es fácil resolver.

Cada país tiende a dictar leyes de protección de datos personales que se automatizan para ingresar en una cadena intangible de archivos, fuentes de información y carriles de comunicación, que en la aplicación concreta, legislan para el lugar donde la persona se considera afectada (en los hechos, la jurisdicción local que tiene el archivo que lo registra), sin atender que el fenómeno está en la necesidad de armonizar y, de ser posible, unificar con reglas y principios, el funcionamiento de estos bancos de datos.

> Comprar y vender datos personales puede ser un gran negocio en América, pero es por demás dificultoso en Europa, porqué la Directiva sobre protección de datos pone mucho cuidado en evitar la transferencia entre fronteras de datos personales de consumidores, a menos que ese país haya dado los pasos oportunos para garantizar que los datos personales continúen siendo privados. En Estados Unidos, ni la "*Electronic Comunications Privacy Act"* de 1986, ni la "*Computer matching and privacy proteccion act"* de 1988, han resuelto la dificultad de mantener intangible a la persona.

Por otra parte, bien apunta Manganelli cuando dice que:

> los europeos no se acercan, de ninguna forma, a la información que, acerca de sus administraciones públicas, disfrutan los estadounidenses a través de su administración y leyes protectoras de la libertad de información, tan abiertas y valiosas. También aceptan los estadounidenses mucha más intrusión de las administraciones públicas en sus vidas, a menudo sin rechistar.[194]

Actualmente, el artículo 3º de la ley argentina establece:

> La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la ley y las reglamentaciones que se dicten en su consecuencia.
>
> Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

349.4. Las legislaciones difieren según prefieran resolver sobre los datos (en cuyo caso cualquier archivo que los contenga queda atrapado en la norma) o actuar sobre los archivos (que significa dividir el alcance según sean públicos o privados, y dentro de éstos, si tienen finalidades informativas o no).

---

[193] MANGANELLI, Claudio, *Internet,* en "XX Conferencia Internacional de autoridades de protección de datos" (1998), Agencia de Protección de Datos, Madrid, 1999.

[194] MANGANELLI, ob. cit., *passim*.

Inclusive la diferencia también se encuentra en las bases que reportan información personal de alguien relacionada con su solvencia económica o su capacidad para responder al crédito, mostrando desinteligencias entre quienes se ocupan de ellos dentro de la protección de datos personales en general, respecto de otros que optan por legislar el tema en particular.

En *Argentina*, los archivos alcanzados son los públicos, y los privados destinados a dar información a terceros.

En *Brasil* la protección funciona dentro de la garantía procesal del *habeas data*, que se concreta como un derecho del interesado a exigir el conocimiento de registros y datos relativos a su persona que se encuentren en *reparticiones públicas* o *particulares accesibles al público*, con el objeto de solicitar si fuera necesario, la rectificación de los datos erróneos, de allí que se haya afirmado que es solo un *habeas data* exhibitorio y correctivo.[195]

> En la práctica, los datos que obran en registros de órganos públicos hacen fe pública y no pueden ser contestados, a no ser con prueba incuestionable, presentada en contrario. Es el caso, por ejemplo, de un solicitante de información respecto de comicio o asalto de que hubiese participado. La rectificación es un poder deber del Estado, en el caso de que el interesado pruebe que, en aquél día y hora, estaba en otro punto del país o internado en un hospital, o en su empleo. En ese caso, la rectificación es obligatoria.[196]

En *Colombia* el artículo 2º de la Ley estatutaria 1266 dispone aplicar los estándares dispuestos a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de *naturaleza pública* o *privada*; sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público.

En *Chile,* la ley 19.628 establece que toda persona tiene derecho a exigir a quien sea responsable de un banco de datos, que se dedique en *forma pública* o *privada* al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son regularmente transmitidos.

La mención de "tratamiento" supone sesgar el alcance, eliminando a los archivos que solo compilan sin procesar ni transferir del alcance dispuesto.

En *México,* referimos solo a la norma federal de reciente creación, que dispone con el decreto sancionado el cinco (5) de julio de 2010 legislar con alcance para toda la República (recordemos que hasta entonces solo existían en México leyes de protección de datos en el Estado de Colima y en el Estado Federal de México) la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

---

[195] PUCCINELLI, Oscar, *El habeas data en indoiberoamérica,* cit., p. 303.

[196] CRETELLA JUNIOR, José, *Os writs na Constituiçao de 1988,* Forense, Río de Janeiro, 1989, pp. 113 y ss.

El artículo 2 aclara que son sujetos regulados por la ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de: a) las sociedades de información crediticia en los supuestos de la ley para regular las sociedades de información crediticia y demás disposiciones aplicables, y b) las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

No obstante, la restricción del alcance puede quedar contrapuesta con el decreto que adiciona un segundo párrafo al artículo 16 de la Constitución Política, que dice:

> Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.
>
> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.
>
> No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que proceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión.

Con esta dicción es posible sostener que la tutela que se dispensa se refiere al derecho que tiene todo ciudadano a la protección de su datos personales y a solicitar que sus datos e información sean actualizados, modificados, cancelados o suprimidos, en caso de que la información acerca de su persona vulnere su imagen, honor y privacidad o haya sido comprometida de tal forma que le cause un perjuicio. Y que, esa información asiente en registros, bases o bancos de datos *públicos* o *privados.*

En *Paraguay,* la ley 1682 cambia el punto de observación. La línea de partida sostiene que toda persona tiene derecho a recolectar, almacenar y procesar datos personales para uso estrictamente privado. Y, como las fuentes públicas de información son libres para todos, toda persona tiene derecho al acceso a los datos que se encuentren asentados en los registros públicos.

Obsérvese que el artículo 3º, en lugar de establecer prohibiciones respectivas, sostiene que es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercados, siempre que en las publicaciones no se individualicen las personas o entidades investigadas. En cambio, se prohíbe dar a publicidad o difundir datos sensibles de personas que sean explícitamente individualizadas o individualizables.

En suma, la ley habilita la formación de archivos y establece sobre ellos reglas y principios, ofreciendo un marco que, en apariencia, se destina a empresas que revelen situación patrimonial, solvencia económica o cumplimiento de obligaciones comerciales de personas.

En *Perú* la preocupación se dio sobre el funcionamiento de las garantías, de allí que en lugar de ofrecer un cuadro de derechos para el archivo de datos personales y el control sobre ellos, se prefirió acordar al afectado una acción constitucional (*habeas data*) que procede contra un hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el art. 2, incs. 5, 6 y 7 de la Constitución.

Es decir que tiene por finalidad tutelar la efectividad derecho que tiene toda persona, para obtener la información que requiera de cualquier entidad pública; y a que los servicios informáticos no suministren información que afecten la intimidad personal y familiar.

La ley 26.470 publicada el 12 de junio 1995, suprimió del texto del inciso 3 del artículo 200°- de la Constitución y el inciso 7 del artículo 2º de la Constitución. En consecuencia, actualmente la protección abarca el derecho a solicitar sin expresión de causa la información que se requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional.

El secreto bancario y la reserva tributaria pueden levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a la ley y siempre que se refieran al caso investigado.

En *Uruguay* la ley 18.331 dispone que el régimen creado para la protección de datos personales sea una garantía constitucional. La tutela alcanza a todos los archivos que registren información personal, en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.

No será de aplicación a las siguientes bases de datos: *a)* a las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas; *b)* las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.

Finalmente, restringiendo la información a los aportados, en *Venezuela* la tendencia jurisprudencial, en especial la dictada por la Sala Constitucional, es concebir al *habeas data* como una acción constitucional que tiene todo ciudadano de rectificar, actualizar o destruir la información que resulte lesiva de sus derechos. La protección supone el 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 conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos.

Estos derechos, como lo señaló la Sala Constitucional (sentencia de 9 de noviembre de 2009, caso *Mercedes Josefina Ramírez*):

> no involucran directamente nulidades, ni indemnizaciones, sino otorgan situaciones jurídicas esenciales al ser humano: como lo es la existencia de un recurso sobre su persona

en archivos públicos o privados, por lo que no resulta vinculante para el juez constitucional lo que pida el quejoso, sino la situación fáctica ocurrida en contravención a los derechos y garantías constitucionales y los efectos que ella produce, que el actor trata que cesen y dejen de perjudicarlo; o simplemente la información sobre sí mismo que tiene derecho a conocer existente en los registros público o privados.

Ahora bien, para el ejercicio de esta acción constitucional establecida en el artículo 28 de la Constitución de la República Bolivariana de Venezuela, hay condiciones respecto a los archivos alcanzados; y por ello desde la decisión judicial se advierten ciertas restricciones, como al dejar de lado los registros laborales o los que tengan un uso particular o privado.

Se trata, por lo tanto, de bancos de datos, no referidos a alguien en particular, con independencia de que estén destinados a producir informaciones al público. Los registros objeto del *habeas data*, como todo registro, son compilaciones generales de datos sobre las personas o sus bienes ordenados de forma tal que se puede hacer un perfil de ellas, de sus actividades, o de sus bienes; los registros oficiales y los privados, objeto de la norma, tienen un sentido general, ellos están destinados a inscribir documentos, operaciones, actividades entre otros de las personas en determinados campos o temas, por lo que se trata de codificaciones de series de asuntos que forman patrones, matrices y asientos temáticos. (*Vid*. Fallo Nº 332, del 14 de marzo de 2001. Caso: INSACA).

350. El órgano de control sobre los archivos

350.1. La distinción entre archivos públicos y privados, antes que una razón metodológica, es una necesidad que surge del control efectivo que sobre ellos se puede concretar. Mientras los primeros responden al principio del acceso sin interferencias y de la transmisión de datos con libertad; el segundo tiene mayores dificultades para la fiscalización en cualquiera de sus etapas (creación, tratamiento y cesión de la información compilada), circunstancias que motivan el establecimiento de reglas comunes pensadas en dos cuestiones esenciales: *a)* los derechos de las personas, y *b)* las obligaciones del archivo.

350.2. *Los derechos de las personas* asientan en los siguientes principios:

a) Toda persona física debe prestar consentimiento expreso para que sus datos personales sean incorporados a un banco de datos. No existe voluntad presunta.

b) Toda persona que se considere afectada por el almacenamiento de sus datos tiene derecho a saber las razones por las cuales ellos fueron registrados.

c) Se debe asegurar el derecho de acceder a los bancos de datos como una proyección del derecho a la información y en salvaguarda del derecho a la privacidad, para que sea el mismo afectado quien resuelva sobre el destino de sus datos personales.

d) En tal sentido, y como consecuencia del principio anterior, se debe asegurar el control sobre el archivo con el fin de mantener la exactitud de los datos, o en su caso, requerir la actualización o corrección de la información errónea o desactualizada.

e) Toda persona tiene derecho a exigir restricción para transmitir sus datos personal1es.

f) Toda persona puede solicitar, como derecho al secreto, que sus datos más íntimos se reserven y mantengan en la confidencialidad del archivo, o en su caso, exigir la supresión.

g) El afectado podrá solicitar una reparación pecuniaria cuando los datos personales que se registraron sin consentimiento, y se transmitan a terceros, le cause un perjuicio cierto.

350.3. Los archivos, por su parte, deben cumplir con las siguientes *obligaciones*:

a) La acumulación de datos personales debe estar autorizada por la persona concernida y limitado a los que sean congruentes con el fin para el que el archivo fue creado.

b) La pertinencia de los datos personales responde al principio de *unicidad,* por el cual, se establece la buena fe en la recolección y el destino adecuado a la finalidad del banco de datos.

c) No se podrán archivar ni registrar datos que no sean proporcionados por la parte y afecten su derecho a la intimidad (datos sensibles).

d) La calidad del registro supone la obligación de mantener actualizada la base de datos, y de expurgar la información que haya caducado (supresión de oficio del dato, o derecho al olvido).

e) Es deber del titular del registro mantener la confidencialidad y secreto de la información que almacena, debiendo cederla únicamente en los supuestos expresamente autorizados por la ley o el particular afectado.

f) Toda base de datos debe ser segura y secreta, debiendo el titular proteger la información, evitando por los medios que fueran, toda invasión o penetración ilegítima.

Según Puccinelli:

> las primeras normas europeas sobre datos personales contienen diez principios comunes, los cuales fueron calcados por la Constitución de Río Negro de Argentina, al regular el *habeas data*: *a)* el de justificación social, según el cual la recolección de datos debe tener un propósito general y usos específicos socialmente aceptables; *b)* el de limitación de la recolección, el cual estatuye que los datos deben ser obtenidos por medios lícitos, es decir, con el conocimiento y consentimiento del sujeto de los datos o con autorización legal, y limitarse al mínimo necesario para alcanzar el fin perseguido por la recolección; *c)* el de calidad o fidelidad de la información, que implica la obligación de conservar los datos exactos, completos y actuales; *d)* el de especificación del propósito o la finalidad, para que los datos no sean usados con fines diferentes; *e)* el de confidencialidad, conforme al cual el acceso de terceros a los datos debe tener lugar con el consentimiento del sujeto o con autorización legal; *f)* el de salvaguarda de la seguridad, por el cual el responsable del registro de datos personales debe adoptar medidas adecuadas para protegerlos contra posibles pérdidas, destrucciones o acceso no autorizado; *g)* el de política de apertura, que implica asegurar el conocimiento, por parte del público, de la existencia, fines, usos y métodos de operación de los registros de datos personales; *h)* el de limitación en el tiempo, que entraña su conservación hasta que sean alcanzados los fines perseguidos; *i)* el de

control público, que implica la necesaria existencia de un organismo responsable de la efectividad de los principios contenidos en la legislación; *j)* el de participación individual, que consagra el derecho de acceso a los datos y los derechos conexos.[197]

En Argentina, el artículo 21 de la ley 25.326 establece:

1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.

2. El registro de archivos de datos debe comprender como mínimo la siguiente información:

a) Nombre y domicilio del responsable;

b) Características y finalidad del archivo;

c) Naturaleza de los datos personales contenidos en cada archivo;

d) Forma de recolección y actualización de los datos;

e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;

f) Modo de interrelacionar la información registrada;

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;

h) Tiempo de conservación de los datos;

i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

3. Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.

El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el Capítulo VI de la presente ley.

350.4. El derecho comparado nos muestra que el control y vigilancia sobre los archivos que tienen datos personales, a veces se deja en manos del poder de iniciativa que tiene la persona (garantía judicial que se encamina con el *habeas data*), es decir, prefiriendo que sea el afectado quien denuncie la violación a sus derechos (autodeterminación informativa). Otras veces, la ley dispone crear un organismo especial que se ocupa de reglamentar los derechos provenientes del uso de información privada de las personas.

La asimetría se produce conforme sea el lugar donde acentúa la protección dispuesta. Si queda en el marco de la reparación *ex post facto* el *habeas data* se convierte en la herramienta por excelencia; pero si la finalidad perseguida es conseguir un estándar mínimo de protección, el funcionamiento reglamentario merced a legislación delegada, cobra autorizada preferencia.

350.5. En Europa, las primeras iniciativas pensaron que el cumplimiento de las reglas y principios para el funcionamiento de los archivos se debía dejar en manos de un organismo creado a tal efecto.

---

[197] PUCCINELLI, "El *Habeas data* en Indoiberoamérica", en *El Amparo Constitucional, perspectivas y modalidades*, cit., p. 255

Es el caso de *Alemania* (Ley de Hesse que refiere referencia a un Comisario para la protección de datos, actualmente suplantado por cuatro funcionarios: Delegado federal para la protección de datos, Comisarios encargados, funcionarios particulares y consejos locales y regionales); *Austria* (Comisión para la protección de datos; y Consejo para la protección de datos); *Bélgica* (Comisión para la protección de la vida privada); *Dinamarca* (Autoridad de vigilancia de registros); *España* (Agencia de protección de datos); *Francia* (Comisión Nacional de la Informática y las libertades); *Finlandia* (Comisión de protección de datos); *Gran Bretaña* (con dos órganos, el Tribunal de protección de datos y el Registro para la protección de datos); *Holanda* (Cámara de registros); *Italia* (Garante para la tutela y el respeto del tratamiento de datos personales); Luxemburgo (Comisión consultiva sobre protección de datos); *Portugal* (Comisión Nacional para la protección del Tratamiento automatizado de datos); *Suecia* (Consejo de inspección de datos)

Esta fiscalización no impide el acceso a la justicia, que es el modelo americano de la denominada "Ley de privacidad" del 31 de diciembre de 1974.

350.6. En América, algunos han creado organismos especialmente destinados. *México* acuerda el control externo al Instituto Federal de Acceso a la Información y Protección de Datos; *Argentina*, a la Dirección Nacional de Protección de Datos Personales. *Colombia* opta por delegar en un organismo vigente (la Superintendencia de Industria y Comercio) el ejercicio de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales que se regula en la ley. En *Chile*, resuelven de igual modo con el Servicio de Registro Civil e Identificación ordenándole que lleve un registro de los bancos de datos personales a cargo de organismos públicos.

350.7. Nosotros creemos que la vigilancia a través de una agencia particular de derecho público permite auspiciar funciones de relevancia para la eficacia de la tutela prometida. Entre ellas se pueden mencionar, el efectuar un relevamiento (censo) de archivos públicos y privados destinados a brindar información; establecer un marco normativo apropiado para la defensa del derecho a la privacidad amenazada por el fenómeno informático; crear un código ético entre los bancos registrados (de carácter obligatorio) y no registrados (aplicado en sede judicial); emitir instrucciones para dotar de seguridad a los archivos, entre otras misiones que se pueden cumplir.

En Argentina el artículo 29 de la ley establece (órgano de control):

> 1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:
>
> *a)* Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;
>
> *b)* Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;

c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;

d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;

e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos de carácter personal que se le requieran;

f) Imponer las sanciones administrativas que se dicten en consecuencia;

g) Constituirse en querellante en las acciones penales que se promovieren por violaciones a la presente ley;

Los incisos 2 y 3 fueron vetados por el Decreto nª 995/2000

2. El órgano de control gozará de autarquía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia de la Nación.

3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el poder ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.

El Director tendrá dedicación exclusiva en función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones, incapacidad sobreviniente o condena por delito doloso.

El Director como así también el resto del personal están obligados a guardar secreto de los datos de carácter personal que conozcan en el desarrollo de su función.

La Fiscalía Nacional de Investigaciones Administrativas, a través de un Fiscal General competente en la materia, podrá ejercer las facultades previstas en el art. 45 de la Ley 24.946 respecto de la observancia de la presente por parte de todos los archivos, registros y bancos de datos públicos. Dictaminará en los asuntos de importancia sometidos a consideración del Director; en los casos en que se haya denegado el acceso o rectificación de datos invocando las causales del art. 17 incisos 1 y 2 su intervención será obligatoria.

350.8. A su vez, el afectado por la información archivada (afectación que puede ser directa o indirecta) tendrá disponibles los mecanismos procesales tradicionales como el reclamo administrativo y la demanda judicial de *habeas data*.

Es conveniente, no obstante, tener en cuenta que el control no puede estar disperso. En España, el gobierno de Cataluña denunció la inconstitucionalidad de la Ley Orgánica 5/92 en relación con la distribución de competencias, porque afirmó que la distinción entre ficheros de titularidad pública, controlados por la misma administración del registro; y los ficheros de titularidad privada que quedan en la órbita de la Agencia de protección de datos, no atendía que la gestión de los archivos no era un criterio legal para la asignación de competencias, porqué la ley se debe cumplir y hacer respetar por las autoridades locales donde el archivo se encuentra.

350.9. La autonomía e independencia que caracteriza estas oficinas de protección de datos personales es imprescindible para homogeneizar la protección y darle un sentido de unidad e igualdad.

Por eso, en Europa los organismos suelen estar fuera de la estructura administrativa, fungiendo como entidades autárquicas que adquieren financiamiento propio. En América, quienes cuentan con estas estructuras, les han reportado cierta jerárquica.

Considera Dávara Rodríguez que:

> es este uno de los puntos claves y más débiles de la ley (española), porque se duda acerca de la verdadera independencia de la Agencia de Protección de Datos, criticando especialmente el tratamiento de un aspecto tan clave en la configuración jurídica de las garantías del individuo en la protección de datos, y al que no ha sabido dar cumplida respuesta el legislador español. De haberse garantizado la independencia de este órgano y de haberse regulado un procedimiento con garantías para que el *afectado* pudiera ejercer los teóricos derechos reconocidos en la Ley, es probable que se salvaran algunas deficiencias que la misma contiene. Como alternativa a la actual constitución y organización de la Agencia, el autor propone la creación de un órgano interpoderes con funciones y competencias claramente asignadas, al tiempo que su independencia no genere dudas, con lo que su funcionamiento garantizaría el cumplimiento de las disposiciones protectoras de daños.[198]

350.10. Las funciones del Director suelen ser enumeradas en la ley y ampliadas por reglamentaciones, como es el caso de Argentina donde también se le asigna la posibilidad de nuevas tareas si ellas se mencionan en las disposiciones reglamentarias que debe dictar la *Dirección Nacional de Protección de Datos Personales*.

> Se han clasificado las funciones del Director de la Agencia de Protección de Datos (España) en tres áreas: *a)* vigilancia, *b)* consultivas, *c)* prestación. La primera categoría de funciones se corresponde con la función genérica de control y vigilancia del respeto a la legalidad, función de la que derivan las demás atribuciones y potestades reconocidas.

En Europa, la Directiva 95/46 CEE, ha establecido un sistema de protección común al que se adscriben cada uno de los miembros comunitarios, quienes a su vez deben adecuar sus leyes de protección de datos personales a las nuevas disposiciones.

En este sentido, las disposiciones vinculadas con la "autoridad de control" son las siguientes:

> ART. 28. *Autoridad de control*
>
> 1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.
>
> 2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.

---

[198] DAVARA RODRÍGUEZ, *La protección de datos en Europa*, cit., p. 65.

3. La autoridad de control dispondrá, en particular, de:

- Poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;
- Poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;
- Capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud. Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.

5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.

6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro. Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil.

7. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso.

ART. 29. *Grupo de protección de las personas en lo que respecta al tratamiento de datos personales*

1. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado "Grupo". Dicho Grupo tendrá carácter consultivo e independiente.

2. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión.

Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente. Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios.

3. El Grupo tomará sus decisiones por mayoría simple de los representantes de las autoridades de control.

4. El Grupo elegirá a su presidente. El mandato del presidente tendrá una duración de dos años. El mandato será renovable.

5. La Comisión desempeñará las funciones de secretaría del Grupo.

6. El Grupo aprobará su reglamento interno.

7. El Grupo examinará los asuntos incluidos en el orden del día por su presidente, bien por iniciativa de éste, bien previa solicitud de un representante de las autoridades de control, bien a solicitud de la Comisión.

ART. 30. *El Grupo tendrá por cometido*

a) Estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;

b) Emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;

c) Asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;

d) Emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

2. Si el Grupo comprobare la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión.

3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad.

4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión y al Comité contemplado en el artículo 31.

5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado.

6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado.

Sección 7ª Principios especiales en la protección de datos personales

351. Principios aplicables al archivo

351.1. Los principios deben diferenciarse de las obligaciones, pues mientras los primeros hacen al conjunto de reglas que determinan la legalidad del archivo; los segundos refieren a los deberes que debe cumplir el titular y el administrador del registro en cualquiera de las etapas (recolección, procesamiento y cesión).

Es importante acotar, antes de seguir con los principios y responsabilidades, que las obligaciones son del archivo en sí, y no de la persona que los administra. El titular del archivo puede ser una persona física o jurídica, de carácter público o privado, mientras que el administrador de los datos, necesariamente, ha de ser una persona física.

Además, el criterio de legalidad se impone interpretarlo como un deber de quien tiene almacenados datos personales y no porque el archivo esté en el plano de los alcanzados por la defensa legal. Vale decir que se trata de una obligación implícita de quienes tengan archivos, sin importar si ellos son fuente o no de atención específica.

En suma, los principios que se aplican a los ficheros son iguales para todos los que posean información particular que ingrese en el ámbito de la intimidad individual, de allí que un banco de datos, *prima facie* no alcanzado por tener como destino una utilización particular, tendrá que resguardar al menos el principio de reserva y confidencialidad de los datos que posee; porque si ellos llegan a un tercero, sin importar si el conocimiento fue imprevisto, existirá afectación e incumplimiento legal.

351.2. Por su parte, cada individuo tiene derechos contra el banco de datos y acciones posibles para entablar.

En síntesis, son normas mínimas que fundamentan la legalidad del archivo, pero que no impiden a cada Estado que reglamente la tutela de los datos personales, ampliarlos con sus disposiciones internas.

El fin inmediato de cada principio es asignar un valor preferencial al dogma establecido, pensando que con ello se afianza el respeto por los derechos individuales, al mismo tiempo que se instrumenta un mecanismo procesal (*habeas data*) que limita el abuso informático.

Por eso, agrega Herrán Ortiz:

> la normativa en materia de protección de datos debe conformar sus medidas e instrumentos de limitación del uso de la informática en atención a los objetivos de garantía y

> respeto de los derechos de la persona; así, se debe instaurar un conjunto de medidas que sean apropiadas, prácticas, reales y proporcionadas al objeto que se pretende salvaguardar, que no es otro que la "privacidad" de individuo y los demás derechos de las personas. De igual manera, la configuración de las fronteras a que debe circunscribirse la utilización informática de los datos personales no debe consistir en imprecisas e indeterminadas medidas jurídicas que imposibiliten su efectiva aplicación y dificulten la consecución del fin perseguido.[199]

351.3. Obvio resulta que la protección a los datos no supone la represión del desarrollo informático, ni levantar vallas contra la creación de archivos, bases, bancos o registros que tengan una finalidad útil que los fundamente.

Se trata, nada más, que establecer una suerte de indicadores o referencias; un marco de orientación del cual tomar un mínimo de requisitos; en definitiva, son principios básicos que no pueden estar ausentes en la constitución y desarrollo de cualquier archivo.

La legislación comparada suele colocar a este conjunto en torno de un sólo principio que es el de "*calidad de los datos"*, reposando la obligación antes que en el archivo, en el producto logrado.

352. El principio general de "calidad de los datos"

352.1. Cuando el impacto informático comenzó a verse como un mecanismo de penetración en la intimidad personal mediante la afectación de datos personales, se promovieron reglas "mínimas" que, bajo el concepto general de exigencia global en la "calidad de los datos", diseñaron principios básicos a resguardar.

De este modo, se entiende al principio general de "calidad de los datos" como un bloque donde residen derechos mínimos que las legislaciones locales pueden ampliar, pero nunca restringir.

Un modelo de cuanto referimos son los principios elaborados por la Asamblea General de Naciones Unidas adoptados en la Resolución 45/95 del 14 de diciembre de 1990.

352.2. En esta se resuelven como exigencias "de mínima" los principios siguientes:

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

b) *Principio de exactitud:* Las personas encargadas de la creación de un fichero o de su funcionamiento deberían tener la obligación de verificar la exactitud y pertinencia de los datos registrados y cerciorarse de que siguen siendo lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen, periódicamen-

---

[199] HERRÁN ORTIZ, ob. cit., p. 266.

te o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando.

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

d) *Principio de acceso de la persona interesada:* Toda persona que demuestre su identidad tiene derecho a saber si se está procesando información que le concierne, a conseguir una comunicación inteligible de ella sin demoras o gastos excesivos, a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos y, cuando esta información sea comunicada, a conocer los destinatarios. Debería preverse una vía de recurso, en su caso, ante la autoridad encargada del control o darse una vía judicial específica para el reclamo

En caso de rectificación, el costo debería sufragarlo el responsable del fichero. Es conveniente que las disposiciones de este principio se apliquen a todas las personas, cualquiera que sea su nacionalidad o su residencia.

e) *Principio de no discriminación:* No debieran registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, o sobre la participación en una asociación o la afiliación a un sindicato.

> Sólo pueden autorizarse excepciones a los principios enunciados si son necesarias para proteger la seguridad nacional, el orden público, la salud o la moral pública y, en particular, los derechos y libertades de los demás, especialmente de personas perseguidas (cláusula humanitaria), a reserva de que estas excepciones se hayan previsto expresamente por la ley o por una reglamentación equivalente, adoptada de conformidad con el sistema jurídico nacional, en que se definan expresamente los límites y se establezcan las garantías apropiadas.
>
> Las excepciones al principio relativo a la prohibición de discriminación, deberían estar sujetas a las mismas garantías que las previstas para las excepciones a los demás principios y sólo podrían autorizarse dentro de los límites previstos por la Carta Internacional de Derechos Humanos y demás instrumentos pertinentes en materia de protección de los derechos y de lucha contra la discriminación.

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

352.3. En *Argentina*, el principio de calidad de los datos, se presenta en el art. 4 de la ley 25.326 que dice:

> 1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para las que se hubieren obtenido.
>
> 2. La recolección de datos no podrá hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.
>
> 3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
>
> 4. Los datos serán exactos y deben actualizarse en el caso que ello fuere necesario.
>
> 5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser cancelados y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.
>
> 6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
>
> 7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recabados.

La ley española califica como *adecuados y pertinentes* los datos que se almacenan respondiendo a la finalidad y ámbito del fichero, agregando que tampoco podrán ser *excesivos en relación* con la causa *explícita y legítima para las que se hayan obtenido.*

Por citar algún ejemplo opuesto, *Colombia*, entiende a la calidad dentro del principio de veracidad del dato, argumentando que así se interpreta la información contenida en los bancos de datos que debe cierta, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error.

352.4. Ahora bien, para comprender el sistema de principios es menester aclarar las dos facetas que se ponderan. Por un lado, los principios comprendidos en la dimensión de los deberes que tiene que cumplir todo banco o base de datos que contiene información privilegiada referida a una persona; y por otro, los principios que se tienen que desplegar para que la persona concernida tenga derecho de acceso (saber si está en los archivos) y control (consentir o negar la actividad que se tiene con sus datos personales, y en su caso resolver con ellos —actualizar, suprimir, o dar en confidencialidad—).

Ambos, en forma conjunta pero al mismo tiempo con independencia, conforman el principio de calidad de los datos.

353. Los principios contenidos en la calidad de los datos: *Principio de legalidad*

353.1. Por este principio se establecen algunas reglas básicas:

a) Licitud en la recolección de datos.

b) Buena fe en la búsqueda de información, como en las etapas sucesivas de almacenamiento, tratamiento, interconexión, cesión y transferencia.

c) Lealtad hacia la persona que resulta concernida.

d) Participación del individuo en la incorporación al banco de datos (cuando fuese pertinente requerir autorización y consentimiento para tomar sus datos personales).

e) Exclusión inmediata de los datos sensibles.

Cada uno tiene un requisito particular a cumplir, y en conjunto representa la justificación del archivo contra eventuales acciones que le atribuya abuso o intromisiones ilegítimas.

El art. 6 de la ley 18.331 (Uruguay) define como principio de legalidad:

> La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia. Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública.
>
> Aquí el cambio sucede con el punto de partida. Son "legales" las bases de datos que se registren y cumplan con la ley, pero las obligaciones se disciplinan en los demás principios que, de este modo, cobran autonomía.

353.2. Ahora bien, ¿es suficiente cumplir cada aspecto reglado para aceptar socialmente al archivo?, ¿basta encuadrar y ajustarse a cada uno de las reglas para ampararse en un marco legal dispuesto?

Responder estos planteos obliga a considerar cada uno de los puntos puestos como exigencias.

Por ejemplo, *licitud en la recolección de datos* supone que las acciones emprendidas para la obtención de informaciones personales han dado cumplimiento a una pauta general de buena fe y lealtad hacia las personas interesadas.

"Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos", indica la Ley de protección de datos española. Mientras que la *Data proteccion act* (Gran Bretaña) dice que "la información contenida en la data personal deberá ser obtenida y deberá ser procesada en forma justa y de acuerdo a la ley", para agregar más adelante que:

> al determinar si la información se obtuvo de manera justa, se deberá tener cuidado en el método por el cual se obtuvo, incluyendo en particular si cualquier persona a través de la cual se haya obtenido dicha información haya sido engañada o confundida en cuanto al propósito o propósitos para lo cual se ha poseído, usado o revelado dicha información. Se considera que una información ha sido obtenida en forma justa si se ha alcanzado a través de una persona que sea autorizada por o bajo cualquier estatuto o por algún convenio u otro instrumento que imponga una obligación internacional en el Reino Unido; y para dicho proceso no se considerará ninguna revelación de la información que se autorice o requiera por o bajo cualquier ley o requerida por tal convenio u otro instrumento mencionado anteriormente.

353.3. La toma de información puede ser *directa* y lograda del mismo interesado en aportarla; o *indirecta* y obtenida por adquisición o penetración en la intimidad de una persona.

En el primer supuesto, la buena fe se demuestra con la información dada a las personas para que sepan que los datos que aportan serán incorporados a una base de datos. La ocultación, el engaño, la apariencia, el sigilo, o cualquier otra maniobra elusiva de la verdad, será causa suficiente para advertir la deslealtad y penar al archivo por este comportamiento.

Por eso, el artículo 5º de la ley argentina establece que:

> 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso o informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias…

La nueva ley española de protección de datos, establece con la finalidad de informar adecuadamente al interesado, una serie de requisitos a cumplir en la toma de datos. Dice el artículo 5 (*Derecho de información en la recogida de datos)*

> 1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: *a)* De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. *b)* Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. *c)* De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. *d)* De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. *e)* De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
>
> Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.
>
> 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
>
> 3. No será necesaria la información a que se refieren las letras *b), c)* y *d)* del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
>
> 1. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras *a), d)* y *e)* del apartado 1 del presente artículo.
>
> 2. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a

> la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

353.4. En el caso de intercepción de datos, la ilegalidad es inmediata, salvo en supuestos donde se obtengan de fuentes accesibles al público, o se recojan para el ejercicio de funciones propias de la administración pública en el ámbito de sus competencias, o bien, se refieran a personas vinculadas por un negocio jurídico, una relación administrativa y sean necesarias para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El ejercicio de buena fe y lealtad en la toma de datos, se asocian al principio de legalidad en la medida que se considera ilegítima (ilegal) la apropiación de información conseguida con prácticas engañosas (por ejemplo, grabando conversaciones, interceptando comunicaciones telefónicas, penetrando en archivos informáticos, etc.) u hostiles (*v. gr.:* violencia en los medios utilizados para lograr la información; seguimiento de la vida privada; etc.).

Cuando se piden datos, es necesario informar para qué se solicitan, donde se archivarán y el destino pensado para ellos. Eso es *lealtad hacia la persona concernida*; no obstante, buena parte de los bancos o registros privados se nutren con información indirecta, por el sistema de interconexión o tratamiento de las bases, logrando resultados sorprendentes que depuran al máximo los datos hasta llegar a la individualización de las personas.

En España, afirma Estadella Yuste:

> las únicas excepciones que se pueden admitir para no informar, se dan cuando la autoridad nacional considera que, por razones muy concretas —por ejemplo, en actividades de investigación criminal—, no es apropiado que el afectado conozca la recogida de datos.[200]

353.5. La forma prevista para detener estas actitudes producidas por el impacto informático se basan en el *principio de limitación* que otros refieren. Esta regla previene la recolección ilegítima y pone trabas al archivo de los llamados "datos sensibles".

El principio de limitación está íntimamente ligado al de legalidad y es casi una consecuencia lógica del mismo en su aspecto negativo. El objetivo que se persigue —dice Estadella Yuste— es evitar la creación o existencia de ficheros con datos de carácter personal elaborados de forma arbitraria, y sin un objetivo específico para impedir su transmisión internacional. El principio de limitación no prohíbe la recogida, el almacenamiento o el procesamiento de datos, sino que simplemente establece márgenes temporales y cuantitativos.[201]

---

[200] ESTADELLA YUSTE, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales*, Tecnos, Madrid, 1995, p. 176.

[201] ESTADELLA YUSTE, ob. cit., p. 178.

Algunas veces, la petición de datos requiere la *participación de las personas*. Es el recaudo previsto idealmente en buena parte de los ordenamientos jurídicos como autorización expresa que se otorga al archivo para registrar informaciones personales y permitir su circulación.

El consentimiento en la entrega de información personal depende, muchas veces, de la naturaleza del requerimiento. Puede ser obligatorio (por ejemplo, censo poblacional) o voluntario (*v. gr.:* encuesta de hogares), y a veces, puede el interesado negar su voluntad de colaboración o apoyarla expresamente suscribiendo un documento de aceptación.

Son modalidades que asumen con variables de procedimiento las distintas agencias de protección de datos.

353.6. Las llamadas "Resolución de Madrid" (2009) que elabora una serie de estándares internacionales sobre protección de datos y privacidad atiende el principio en cuestión, sosteniendo que los tratamientos de datos de carácter personal se deberán realizar de manera leal, respetando la legislación nacional aplicable y los derechos y libertades de las personas, de conformidad con lo previsto en el documento creado y con los fines y principios de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos.

En particular, se consideran desleales aquellos tratamientos de datos de carácter personal que dan lugar a una discriminación injusta o arbitraria contra los interesados.

En esta resolución, el principio de calidad se desintegra para alojarlo únicamente en el derecho que tiene el afectado de requerir a la persona responsable del archivo (y como deber implícito de éste) que asegure en todo momento que los datos de carácter personal sean exactos, así como que se mantengan tan completos y actualizados como sea necesario para el cumplimiento de las finalidades para las que sean tratados.

La persona responsable deberá limitar el periodo de conservación de los datos de carácter personal tratados al mínimo necesario. De este modo, cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento deberán ser cancelados o convertidos en anónimos.

354. Los principios contenidos en la calidad de los datos: *El principio de finalidad*

354.1. Finalidad se relaciona con pertinencia, por eso suele llamarse a este principio con cualquiera de ambas referencias. En las dos, significa que el archivo esta autorizado para registrar datos solamente en la actividad prevista al tiempo de su creación.

A veces, se denomina "*principio de unicidad*" por el cual se entiende que, finalidad exige conocer desde el primer momento las razones por las que se recaban datos, justificándose así la necesidad de obtener y procesar algún tipo de información sensible.

354.2. El art. 4º inciso 3º de la ley de Argentina nº 25.326 especifica que: "Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención"

> Las excepciones autorizadas se llaman "cláusulas humanitarias", y permiten al archivo tomar datos personales de carácter sensible cuando el propósito sea la protección de derechos humanos o libertades fundamentales, o en su caso, la asistencia humanitaria.

Según Estadella Yuste:

> hay directrices que también reconocen excepciones cuando están implicados temas de soberanía, seguridad nacional y orden público, aun cuando se exige que estas excepciones sean las mínimas posibles y que se pongan al conocimiento del público.[202]

354.3. Lo mismo sucede en *Uruguay* con el art. 8 de la ley que refiere al principio de finalidad. En ese sentido los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Por ello deben ser eliminados cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados. La norma, con una vaguedad exagerada, que puede encubrir una delegación legislativa por la importancia del tema de que se trata según los casos,[203] deja a la reglamentación determinar los casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo con la legislación específica, se conserven datos personales aun cuando haya perimido su necesidad o pertinencia. Si bien serían hipótesis de excepción, la disposición se entiende como posible causante de litigios jurídicos.

354.4. Muchas empresas en *Chile* obtienen por diversas fuentes datos, bien sea de sus clientes, proveedores o de la competencia, dando lugar, entonces, a relevar como se protege el principio de finalidad del dato.

La finalidad de los datos deben estar determinadas de forma explícita y ser legítima y, por tanto, no podrá utilizarse aquella información cuya finalidad sea incompatible con la que motivó su obtención, teniendo en cuenta que no se considera incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos. En cualquier supuesto ante el que nos encontremos, el levantamiento de datos personales debe estar fundamentada en una finalidad explícita, no siendo posible la recopilación de datos personales para su uso de forma generalizada y determinada a *posteriori*.

Se ha de tener en cuenta que la facultad para crear bases de datos con determinados datos de carácter personal tiene que existir una relación directa entre la finalidad perseguida y el dato levantado.

---

[202] ESTADELLA YUSTE, ob. cit., p. 180.

[203] FLORES DAPKEVICIUS, Rubén, "La nueva ley de *habeas data* en Uruguay nº 18.331", en *Informática Jurídica*, Punta del Este, 2008, passim.

> El artículo 9° de la ley 19.628 (Chile) dice: Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público. En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos.

354.5. En *Perú* el principio de finalidad está diluido en los márgenes que reporta el Código Procesal Constitucional, cuyo art. 61 (derechos protegidos), sostiene la procedencia del *habeas data* para:

1) Acceder a información que obre en poder de cualquier entidad pública, ya se trate de la que generen, produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material.

2) Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales.

De allí que la relación de tutela provenga únicamente de la pretensión procesal que deduzca el afectado, argumentando que la información tomada y archivada es incompatible con la aplicación que de ella se hace.

354.6. En *Ecuador*, el art. 94 de la Constitución Política en vigencia dice:

> 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 […].

Luego el art. 49 de la nueva ley de jurisdicción constitucional dispone, en la parte pertinente, que "toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos".

354.7. En Colombia el artículo 4 de la ley estatutaria 1266 destaca en el principio de finalidad el contenido siguiente: "La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización, cuando ella sea necesaria o en general siempre que el titular solicite información al respecto".

Como se ve el deber no está aplicado al contenido de la base de datos sino al derecho de información que tiene toda persona cuyos datos se han relevado y almacenado.

354.8. Justamente en *México,* el artículo 6 de la ley federal establece que los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

Tras disponerlo especifica sin alegarlo expresamente como "principio de finalidad" que el tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable (art. 13).

El "aviso de privacidad" innova en la materia, porqué le asigna al titular o responsable del archivo el deber de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines. De esta manera revierte la tendencia de otras legislaciones que esperan el reclamo directo del afectado.

> ART. 16.—El aviso de privacidad deberá contener, al menos, la siguiente información:
> I. La identidad y domicilio del responsable que los recaba;
> II. Las finalidades del tratamiento de datos;
> III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
> IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
> V. En su caso, las transferencias de datos que se efectúen, y
> VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.
> En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.
>
> ART. 17.—El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:
> I. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y
> II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo anterior, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

354.9. En síntesis, el principio de finalidad se vincula con el de legalidad en cuanto a los límites que fija para la recolección y la conservación de los datos en el banco creado.

Ningún archivo puede colectar datos que no estén vinculados con el fin que persigue su objeto, y de serlo, surge un nuevo impedimento para la interconexión en la medida que está prohibido desviar la información de su propósito original.

Asimismo, la permanencia del dato en la base debe estar relacionada con los motivos del registro, y mantenerse en él hasta que el mismo se alcance.

Tal es el objetivo del art. 4º inciso 7º de la ley argentina al establecer que: "Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido colectados".

Iguala así la regla aconsejada mundialmente, respecto a que el tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas de la persona responsable. Ésta se abstendrá de llevar a cabo tratamientos no compatibles con las finalidades para las que hubiese recabado los datos de carácter personal, a menos que cuente con el consentimiento inequívoco del interesado.

355. Los principios contenidos en la calidad de los datos: *El principio de congruencia (proporcionalidad - pertinencia)*

355.1. Todo dato debe ser congruente con las finalidades que se buscan al archivarlo. Se trata de bosquejar una suerte de adecuación material y objetiva según la cual cada registro debe colectar y trabajar sin variar los fines de su creación.

Sin embargo, entendemos que es bastante difícil dar cumplimiento a este principio, porqué los datos informatizados se suelen buscar y clasificar aleatoriamente.

> Es de esperar que reglamentariamente —dice López Muñiz— se establezca qué criterios van a imponerse en este terreno, ya que es lógico pensar que deban especificarse los campos que compongan cada registro, y cuáles de ellos van a ser los que sirvan como elemento de recuperación. Igualmente se espera que deberán constar en la Agencia de Protección de Datos los sistemas de recuperación de la información.[204]

355.2. También se nomina a esta regla como "*principio de proporcionalidad*", con la idea de colegir que los datos no deben ser más de los necesarios para la información que persiguen. Vinculado, claro está, al principio de limitación anterior.

> Esta solución parece postular —en el pensamiento de Estadella Yuste— en favor de la existencia de datos inofensivos que se conservan en el fichero mientras no se apliquen al fin buscado; pero puede resultar peligroso, ya que al almacenar datos personales sin un objetivo concreto puede facilitar que, en un futuro, se establezca un nexo identificador que permita utilizar la información para finalidades diferentes de las que existían originariamente.[205]

355.3. Asimismo se conoce a este principio como de *pertinencia*, exigiendo que los datos que se recaben y almacenen en una base de datos sean pertinentes y adecuados, es decir, que se vinculen con el fin perseguido en el momento de creación de la base de datos. En una palabra, significa que la recolección y el tratamiento de los datos han de ser proporcionales con respecto a los fines queridos, sin que en

---

[204] López-Muñiz Goñi, ob. cit., p. 266.

[205] Estadella Yuste, ob. cit., p. 180.

ningún caso se puedan utilizar los datos obtenidos con abuso o desvío de aquello que fuera informado al titular concernido.

El principio de pertinencia, por tanto, delimita las circunstancias personales sobre las que pueden indagar y recabar información quienes mantengan bases de datos que incluyan información personal.

> De tal forma, como enseña Salom,[206] este principio supone que no obstante la posible autorización del titular de los datos o la habilitación legal para someter la información a tratamiento, no se permite que puedan incluirse más datos que aquellos que sirvan o puedan servir para la consecución de la finalidad que justifica dicho tratamiento, que debió determinarse en el momento de la obtención del consentimiento, o que sirve para presumir la concurrencia de éste en los supuestos en que se establecen presunciones legales de su otorgamiento.

356. Los principios contenidos en la calidad de los datos: *El principio de corrección*

356.1. También suele llamarse principio de *exactitud*, o verdad de los datos, esto es, que reflejen con autenticidad y fehaciencia la información que compilan y transmiten. Se relaciona con la "actualidad" del registro, en virtud de que los datos se deben guardar y conservar "al día", obligando en consecuencia, a un trabajo permanente de control sobre ellos.

El carácter de principio hace a la legalidad del archivo, y se convierte en obligación para el titular o administrador, quienes son responsables por la inexactitud informativa.

Por eso señala el art. 4º inciso 4º de la ley argentina, que *los datos deben ser exactos y actualizarse en el caso que ello fuere necesario*. Además, *los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados por el responsable del archivo o base de datos, cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate* […].

En este país la jurisprudencia registra el caso de una base de datos condenada por no haber actualizado la información en ella contenida. La sentencia sostuvo que:

> cabe responsabilizar a la entidad operadora de un banco de datos que, habiendo tomado conocimiento del error en virtud del cual se había incorporado al actor dentro de la base de datos del Banco Central no procedió a borrarlo de sus respectivos registros, pues no existe norma alguna que le impdiera dejar sin efecto tal incorporación…Habiendo quedado demostrado que el actor ha sido erróneamente incluido en la base de datos del Banco Central; sin que esta obligación pueda verse condicionada al cumplimiento de ciertos requisitos contenidos en una disposición interna de aquél que no ha sido aun publicada en el *Boletín Oficial*, pues no se trata de una norma vigente en los términos del art. 3º del Código Civil. Tanto más que, en el caso, el demandante ni siquiera operaba con

---

[206] SALOM, Jaiver Aparicio, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi. Pamplona, 2000, p. 95.

el banco que le comunicó la errónea información a la entidad de contralor…Si bien es cierto que, en el caso, el banco que le comunicó al Banco Central la errónea información respecto del actor que provocó la inclusión de este dentro del registro de deudores del sistema crediticio, no tiene la obligación de borrarlo de ninguna base de datos propia, también lo es que los aquí codemandados Banco Central y Organización Veraz S.A. sólo podían desafectarlo de sus registros una vez que se les hubiese informado el error cometido, por lo cual, la mencionada entidad bancaria deberá ser responsabilizada por no haber realizado oportunamente tal notificación…Dada la ligereza y la falta de prudencia con que se opera en orden a la información pública que se brinda a través de las bases de datos, y habida cuenta de los perjuicios que con ello se puede provocar a los ciudadanos, que no pueden justificarse en función de la mayor agilidad que tal operatoria puede reportar para el comercio, resulta necesario que este hecho sea puesto en conocimiento del Honorable Congreso de la Nación a fin de que en ejercicio de su propia competencia adopte las medidas legislativas que estime corresponder.[207]

356.2. La norma impone el deber de notificar datos ciertos, porque de otro modo, sería imposible de cumplir por el titular del banco, archivo o registro, con el mandato legal. Surge entonces el problema de actualizar la información y de saber hasta cuando se puede mantener en la base de datos cierto tipo de ella.

De acuerdo con los términos legales, la obligación del archivo es mantener actualizada y exacta la información que contiene, pero no se resuelve en todos los casos, cómo se debe proceder para mantener en tal sentido a la base de datos.

Si la respuesta fuera que deba ser directamente de la actualización que la persona concernida debe realizar, se revertiría el derecho de control que está en la base misma de la autodeterminación informativa.

En cambio, si estuviera en el deber del titular o responsable del archivo, las fuentes de producción informativa serían proclives a mostrar su debilidad al ser ellas mismas quienes asientan la caducidad de ciertos datos personales (*v. gr.:* un registro puede mantener en la base la información del estado civil soltero de alguien que contrajo matrimonio; o decir un domicilio que fue cambiado; etc.).

Por eso, el derecho comparado prefiere aplicar el uso del tiempo en la conservación de los datos.

356.3. Ahora bien, el dato debe ser exacto mientras esté en el archivo; una vez que ha cumplido la finalidad para el que fue colectado, es deber del titular de la base, cancelar la información suprimiéndolo. No obstante, como se dijo con anterioridad, la colección de datos resulta a veces aleatoria, de modo tal que la posibilidad de conservar la realidad acopiada puede ser más que difícil, en cuyo caso, se debería establecer un mecanismo de actualización periódica o la disociación de los datos.

La UNESCO ha propuesto que esta actualización se efectúe anualmente, salvo que el propio sistema operativo permita comprobaciones rutinarias sobre la veracidad de la información (*Cfr.* Doc. A/44/606 del 24 de octubre de 1989, en sesiones de la ONU).

---

[207] CNContenciosoadministrativa, Sala I, 1999/04/21, "*Finoli, Leonardo Luis c/ Banco Central de la República Argentina y otros s/ habeas data*", La Ley Online.

> Por su parte Estadella Yuste propicia que los instrumentos internacionales debieran considerar la propuesta a los siguientes fines: 1) para asegurar el principio de calidad de la información; y 2) que tal actualización fuese comunicada de oficio (y en caso contrario pudiera reclamarse responsabilidad) a todos los ficheros automatizados de otros países a los que se hubiese efectuado, con fecha anterior, una transmisión de tales datos.[208]

356.4. En Argentina, el deber de actualización se mantiene mientras sea necesaria la información que se almacenó para un fin determinado. Luego de ello, el deber de veracidad informativa se convierte en derecho a exigir la supresión del dato caduco.

Esta obligación es diferente, porque la ley establece que el *dato total o parcialmente inexacto o incompleto* se debe suprimir, sustituir o completar, *cuando se tenga conocimiento* de la inexactitud o carácter incompleto de la información, sin perjuicio del derecho que al afectado le corresponde para integrar la información que considera errónea (*falsa o inexacta*); en cambio la reglamentación dispone que la *supresión debe ser una consecuencia inmediata* cuando el mantenimiento del dato en el archivo *no tiene prevista una finalidad igual para la que se obtuvo oportunamente*. Es una pequeña diferencia, es verdad, pero muy importante a la hora de establecer el cumplimiento del principio de legalidad y calidad de los datos.

En efecto, al responsable o usuario del archivo, registro, base o banco de datos, la información le llega de manera *directa* (del titular, del acreedor del titular, de otras bases de datos) o *indirecta* (por interconexión o tratamiento —entrecruzamiento de datos), de forma tal que la actualización de sus registros depende de la movilidad de dicha información. Hay datos que se logran directamente del titular. Por ejemplo, si alguien requiere el consentimiento para archivar datos que se destinarán para un concurso, se puede afirmar que efectuado el sorteo la finalidad se ha cumplido y esa base de datos debe suprimirse. Tal sería el objetivo del artículo 4º, párrafo tercero de la reglamentación. Es decir, asociar la información que se le reporta a la persona cuando se obtienen sus datos, y sin necesidad de que éste lo pida, eliminarlos inmediatamente cumplido el objeto reportado.

Sin embargo, hay archivos que se forman sin necesidad de requerir expreso consentimiento y esa información se transmite con una amplia libertad de circulación (*v. gr.:* bases de datos de marketing directo; encuestas; etc.), de forma tal que la eliminación se plantea como una cuestión de interés del afectado (*opt out*, que le facilita al interesado no participar del supuesto beneficio, o requerir el retiro de su nombre del listado donde se encuentra cuando se trata de los archivos de marketing directo.

356.5. Ahora bien, la supresión del dato no significa que se elimine a la persona del archivo, sino únicamente, que la información se debe actualizar o completar. Obsérvese que la ley 25.326 (Argentina) obliga a suprimir el dato inexacto para sustituirlo por el exacto. O en su caso, si se trata de información incompleta, habrá que

---

[208] ESTADELLA YUSTE, ob. cit., p. 200.

actualizarla. Esta diferencia se explica atendiendo las finalidades previstas en la creación de los archivos, condición que determinará la obligación de supresión o actualización. Un fichero cuya única finalidad se cumpla de inmediato (*v. gr.:* oferta de servicios ocasionales) podrá tener pocos datos (ej. nombre y domicilio) y ser completo y correcto para el fin previsto. Cumplido su objetivo, la base se destruye. Pero, si el archivo se crea con otras finalidades, el dato se puede usar y cancelar a ese fin inmediato, pero actualizarlo o completarlo para otros destinos.

Dato correcto no supone dato completo, es decir, la verdad que registra puede ser parcial, y para revestir de integridad la información necesitar de complementos que el archivo no ha recabado. Esta deficiencia no ilegitima la base, sólo provoca que los datos sean incompletos pero nunca incorrectos.

No obstante, siguiendo el criterio de la comunidad europea, el dato incompleto se debe suprimir y sustituir por el correcto.

> La normativa comunitaria europea piensa que todo dato incompleto es inexacto y la permanencia en el fichero depende de los propósitos perseguidos en la creación. Es el criterio de la reglamentación en el artículo 4.4
>
> En Europa se ha establecido un acuerdo de cooperación para que los datos transfronterizos no sufran controles independientes, permitiendo su libre circulación entre los países signatarios y la actualización constante de la base mediante el aporte de cada uno. Se denomina "*Acuerdo Schengen"* y contiene información referente a: *a)* personas buscadas a efectos de extradición; *b)* personas desaparecidas; *c)* personas extranjeras incluidas en las "listas de no admisibles"; *d)* personas en interés de su propia protección o para prevenir amenazas; *e)* testigos protegidos.
>
> La característica central está en que los datos compilados no pueden ser más que éstos: *a)* nombre, apellido o seudónimo; *b)* rasgos físicos; *c)* primera letra del segundo nombre; *d)* fecha y lugar de nacimiento; *e)* sexo; *f)* nacionalidad; *g)* indicación de que la persona de que se trate está armada; *h)* indicación de las personas de que se traten son violentas; *i)* motivo de la inscripción; *j)* conducta que debe observarse. Este acuerdo esta suscripto entre Francia, Alemania, Bélgica, Holanda y Luxemburgo.

356.6. En *México,* la Ley Federal de Protección de Datos Personales establece en el art. 11 que:

> [...] El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados. Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.
>
> El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

El plazo de setenta y dos (72) meses (6 años) parece demasiado extenso para conservar datos en un fichero que no actualiza el cumplimiento de las obligaciones

contractuales; pero es congruente con el tiempo de prescripción de las acciones que se tengan contra quien ha dejado de cumplir con los pactos preexistentes.

356.7. En *Chile*, al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete (7) días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor.

El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito.

Quienes efectúen el tratamiento de Datos Personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres (3) días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información.

La ley La *Fair Credit Reporting Act* establece en siete (7) años el límite de conservación de los informes.

En *Uruguay* los datos personales relativos a obligaciones de carácter comercial sólo podrán estar registrados por un plazo de cinco (5) años contados desde su incorporación. En caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al titular de la base de datos, por única vez, su nuevo registro por otros cinco (5) años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original.

Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco (5) años, no renovable, a contar de la fecha de la cancelación o extinción.

En *Colombia*, la Corte Constitucional dijo que

> […] los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de "personas virtuales" que afecten negativamente a sus titulares, vale decir, a las personas reales. De otra parte, es bien sabido que las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia después de algún tiempo tales personas son titulares de un verdadero derecho al olvido.[209]

La ley colombiana estableció que la información de carácter positivo permanecerá de manera indefinida en los bancos de datos de los operadores de información. Los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera, y en general, aquellos datos referentes a una situación de incumplimiento de obligaciones, se regirán por un término máximo de permanencia, vencido

---

[209] Corte Constitucional de Colombia, sala Primera de Revisión, sentencia T- 414/1992.

el cual deberá ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información.

El término de permanencia de esta información será de cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea pagada la obligación vencida.

356.8. Mencionamos solo estas legislaciones para confrontar la diversidad del tiempo dispuesto en la caducidad del plazo para conservar información personal almacenada.

En definitiva, el derecho asienta en la tutela que se le debe a las personas para que sus datos sean objeto de tratamiento adecuado y congruente por los archivos, evitando que el mal uso de ellos, afecte el derecho a la intimidad o el honor, imponiendo a tales fines, principios y presupuestos que se conocen como de "calidad de los datos".

La base del derecho a la protección de datos personales está en el libre consentimiento que pueda dar quien sea requerido a esos efectos, y en el control que a *posteriori* se pueda ejercer. Esta vigilancia apunta hacia dos objetos precisos. Controlar al archivo autorizado para que cumpla la finalidad oportunamente expuesta al requerir la autorización; y verificar la actualidad de los datos para que no se ofrezca información obsoleta, equívoca o inexacta.

En ambos casos se establecen los deberes que tiene el registro en cuanto a la adecuación, pertinencia y congruencia del almacenamiento con los datos autorizados que se van compilando de la persona concernida.

356.9. Es necesario aclarar que el deber de actualización de los datos es del archivo y no de la persona afectada, incurriendo en negligencia el responsable que no cumpla con esa obligación de veracidad.

> Al respecto, ha señalado Orozco Pardo que la ley impone al titular del fichero: mantener los datos exactos y al día; rectificándolos de oficio, sustituyéndolos por los correspondientes datos rectificados y completos, sin que sea necesario que ello se solicite. Los datos deben cancelarse de oficio cuando ya no sean pertinentes o necesarios para la finalidad con que se recogieron, mientras tanto, deben estar almacenados de forma que posibiliten el ejercicio de los derechos de los afectados.[210]

La vigilancia es un poder del afectado para controlar directamente al registro, pero se debe diferenciar del control externo que los bancos de datos tienen del organismo de fiscalización.

El dato caduco origina el llamado "derecho al olvido", evitando que la persona quede prisionera de un pasado que ha superado, y que no sirve a justificativo alguno recordarlo.

Básicamente consiste en el derecho a que no se divulguen datos, aun de conocimiento público, que, por el paso del tiempo o la distancia, resultan intrascendentes

---

[210] OROZCO PARDO, Guillermo, *Los derechos de las personas en la Lortad,* cit., p. 158.

para la comunidad en la que se difunden. De divulgarse injustificadamente, se violaría el derecho a conservar el honor adquirido con posterioridad ([211]).

Este beneficio a la destrucción del dato sin destinos objetivos, o carente de finalidad por devenir abstracto o aplicado al objeto previsto, es común en los informes comerciales.

En la *Fair Credit Reporting Act*, se establece:

> ART. 1681c. *Prohibición de transmitir información obsoleta:*
> *a)* Excepto en lo autorizado en el inciso *b)*, ninguna empresa de informes del consumidor puede hacer un informe del consumidor que contenga cualquiera de los siguientes ítems de información:
> - Casos enumerados en el título 11 del Código de los Estados Unidos o en la Ley de Quiebras que, por la fecha de entrada de la orden de desagravio o por la fecha del fallo, depende el caso, precedan al informe en más de 10 años.
> - Juicios o fallos que, por la fecha de entrada, precedan al informe en más de 7 años o hasta que la ley de prescripción reguladora haya expirado, teniendo en cuenta el período más largo.
> - Embargos tributarios pagos que, por la fecha de pago, precedan al informe en más de 7 años.
> - Saldos informados de cuentas pendientes y de resultados de ganancias y pérdidas, que precedan al informe en más de 7 años
> - Antecedentes de arresto, denuncia o condena por crimen que, por la fecha de disposición, liberación o libertad condicional, precedan al informe en más de 7 años.
> - Cualquier otro ítem adverso de información que preceda al informe en más de 7 años.

356.10. Igualmente, hay que diferenciar entre el derecho a la supresión del dato caduco y el secreto sobre esta misma información. Una cosa es ocultar aquello que está protegido en virtud del acuerdo de confidencialidad con la persona concernida; y otra distinta, otorgarle un derecho a silenciar todo conocimiento que se tenga sobre la vida privada cuando el conocimiento se obtiene de los agentes que intervienen el proceso de tratamiento. Esto es consecuencia del deber de secreto y confidencialidad que los registros deben preservar. La violación o amenaza que potencialmente exista, la controla el afectado a través del proceso de *habeas data*.

Asimismo, cuando el dato ha cumplido la finalidad para la cual se archivó, aparecen dos consecuencias que se traducen en derechos y deberes de la persona y el banco de datos, respectivamente. El derecho se fundamenta en la potestad de reclamar la eliminación de toda información que violente la esfera de privacidad personal cuyo almacenamiento no fuera autorizado. También, el poder de exclusión o supresión permite demandar la cancelación del dato que se ha tornado impertinente o ha devenido innecesario.

---

[211] RUIZ MARTÍNEZ, Esteban, *Los informes comerciales y el derecho a la información,* Ábaco, Buenos Aires, 2000, p. 122.

> Los derechos al silencio y al olvido se recogen de la ley de tratamiento de datos española que obliga a las personas que intervienen en cualquier fase del tratamiento de datos a mantener reservada la información que adquieren en ocasión del trabajo. Se trata por tanto —afirma Orozco Pardo— de la situación en que la existencia y contenido de los datos debe quedar dentro del ámbito funcional y finalidad del fichero para el que fueron recabados evitando el "rumor informático" (derecho al silencio) y del derecho a que, de oficio, el titular o responsable cancele o destruya los datos personales cuando se den alguno de los supuestos antes citados, sin que tenga que mediar previamente el ejercicio del derecho de cancelación (derecho al olvido).[212]

El deber, por su parte, es del titular del archivo, quien debe eliminar la información personal compilada que ha perdido interés, actualidad o sentido para el objeto inicialmente guardado.

El afectado, si considera que los datos carecen de pertinencia o devienen inadecuados, puede ejercer el derecho de cancelación o bloqueo de transmisión, propiciando en el pedido al registro que se borren todos los datos innecesarios.

357. Los principios contenidos en la calidad de los datos: *El principio de seguridad*

357.1. Los bancos de datos deben resguardar la seguridad de sus archivos, para evitar accesos no autorizados, o la penetración de la red informática por personas distintas a las que administran y están autorizadas para hacerlo.

El problema de la seguridad del archivo tiene dos facetas importantes: una atiende de la protección de los datos en particular; la otra, el cuidado especial que se debe tener con las personas que tratan la información y custodian la seguridad general del archivo.

En líneas muy amplias, este principio persigue el estricto cumplimiento de los derechos a la reserva y confidencialidad de la información personal almacenada, propiciando que los responsables en el tratamiento de los datos resuelvan los riesgos de filtración, inmiscusión directa, robo de información, y eventualmente, la pérdida parcial, destrucción total, o alteración de las bases.

> El objetivo que se persigue —según Estadella Yuste— es mantener la confidencialidad e integridad de los datos personales frente a actos exteriores que puedan ponerlos en peligro y, consecuentemente, perjudicar los intereses y derechos individuales. Asimismo, se informa que por un estudio realizado sobre las categorías principales relacionadas con la seguridad del procesamiento de datos, son atribuibles a los siguientes factores: equivocaciones 65%; empleados deshonestos 13%; infraestructura inadecuada 8%; varios 5%; personas externas a la actividad del fichero 3%.[213]

357.2. Los objetivos del principio de seguridad abarcan personas y equipamientos, y especialmente los sistemas de atención sobre los datos y los sistemas de comunicación. Por tanto, es conveniente puntualizar el alcance de cada uno.

---

[212] Orozco Pardo, ob. cit., p. 157.

[213] Estadella Yuste, ob. cit., p. 201.

El *primer problema* aparece con la seguridad que manifiesta el archivo en su calidad intrínseca, en suma se trata de asegurar la confianza de las personas sobre la reserva y confidencialidad que mantiene el banco de datos que almacenó informaciones personales.

Para ello es necesario afianzar la responsabilidad del registro en tres niveles sucesivos: *a)* controles realizados sobre las personas que trabajan para el archivo y toman conocimiento de los datos personales de otros; *b)* qué se hace para asegurar al sistema informático, en sí mismo; y *c)* cómo se controla o impide el ingreso de terceros (directo o indirecto) a las bases de datos.

En este aspecto se dan los niveles de seguridad siguientes:

a) *Seguridad técnica*

La seguridad técnica, evidentemente, cambia y se transforma constantemente, al punto que no es posible sentar reglas sobre tal o cual mecanismo para certificar el cumplimiento de la regla.

No obstante, existen algunas guías:

> las protecciones han de ser físicas y lógicas (entre éstas últimas están los paquetes de control de accesos), y existir una separación de entornos y una segregación de funciones, además de una clasificación de la información; y deben existir los medios para garantizar su eficiencia: asignación de responsables de los ficheros, administración de la seguridad, auditoría informática interna y posible contratación de la externa.

La opinión transcripta es de Miguel A. Ramos, quien agrega la necesidad de efectuar controles, que suelen dividirse en:

> a) *controles preventivos*: los que contribuyen a evitar que se produzcan hechos como incendio, acceso ilegítimo, etc.; b) *controles detectivos*: los que, una vez producidos, ayudan a conocer el hecho y actuar hacia el futuro; c) *controles correctivos:* que contribuyen a restaurar la situación de normalidad, como la recuperación de un fichero dañado a partir de copias de procesos anteriores.[214]

Asimismo cabe agregar lo dispuesto en el Estatuto de la Agencia de Protección de Datos (España) que aconseja las siguientes funciones inspectoras:

> *a)* sobre los soportes de información que contengan datos personales; *b)* sobre los equipos físicos; *c)* requerir el pase de programas y examinar la documentación y algoritmos de los procesos; *d)* examinar los sistemas de transmisión y acceso a los datos; *e)* auditorías sobre los sistemas informáticos.

En materia informática la seguridad técnica supone la integración de elementos externos al equipamiento (hardware y software) para que los controlen y aseguren de riesgos normales y anormales. En este sentido sería numerosa la enunciación de acciones posibles, aunque básicamente se refieren a las instalaciones donde funciona

---

[214] RAMOS, Miguel Ángel, "La seguridad y la confidencialidad de la información y la LORTAD", en revista *Informática y Derecho*, números 6/7, UNED, Mérida (España), 1994.

el archivo; sensores infrarrojos; blindajes; cámaras de televisión; contraseñas; seguros de riesgo, etc. etc.

b) *Seguridad lógica*

Se vincula con la intromisión que pueda sufrir una base de datos, sea desde otras terminales (locales o remotas), y las acciones que se pueden intentar para evitarlo.

En definitiva, son medidas organizacionales que deben adoptarse frente a la debilidad de los sistemas para contrarrestar las interferencias en la información.

> Es importante resaltar —dice del Peso Navarro— que hasta el momento presente en muchas empresas los datos de carácter personal han sido datos de segunda categoría toda vez que la preocupación principal estaba en garantizar la seguridad y la integridad de los datos de carácter simplemente económico, que eran los que se tenían que cuadrar y que podían reflejar el estado financiero de la empresa, teniendo más importancia que los datos de carácter puramente personal.[215]
>
> La Lortad vino a modificar ese temperamento, pues el objeto de la misma no es regular el sistema de seguridad de los archivos de las empresas con todas las implicancias que esto lleva, sino desarrollar un derecho fundamental de la persona que figura en la Constitución.

Como en el caso anterior, son múltiples las posibilidades de protección, pero cuentan con un problema de costos que han demostrado la reticencia de las bases de datos para asumir con decisión los programas de protección que deben tomar.

> El Convenio 108 del CE (28/1/81), así como las Directivas 95/46 y 97/66 relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de ellos, han afincado en el sector de las telecomunicaciones algunas medidas de seguridad que se deben cumplir en los ficheros automatizados; pese a que todas las normas continúan la imprecisión o nominado abierto, como cuando se dice que las medidas de seguridad deberán tener un nivel de seguridad apropiado con los riesgos que presente el tratamiento y con la naturaleza de los datos que deben protegerse, debiendo tener presente para conseguir tales fines, no sólo los conocimientos técnicos existentes en cada momento sino también el coste que pueda suponer su aplicación.

Las medidas más frecuentes tienen en común los pasos que orienta el llamado *"libro naranja"* del Departamento de Defensa de los Estados Unidos de América, del que se toman diez procesos: *a)* control de acceso; *b)* medios de almacenamiento; *c)* control de memoria; *d)* control del usuario; *e)* control de acceso específico; *f)* control de comunicación; *g)* control de insumos; *h)* control de encargos; *i)* control de transferencias, y *j)* control de organización.

Un mecanismo lógico de protección es el "*encriptado*" que asegura, en condiciones de acceso libre a los datos, un sistema de filtración al que sólo pueden llegar quienes tienen permitida la entrada (lo cual se consigue a través de la firma digital o de claves de identificación).

---

[215] DEL PESO NAVARRO, ob. cit., pp. 122 y ss.

Existen dos tipos de criptografía, explica Erica Baum:[216]

1. La de *clave de llave secreta o simétrica*: consiste en una clave compartida por dos entidades, una transmisora y otra receptora, que solo es conocida por ellas. Se dice que el sistema es simétrico porque requiere de un proceso de especificación de la clave.

2. La de clave de llave pública o asimétrica: en la cual se usan dos claves (sistema binario) una pública que, como su nombre lo indica, es de público conocimiento y otra privada, la cual no es revelada ni transmitida a persona diferente a la cual la misma pertenece. En este sistema asimétrico la clave pública se usa para cifrar el mensaje y la privada para descifrarlo.

La ventaja de este sistema respecto del anterior es que permite a través de la firma digital o autenticación digital mantener en confidencia tanto la identidad de quien envía el mensaje como la integridad del mismo.

Por lo tanto, la firma digital torna imposible la alteración de la firma y permite verificar con certeza la identidad de quien dice ser el firmante, quien no podrá a la postre alegar adulteración o falsificación de la misma.

Para hacer uso de la firma digital es necesario que la persona posea un certificado de autenticación, el cual solo puede ser extendido por una autoridad certificante legítimamente habilitada a tal efecto y cuya función es otorgar respaldo acerca de la información contenida en el certificado. Dicho certificado es un documento digital firmado digitalmente por un certificador de clave pública, que asocia esa clave pública con su titular durante el período de vigencia del certificado.

Es atribución del estado nacional garantizar a sus ciudadanos el derecho constitucional a la seguridad e intereses económicos y a una información adecuada y veraz. En Argentina, el 16 de abril de 1998, mediante Decreto 427/98 se aprobó la implementación de esta tecnología en el ámbito de la Administración Pública Nacional con el objeto de hacer más eficientes los circuitos administrativos.

c) *Seguridad organizada por vía reglamentaria*

El Convenio 108 del Consejo de Europa (CE) ha resuelto que se tomen medidas de seguridad adecuadas para la protección de datos personales con el fin de evitar inconvenientes derivados de la destrucción, pérdida accidental o provocada, así como para eliminar en el mayor grado de certeza posible, la intromisión en los archivos y la difusión no autorizada.

En la exposición de motivos se confirma el sentido de las medidas al exponerlas en relación con las funciones que se deben asegurar: *a)* La vulnerabilidad de los datos (por eso, los datos sensibles exigen medidas de prevención más estrictas); *b)* la necesidad de que el acceso sea restringido*; c)* que el archivo o recolección de datos tenga en cuenta el tiempo que permanecerá disponible el dato; *d)* los riesgos propios de cada archivo; *e)* la finalidad prevista.

En países donde el tema está en ciernes, existe un vacío legislativo evidente que permite interferir las bases de datos sin que la acción tenga prevista una consecuen-

[216] BAUM CORTE, Erica, "La propiedad de la información", *Revista de Derecho Informático*, versión on line.

cia punible. Por eso, buena parte de la tarea que se viene será resolver la complejidad del problema y orientar con medidas las acciones a concretar.

Tomemos por ejemplo, la "Agencia de Protección de Datos" de España, aprobada por el Real Decreto 428 del 26 de marzo de 1993 que se ha dado para sí un Estatuto y dos reglamentos.

La profusión normativa asigna una de los conjuntos legales para el tema de la seguridad de la información y la forma en que ésta ha de ser aplicada por los responsables de los ficheros.

> La publicación de la ley ha creado cierta alarma en los medios empresariales y ha servido también para llevar cierta inquietud a más de un directivo del sector privado. Según Del Peso Navarro, esto no ha sido así en el sector público, y las razones pueden ser de dos tipos: una empresarial y otra personal. Respecto de la primera se afirma que está motivada por la inexistencia en el mundo empresarial español de una cultura de la seguridad en sus tres aspectos físico, lógico y jurídico; mientras que en otros países, además de dar mayor importancia a los problemas relacionados con la seguridad, han pasado ya por tres generaciones de leyes de protección de datos y por tanto la entrada en vigor de leyes de este tipo no ha supuesto ningún trauma pues esta cultura de la seguridad se ha ido imponiendo poco a poco y su aplicación no ha representado sacrificios económicos; el problema personal se analiza desde la perspectiva de la misma ley que hace pensar a los directivos de empresas privadas que son ellos los responsables del archivo y, por tanto, sobre quienes pesa el riesgo patrimonial frente a las eventuales crisis del sistema.[217]

La imposibilidad de generar por vía normativa una consigna sobre medios y acciones técnicas y lógicas que resuelvan la seguridad de los archivos con datos personales, ha sugerido el establecimiento de niveles para identificar donde ha de asentarse la mayor preocupación.

En tal sentido se establecen escalas de riesgo:

Nivel básico

Orienta a que el responsable del archivo tenga un manual de instrucciones de conocimiento obligatorio para todas las personas que actúan bajo su dependencia y, sobre todo, de aquellos que tienen la tarea de incorporar datos y procesarlos a los fines que el registro ha previsto. Este documento debe contener, como mínimo, el ámbito de aplicación y los recursos protegidos; las medidas, normas, procedimientos y estándares aplicados; las funciones y obligaciones del personal; la estructura de los archivos o bancos de datos con la descripción de los sistemas de información que los tratan; los procedimientos de notificación, gestión y respuesta ante las eventuales incidencias; procedimientos previstos para la actualización permanente del manual, entre otras.

En este nivel es obligatorio que exista una relación de personas que tengan derecho de acceso, y establecer procedimientos de identificación y autenticación para dicho acceso. Es, en otros términos, el método de identificación del usuario.

---

[217] DEL PESO NAVARRO, ob. cit., *passim*.

Cuando el mecanismo de autenticación se base en contraseñas existirá un procedimiento de asignación, distribución y almacenamiento de claves que garantice su confidencialidad e integridad. Las contraseñas se cambiarán con una periodicidad que tendrá que estar establecida en el documento y se registrarán en forma ininteligible (cifradas).

Nivel medio

En este nivel la actividad de simple colección de datos agrega el aditamento del tipo de archivo creado y, por ello, la mayor intensidad en los sistemas de seguridad.

Hablamos de registros sobre infracciones administrativas, penales, crédito, situación patrimonial, servicios financieros, etc., en los cuales, además de cumplir las medidas señaladas anteriormente para el nivel básico, deben tener un responsable de la seguridad, encargado del control directo y auditoría permanente del sistema.

Nivel alto

Es el nivel destinado para al tratamiento de datos sensibles.

La Directiva 95/46 CE, en el artículo 8 (Tratamiento de categorías especiales de datos) dice:

> 1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.
>
> 2. Lo dispuesto en el apartado 1º no se aplicará cuando:
>
> *a)* el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o
>
> *b)* el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o
>
> *c)* el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o
>
> *d)* el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o
>
> *e)* el tratamiento se refiera a datos que el interesado haya hecho manifiestamente público o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.
>
> 3. El apartado 1º no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en

virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.

4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2º, bien mediante su legislación nacional, bien por decisión de la autoridad de control.

5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.

6. Las excepciones a las disposiciones del apartado 1º que establecen los apartados 4 y 5 se notificarán a la Comisión.

7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Las medidas de seguridad se extreman, así como las responsabilidades por su violación son superiores. El establecimiento de prevenciones ha de ser permanente y las infracciones penadas y multadas.

357.3. El *segundo problema* es la protección directa sobre los datos personales que se han colectado para el archivo.

El nivel de seguridad difiere en los de fácil acceso respecto a los denominados sensibles. En unos (por el caso, nombre y apellido, domicilio, teléfonos, identificación, estado civil) la simplicidad del acceso y la multiplicación de lugares de búsqueda, impiden sentar reglas demasiado estrictas.

En otros datos más privados y personales (o personalísimos como la ideología, enfermedades, hábitos sexuales, etc.) se reserva un tratamiento más severo requiriendo un alto nivel de seguridad para impedir el acceso a ellos.

Las tareas que se encargan a los formadores de archivos y sus responsables, no impiden el diseño de programas generales de protección hacia los datos personales, como los desarrollados por *la World Wide Web Consortium* (W3C) con el fin de mejorar la defensa de la intimidad.

Se trata de un protocolo denominado P3P, o *plataforma para las preferencias de privacidad,* por el cual mediando un intercambio de información entre el usuario y el sitio en la red, ésta le informa qué posibilidades tiene para ocultar sus datos ofreciendo opciones que se resuelven y comunican a través del navegador.

El funcionamiento es bastante sencillo. Un usuario de Internet expresa que no quiere dejar sus datos personales para que sean revelados a terceros pero que lo hará a los fines de concretar una adquisición que, posteriormente a ella, lo podrá identificar de un modo

codificado. Según Ann Cavoukian, el acceso a la información necesaria para las operaciones de red puede dificultarse aún más mediante la navegación basada en la utilización de un dispositivo específico (*Web anonymizer*) que permite una actuación completamente anónima. El usuario tiene la capacidad de mantener el anonimato y revelar de todos modos ciertos datos no identificativos (como el equipo deportivo para acceder a una página de noticias, la ciudad de residencia para recibir previsiones metereológicas, etc.).[218]

Otra opción son los sellos para la protección de la intimidad, por los que cualquier persona que no se quiere identificar puede exigir a la firma que opera en comercio electrónico, la certificación del respeto al secreto y confidencialidad de la operación. De esta calidad son firmas como WEBTrust (algo así como Instituto de Censores Jurados de Cuentas de Estados Unidos) o el "*Privacy seal program*" (Programa de sellos para la protección de la intimidad).

Cabe recordar también las llamadas "*Listas Robinson*" que fueron implementadas con la finalidad de impedir la molestia que ocasiona la venta telefónica de productos o su oferta por correo. Para ello, quienes desean no recibir esa información se anotan en las listas y quedan automáticamente excluidos.

[218] CAVOUKIAN, Ann, *Comercio electrónico: las personas necesitan protección, no perfección,* en XX Conferencia Internacional de autoridades de protección de datos (1998), Agencia de Protección de Datos, Madrid, 1999, pp. 277 y ss.

Sección 8ª La responsabilidad de los operadores de datos personales

358. Los alcances de la responsabilidad

358.1. Los principios recién enseñados encuentran responsables en distintos niveles. Por eso el tema se presenta desde el "*principio de responsabilidad*", por el cual se exige la identificación del titular del fichero, sea nacional o extranjero, a fin de poderle asignar una serie de responsabilidades proyectadas desde las obligaciones legales sobre la protección de datos de carácter personal.

> Este planteo lo hacen muchos autores que han interpretado la Ley de protección de datos española. Particularmente, Estadella Yuste dice que hay que averiguar si la responsabilidad por incumplimiento debe recaer exclusivamente sobre el titular del archivo, o si debe ser compartida entre las personas involucradas en la recogida, procesamiento o transmisión de datos personales.[219]
>
> Hellner se ha manifestado en contra de que las disposiciones sobre responsabilidad estén demasiado relacionadas con el concepto de control general sobre el sistema computarizado, pues interpreta que el tema de responsabilidad se debe juzgar separadamente.[220]

En todo caso la situación tiene que establecer la diferencia entre: *a)* administrador del archivo; *b)* persona encargada del tratamiento, *c)* características del servicio; *d)* interconexión de los datos.

358.2. *Administrador del archivo* puede ser una persona física o jurídica, de carácter estatal o particular, que por las funciones que lleva a cabo puede resolver sobre la finalidad, contenido y destino de los datos personales que almacena. Es el verdadero responsable porqué tiene el control y el poder de decisión. También se denomina *usuario*, cuando la persona —pública o privada— realiza a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos o a través de conexión con los mismos.

Cualquiera sea la nominación lo exacto es deducir la representación primera en el responsable, debiendo entender por tal a quien decide sobre el tratamiento de datos personales.

---

[219] ESTADELLA YUSTE, ob. cit., p. 203.

[220] HELLNER, John, *From data proteccion to knowledge machines,* Kluwer, Deventer, 1990, pp. 18 y ss.

Encargado del tratamiento es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trabaja con datos personales por cuenta del responsable del tratamiento. En otros términos, es el operador de las bases, quien está obligado por el código de confidencialidad que debe tener el lugar donde trabaja.

358.3. Finalmente, donde mayores inconvenientes se encuentra, es en la eventual *interconexión de los datos* que puede llevar a que el tratamiento sea realizado por terceras personas contratadas al efecto.

De suyo, el administrador o titular del archivo no elimina su responsabilidad, ni la descarga en otro; la situación a resolver es el alcance de la obligación al tercero que viola el secreto conferido cuando se le encargó el trabajo.

El art. 10 de la ley argentina (Deber de Confidencialidad) establece que:

> 1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aún después de finalizada su relación con el titular del archivo de datos.
>
> 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Esta situación merece ser considerada en la doble dimensión que supone. Por un lado el deber del archivo, registro o banco de datos para dar estricto cumplimiento con los principios y deberes a que se encuentra obligado; y por otro las sanciones civiles (resarcitorias) y penales (represiones) que la violación determine.

358.4. De la dualidad se desprenden dos consecuencias. Si el titular o responsable del archivo no cumple con los mandamientos legales impuestos, se presume la culpa y el derecho del afectado a ser resarcido en la medida del perjuicio habido; de otro lado, el organismo de fiscalización, allí donde sea instalado, puede aplicar sanciones y multas de acuerdo con la gravedad del ilícito.

De esta forma se resuelven ambos frentes derivados de la responsabilidad emergente por la administración de los datos personales de los individuos concernidos.

> Interpretando la ley española, Herrán Ortiz afirma que la responsabilidad del titular del fichero frente al afectado por el incumplimiento de las obligaciones, ya se realice materialmente por él o por un tercero a su cuenta, está regulado en la misma normativa. De forma tal que el titular es el responsable, aunque ello no obsta a que, en aquellos supuestos en que sea posible individualizar la responsabilidad en otro sujeto interviniente, se pueda actuar solidariamente contra ambos, eso sí, sin excluir la responsabilidad del beneficiado por el tratamiento y a cuyo nombre se verifica, que en ningún caso quedaría librado de sus obligaciones, sin perjuicio de que pueda repetir contra el tercero causante del daño cuando él haya soportado las consecuencias de dicha actuación.[221]

---

[221] HERRÁN ORTIZ, ob. cit., p. 278.

359. La fuente legal de atribución de responsabilidad administrativa

359.1. La responsabilidad administrativa se puede dar en dos niveles. En las legislaciones que introducen un órgano de fiscalización sobre archivos, registros, bases o bancos de datos públicos y privados, son ellos quienes aplican penas cuando la ley no se cumple.

Comparativamente se puede afirmar que el ámbito de facultades no es preciso, porqué la sanción admite revisión judicial, o en ocasiones, se subordina a que sean los jueces quienes dispongan la pena a petición del órgano de control.

No obstante queda establecida la potestad de investigar de oficio cualquier hecho que, a su discreción, considere que deba ser motivo de control.

> En tal sentido, la organización administrativa de la Dirección Nacional de Protección de Datos Personales (Argentina) pone énfasis en la necesidad de contar con un cuerpo profesional experto en las técnicas de procesamiento de datos.
>
> En España, informa Herrán Ortiz que, la función de inspección se limita a la obtención de información y hechos en relación al tratamiento de datos, de ahí que se encomienden en el artículo 28 del Estatuto, a la Inspección de Datos, inspecciones periódicas o puntuales, de oficio o a instancias de los afectados, de cualesquiera ficheros de titularidad pública o privada, en los locales que se hallen. A tal efecto, podrá examinar los soportes de información que contengan los datos personales, los equipos informáticos, así como los sistemas de transmisión y acceso a los datos, y podrá requerir el pase de programas y examinará la documentación pertinente al objeto de determinar los algoritmos de los procesos sean objeto; podrá igualmente, realizar auditorías de los sistemas informáticos, así como requerir la exhibición de los documentos que se consideren pertinentes para el cumplimiento de la inspección.[222]

359.2. Al no ser absolutamente claro el alcance de sus posibilidades de intervención, cada entidad suele elaborar cuanto un reglamento propio, con el fin de disponer de un marco más acertado y menos conflictivo.

Las funciones esenciales que se vinculan con la potestad de fiscalización son:

a) Control sobre la creación y registro de archivos.

b) Control sobre el funcionamiento de los archivos.

c) Controlar la observancia de las normas sobre integridad y seguridad de datos.

d) Controlar el cumplimiento de los principios sobre calidad de los datos.

e) Evaluar de oficio, o a pedido de parte, el nivel de protección proporcionado por las normas de un Estado u organismo internacional hacia donde se transfiera información personal.

359.3. En líneas muy amplias, la autoridad de control debe intervenir de oficio y/o por requerimiento, cuando cumpla funciones de vigilancia; es decir, en los casos que actúa como organismo de aplicación y fiscalización de la ley sobre protección de datos personales.

---

[222] HERRÁN ORTIZ, ob. cit., p. 288.

Es evidente la necesidad de contar con estas entidades, no solo para evitar que la tutela legal se confiera *ex post facto*, sino para conseguir que los principios creados sean efectivos y aplicables en un contexto real.

En consecuencia, donde no existen órganos de control, la propia ley se posterga, y deja todo en manos de los jueces y tribunales constitucionales.

359.4. Si a estas dificultades le agregamos el carácter programático de muchas disposiciones, las que requieren de interpretación y complemento jurisdiccional, observaremos lo simple y elemental que resulta la creación de este organismo de fiscalización.

En realidad, las funciones de vigilancia llevan a la eventual aplicación de sanciones; mientras que las acciones de carácter consultivo y las funciones de prestación como es el registro y el censo de archivos, no provocan demasiados problemas.

Cuando se forma un sumario o se practica una investigación, el efecto puede llevar a la denuncia o querella penal, y a la aplicación de sanciones (multas).

La responsabilidad de titulares o usuarios de archivos, registros, bases o bancos de datos públicos se debería sustanciar a través de sumarios e investigaciones preliminares, sin perjuicio de la actividad judicial que corresponda en las etapas procesales pertinentes. En todos los casos no se puede soslayar el derecho de audiencia y prueba.

360. Clasificación de las infracciones

360.1. Las infracciones se pueden calificar como leves, graves o muy graves. Como sanciones leves, se consideran, a título ejemplificativo: *a)* no atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda; *b)* no proporcionar la información que solicite la autoridad de control en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos; *c)* no solicitar la inscripción del fichero de datos de carácter personal, cuando no sea constitutivo de infracción grave; *d)* proceder a la obtención de datos de carácter personal de los propios afectados sin proporcionarles información sobre el alcance y destino; *e)* incumplir el deber de secreto y confidencialidad, entre las más evidentes.

360.2. Se consideran sanciones graves: *a)* Proceder a la creación de archivos, registros, bases o bancos de datos públicos o iniciar la obtención de datos de carácter personal para los mismos, sin autorización; *b)* originar la creación de archivos, registros, bases o bancos de datos privados o iniciar la obtención de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad; *c)* implementar la obtención de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible; *d)* tratar los datos de carácter personal o usarlos posteriormente con violación de los principios y garantías establecidos o con incumpli-

miento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave; *e)* el impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada; *f)* mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas; *g)* conservar archivos, registros, bases o bancos de datos, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen; *h)* no remitir a la autoridad de control las notificaciones previstas en las leyes o en sus disposiciones reglamentarias, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos; *i)* la obstrucción al ejercicio de la función inspectora; *j)* no inscribir el archivo, registro, base o bancos de datos de carácter personal en el Registro correspondiente, cuando haya sido requerido para ello por la autoridad de control y aplicación normativa.

360.3. Se estima que pueden ser sanciones muy graves: *a)* La obtención de datos en forma engañosa y fraudulenta; *b)* no cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por la autoridad de control o por las personas titulares del derecho de acceso; *c)* tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales; *d)* la vulneración del deber de guardar secreto sobre los datos de carácter personal; *e)* no atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición; *f)* denegar de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en archivos, registros, bases o bancos de datos.

360.4. En Argentina la reglamentación establece que el sumario administrativo se inicia: *a)* de oficio; *b)* a petición de parte interesada; *c)* por la acción del Defensor del Pueblo y *d)* por la actividad que realicen, en tal sentido, las asociaciones de usuarios y consumidores.

La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora.

Ahora bien, si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuricidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

En ningún caso podrá imponerse una sanción más grave que la fijada en la ley para la clase de infracción en la que se integre la que se pretenda sancionar.

361. Responsabilidad civil

361.1. La posibilidad de reclamar daños y perjuicios originados por la afectación que a una persona le produce el tratamiento de sus datos personales, está reconocido en numerosas legislaciones.

En *Argentina* surge del propio articulado de la ley y del sistema de fondo que une el factor de atribución con el nexo de causalidad, es decir que relaciona al titular o usuario de la base de datos con el afectado, presuponiendo que la violación legal es causa fundada para la reparación.

Panamá lo establece en la línea de los derechos de los consumidores o clientes:

> que sufran algún daño o perjuicio por razón de la inclusión de uno o más datos erróneos, inexactos, equívocos, incompletos, atrasados o falsos, en la base o banco de datos de una agencia de información de datos, tendrán derecho a ser indemnizados por quien resulte responsable por la inclusión de dichos datos, ya sea por culpa o por negligencia, sea este el agente económico o la agencia de información de datos [...].

En *Paraguay* se sanciona y responsabiliza a la entidad que da informes erróneos de solvencia o cumplimiento de las obligaciones. Lo mismo en *Ecuador* que establece:

> Los burós y las fuentes de información crediticia serán legalmente responsables por los daños ocasionados al titular como consecuencia de la transmisión de información ilegal, inexacta o errónea y, por tanto, no estarán exonerados alegando ausencia de dolo o de culpa. La responsabilidad de las fuentes es entregar información a los burós de manera exacta y legal; la responsabilidad de los burós es reportarla sin alteración o modificación alguna. Sin perjuicio de lo anterior, en los procesos promovidos contra los burós, éstos podrán pedir que se cite también con la demanda a la o las fuentes de las que hubieren obtenido la información crediticia materia del proceso, siguiendo el procedimiento establecido en el artículo 94 del Código de Procedimiento Civil. También responderán por los daños causados al titular de la información crediticia, quienes utilicen dolosa o culposamente informaciones o reportes provenientes de los burós. El afectado podrá demandar indemnización, cuando la información errónea no ha sido rectificada por los burós.

La ley *peruana* 27.489, sobre Centrales de Información de riesgo y protección del titular de la información estipula: "[...] 18.1 La responsabilidad civil de las CEPIRS por los daños ocasionados al titular por efecto del tratamiento o difusión de información será objetiva. Las CEPIRS podrán repetir contra las fuentes proveedoras de información cuando el daño sea ocasionado como consecuencia del tratamiento de información realizada por éstas".

La ley 19.628, de *Chile* establece: "Artículo 11.—El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños".

Aún en los países que no tienen norma expresa, como Costa Rica, se encuentran sentencias judiciales condenatorias que ordenan excluir determinados datos crediticios negativos, por haber caducado su vigencia (derecho al olvido) y condenan a la empresa que había difundido la información a pagar los daños y perjuicios correspondientes.[223]

361.2. La responsabilidad civil se produce a consecuencia de generar el banco de información de datos personales, un reporte que le causa al concernido un daño directo que puede anidar en la esfera de sus sentimientos (intimidad, vida personal; privacidad; etc.), o bien generarle un perjuicio (*v. gr.:* denegatoria de un crédito; interdicción en sus cuentas bancarias; etc.) o alterar su imagen personal (*v. gr.:* reputación; fama, etc.).

Es decir que no solamente el error o la deficiencia de las oficinas de información comercial son las que producen un daño a resarcir; sino todos lo responsables, titulares y/o usuarios que trabajan con datos personales.

Los daños pueden ser de fuente contractual o extracontractual. Cuando interviene una empresa emisora de tarjetas de crédito, el servicio en el cual se enmarca ese sistema ubica la responsabilidad de sus integrantes en el ámbito contractual, imponiendo una obligación solidaria entre todos los intervinientes (art. 40, ley 24.240 que, en Argentina, es la ley de defensa de usuarios y consumidores) y en todo caso, le queda a la emisora una acción de repetición contra el banco, si así lo considera.

Pero también se considera que el error en que incurrió el banco demandado, sin perjuicio de la relación que lo vincula al afectado, configura un obrar antijurídico que encuadra dentro del ámbito de la responsabilidad aquiliana, en cuanto a las publicaciones en diversos sitios de Internet del informe erróneo que proporcionó. Ello justifica la condena tanto por las consecuencias inmediatas, como por las consecuencias mediatas, ocasionadas por su imprudente comportamiento (arts. 904 y 1109 del Código Civil de Argentina).

361.3. Según Molina Quiroga:

> […] el carácter profesional juega un papel importante para establecer la responsabilidad de las entidades financieras, ya que la superioridad técnica que detentan les impone el deber de obrar con mayor prudencia y pleno conocimiento del negocio y les exige una diligencia acorde con su objeto haciendal, con organización adecuada para desarrollar su giro, o sea su carácter profesional.
>
> Es que parece evidente que la conducta de una entidad bancaria o de una emisora de tarjetas de crédito no puede apreciarse con los parámetros exigibles a un neófito, sino conforme al standards de responsabilidad agravada que el profesional titular de una empresa con alto nivel de especialización tiene frente al usuario, dado que en los contratos en los que una de las partes detenta superioridad técnica, la otra soporta una situación de inferioridad jurídica.

---

[223] MOLINA QUIROGA, tesis doctoral, inédita

Similares argumentos son aplicables con relación al gestor de una base de datos sobre riesgo crediticio, quien por su indudable condición profesional, asume una obligación de diligencia especial, que está claramente establecida en nuestra Ley de Protección de Datos Personales y puede advertirse en las normas de derecho comparado.

En tal sentido, se ha destacado que la complejidad del tráfico hace exigible una protección responsable del consumidor desde que la confianza como principio de contenido ético impone a los operadores un inexcusable deber de honrar esas expectativas, y cuando ello se quiebra se contravienen los fundamentos de toda organización, tornando inseguro el tráfico.

Esta exigencia de mayor diligencia, en el tema que nos toca abordar, se traduce también en una adecuada respuesta para rectificar datos erróneos, medida en términos de tiempo. En esta línea, por ejemplo, se ha aplicado el principio de las cargas probatorias dinámicas, al sostener que la circunstancia que la entidad financiera no acompañe la documentación (que respalde sus defensas), en rigor, es invocar su propia torpeza en una técnica operativa concerniente a su esfera de actuación, lo que resulta enteramente inadmisible, y que se trata de un empresario titular de hacienda especializada en razón del objeto; y ello no sólo implica estándares agravados de responsabilidad; sino plena oponibilidad a su respecto de un modo operacional convencionalmente pactado y dotado de fuerte tipicidad.

Relacionado con tarjetas de crédito se ha responsabilizado tanto al banco como a la emisora de la tarjeta, cuando no han obrado con diligencia frente a maniobras dolosas de terceros que llevaron a la inclusión del actor como deudor moroso, o a errores del banco al emitir tarjetas no solicitadas. También se ha resuelto que existe daño moral cuando se ha debido sufrir la destrucción en público de tarjetas de crédito, con motivo de informes erróneos suministrados por un banco. En los casos de "robo de identidad" se ha responsabilizado a las entidades bancarias, sosteniendo que no las exime de responsabilidad el hecho de un tercero (que había sustraído el DNI de la actora), si al momento de dar curso a la apertura de cuenta corriente a nombre de la accionante, no cumplió con las exigencias que su especialización y diligencia requerían a fin de dar cumplimiento con las disposiciones bancarias respecto a la comprobación de la identidad y la solvencia moral y económica del solicitante.[224]

361.4. En el caso de los burós de créditos, o de empresas destinadas a dar información comercial, la situación es más difícil porque si los datos se toman de fuentes de acceso público, la central podría argumentar que el deber de actualizar la base es de quien se responsabiliza por ella. En cambio, si el test de legalidad se toma de los principios que asienta la protección de datos personales, bastaría con analizar el defecto que se atribuye para derivar la responsabilidad eventual.

En Argentina no se resuelve aun con precisión este tema, existiendo dos tendencias, una que fundamenta la ausencia de responsabilidad de las empresas de informes crediticios, afirmando que si ellas debieran verificar la veracidad de cada uno de los datos informados por el Banco Central antes de comunicarlos a terceros (lo que se da por descontado que sería imposible, porque les exigiría tener acceso a la totalidad de las carpetas de las entidades financieras), sería tal la magnitud de la

[224] MOLINA QUIROGA, tesis doctoral citada, *passim*.

ímproba tarea, que concluirían por cerrar sus puertas, con lo que literalmente una actividad lícita vendría a resultar prohibida por efecto de una teoría pretoriana.[225]

> En similar sentido se ha argumentado que las empresas dedicadas a brindar información comercial, registran datos obtenidos de una fuente pública, como la Central de Deudores del Sistema Financiero del B.C.R.A. y no intervienen en la calificación efectuada respecto de la situación financiera de los deudores (o presuntos deudores), por lo que no pueden ser responsables de los daños ocasionados por causa de los informes erróneos.

Otros, en cambio, observan los deberes que la ley impone a todo aquél que trabaja con datos e información confidencial de personas físicas o jurídicas. En este aspecto, cuando se encuentra que hay un uso indebido de los datos (sin importar cual sea el error) existe un deber de indemnizar, que se toma de la responsabilidad que tiene el operador y su profesionalidad implícita.

361.5. Por eso, la doctrina pendula entre una y otra tendencia. Algunos argumentan que:

> […] como es sabido los bancos realizan operaciones de servicios que consisten en brindar informaciones a clientes, terceros y jueces mediante los oficios judiciales correspondientes a causas judiciales en trámite. De ahí que revista importancia el tema de la responsabilidad de los bancos cuando en dichos informes aparecen errores en la información, o bien ésta resulta falsa y como en consecuencia origina perjuicios. En este sentido el moderno derecho de daños reconoce siempre que exista una relación causal adecuada entre el daño y la información falsa o errónea el derecho a una indemnización o reparación del perjuicio sufrido.
>
> Considerar la información como producto o como servicio es importante a los fines de establecer las consecuencias derivadas para el titular de un banco de datos por los daños causados al receptor de dichos datos. Para Bekerman[226] conforme sea la respuesta, la responsabilidad se hará extensiva a otros haciendo a un lado la regla de *res inter alios acta*. Asimismo cabe preguntarse en el caso específico de los bancos de datos de los clientes de las entidades financieras si se trata de un servicio o producto, ya que para el autor que venimos citando, en el primer caso no se genera una obligación de resultado mientras que el segundo sí. También otro elemento importante es evaluar si el banco de datos está destinado a ser utilizado en forma indiscriminada por un número indiscriminado de personas o sí está dirigido a usuarios determinados. Para el autor de referencia las publicaciones que realiza el B.C.R.A. con relación a los inhabilitados para la obtención de cuentas corrientes o de los registros oficiales de bienes registrables, puede considerarse a la vez un servicio y un producto. Arriba a esta conclusión partiendo de la base que el titular del banco de datos determina su carga en función del objetivo tenido en cuenta para su generación. En función de ese objetivo y de cómo trasciende a los terceros usuarios, el banco de datos puede ser considerado servicio o producto.

---

[225] MOLINA QUIROGA, tesis doctoral citada, *passim*.

[226] BEKERMAN, Jorge, *Bases de datos y bancos de datos. Producto o servicio (consideraciones sobre la responsabilidad*), La Ley, 1990-C, 943.

> Bekerman concluye que la información generada por un banco de datos es siempre un producto, y que el consumidor de la información, tiene acción por responsabilidad objetiva contra los elaboradores del producto. Por nuestra parte disentimos con el original planteo del autor citado, que en su afán de asimilar el servicio de información bancaria pretende aplicarle una responsabilidad objetiva consagrada en la Ley de Defensa del Consumidor para los productos elaborados. Parece ser evidente la tentación de cierto sector de la doctrina nacional en querer imponer un criterio de responsabilidad objetiva para la responsabilidad de los bancos. Pero lamentablemente no tiene en cuenta que la responsabilidad objetiva es excepcional y por lo tanto requiere su consagración expresa como es el caso del art. 1113 del Código Civil, al que también se ha recurrido para justificar esta posición doctrinaria partidaria de la responsabilidad objetiva de los bancos. No hay que olvidar que el art. 1113 del Código Civil se refiere a la responsabilidad extracontractual, mientras que los errores cometidos por la entidad financiera en el servicio de información constituyen un incumplimiento contractual frente a una obligación de resultado, que surge de la profesionalidad del vínculo del banquero con su cliente.[227]

361.6. En forma diferente, y creemos más apropiada, se sostiene que el estudio debe partir de los presupuestos para imputar responsabilidad, tomando en primera línea al factor de atribución.

El uso informático y la creación de archivos generan deberes y responsabilidades que, al incumplirse, ingresan en el terreno de lo ilícito, de modo que los objetos y actividades de la informática pueden adscribirse en la idea de riesgo creado. El factor de atribución es objetivo.

Así se entiende que:

> […] si apreciamos el problema bajo la faz de la responsabilidad objetiva, resulta evidente que un Banco de Datos conforma un instrumento riesgoso de por si (riesgo de la cosa) que hace plenamente aplicable la responsabilidad del dueño o guardián por vicio o riesgo de la cosa que sólo puede quedar neutralizada si éste último acredita, sin asomo de duda, la culpa de la víctima o de un tercero por el que no debe responder, o alguna circunstancia de caso fortuito o fuerza mayor.[228]

Pero el deber de tener información veraz y actualizada es del responsable o titular, que es una persona diferente al que aporta esa información. Si es el titular concernido, no habría responsabilidad porque quien da los datos es el afectado; mientras que cuando se toman de fuentes de acceso público, la duda cierne sobre la responsabilidad del que cede y comunica los datos.

Aquí lo evaluado es la situación desde una óptica subjetiva. Se trata de determinar la existencia de culpa, la cual es evaluada de manera rigurosa atento su profesionalidad, responsabilidad que en su caso está agravada por el deber de actuar con pericia.

---

[227] LIVELLARA, Silvina, "*Habeas data* e información crediticia. La eventual responsabilidad civil de las entidades financieras y del Banco Central de la República Argentina por cesión y publicidad de datos inexactos", *Revista de Derecho Informático*, versión on line (www.alfa-redi.com).

[228] CNCiv., Sala K, 2002/10/22, "*Gutiérrez Juan Carlos Demetrio c/ Banco de la Provincia de Buenos Aires y otro*", La Ley Online.

La diligencia exigible al organismo de información crediticia es la de un profesional experto y no un *bonus pater familiae*, que en función de su actividad, debido a la especialización de las operaciones que realiza, tiene que guardar objetiva y subjetivamente la diligencia que comporta los riesgos derivados de su alta cualificación.

Adicionalmente, se ha puesto de resalto que la responsabilidad del banco es agravada por su condición de experto frente al desconocimiento del cliente respecto de la materia. Así se dijo: "la diligencia de un banco ha de ser la de un comerciante prudente y experto y, en consecuencia, deberán juzgarse con mayor severidad sus errores o negligencias, al tratarse de la actuación de un técnico en el que se confía el cliente, carente, en generalidad, de conocimientos específicos sobre la materia".[229]

En materia contractual también se habla de la obligación de seguridad que tienen los bancos para con los clientes, que son considerados consumidores a tenor de la ley de defensa de consumidor. En consecuencia acaecido el daño la culpa se presume y será el Banco el que deberá demostrar que la causa del daño le es ajena.[230]

362. Obligaciones de registro o inscripción

362.1. La posibilidad de ejercer una fiscalización efectiva sobre los bancos de datos personales no podría concretarse sin saber cuáles son ellos y qué finalidades reportan.

Las *características del servicio* obedecen a la característica pública o privada del banco de datos, determinando obligaciones diferentes pero un régimen igual. En ambos casos se ha dicho que *todo archivo, registro o banco de datos público y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control* (art. 21 inciso 1º, ley 25.326 de Argentina).

Recordemos que los sistemas de protección de datos se dividen entre quienes dejan la voluntad de control en la acción de *habeas data* deducida por el afectado u otros legitimados; y los que crean organismos de fiscalización. El primer mecanismo corre el riesgo de dispersar los esfuerzos en favor de proteger la intimidad solamente a partir de la disposición del particular, sin que el banco de datos observe un mecanismo de vigilancia sobre sus actos. Los otros pueden provocar aparatos burocráticos que si no tienen independencia del poder central de administración caen en el vicio de la inoperancia.

362.2. Señala Gils Carbó que la designación de una autoridad administrativa para controlar el tratamiento automatizado de datos personales ha suscitado las quejas

---

[229] Pellon Rivero, R. *Cancelación de tarjeta de crédito por error*, Actualidad y Derecho, 1995-I, 168.

[230] Martínez Medrano, Gabriel, "Responsabilidad Civil de las Entidades Financieras por la generación, difusión y mantenimiento de información crediticia errónea", *Revista de Derecho Informático,* nº 80 (2005), versión on line (www.alfa-redi.com).

del sector privado debido a la injerencia que puede tener en el uso de la informática, ya que las empresas realizaron grandes inversiones de tiempo y dinero procesando datos obtenidos de los titulares o de registros públicos, que los recopilaban en sistemas viejos e inaccesibles. Sin embargo, lo cierto es que los principios de la ley quedarían como una declaración retórica si no se establece un modo eficaz de imponer su aplicación y sancionar a los responsables. Máxime, que se presenta una situación de notoria desigualdad entre el individuo titular de los datos y los responsables de los registros o bases de datos, sobre todo cuando éstos son el Estado y las corporaciones empresarias. Si al poder de la tecnología, que permite procesar millones de datos con sentido de prospección, le sumamos el poder político o económico, la suerte de los individuos para defender su intimidad está echada. La autoridad de control está llamada a subsanar esa brecha entre unos y otros, ya que si esa situación objetiva no fuera atendida por el Estado habilitando esa modalidad de garantía administrativa, los conflictos se resolverían por el abandono de los derechos de la parte más débil, en beneficio de la parte dominante y la intimidad podría transformarse en un recurso en vías de extinción.[231]

362.3. Usualmente las funciones de las entidades organizadas para la protección de datos personales contenidos en archivos o bancos de datos, son de tres tipos: *a)* Finalidades de orientación y creación normativa; *b)* Finalidades administrativas destinadas a promover y difundir la problemática de los datos personales; y *c)* Finalidades económicas que persiguen lograr fuentes de rentabilidad para el Estado.

La *orientación al usuario* y/o consumidor se relaciona con las actividades de protección integral a los datos personales y al deber de garantizar la defensa del honor y la intimidad de los afectados por el tratamiento de información que les concierne, que ha sido archivada con finalidades contrarias a la ley en ficheros de titularidad pública y/o privada.

La *creación normativa* está reglamentada en varios lugares (*v. gr.:* sesenta (60) días para dictar su propio Estatuto; treinta (30) días para presentar la estructura administrativa; ciento ochenta (180) días para proceder al censo y registro, etc.). La denominada cooperación normativa no elude la posibilidad de modificar el cuerpo legal establecido, con el fin de mejorarlo o proponer nuevas alternativas tendientes a su mejor aplicación.

Las *finalidades administrativas de fomento a la protección de datos personales* se revelan en la acción de aliento para la *elaboración de códigos de conducta* (art. 30 reglamentario de la ley argentina.); *en el diseño de los instrumentos adecuados para la efectiva defensa de los principios legales implementados* (art. 29.5, ley 25.326); *en las condiciones y procedimientos para la aplicación de las sanciones administrativas* que correspondan por violar los principios de la ley (art. 31.2 de la ley citada), etc.

Finalmente, la *fuente de recursos económicos* de significado comprensible e importante.

---

[231] GILS CARBÓ, ob. cit., p. 177.

363. Responsabilidades derivadas del deber de información

363.1. El trabajo sobre datos personales no puede ser desconocido para los afectados ni para la sociedad en general. Aun sin exigir difusión publicitaria masiva, es necesario que el banco de datos haga pública su actividad proclamando así el derecho a la información que todos merecen.

Sin la proclamación del principio de publicidad de los derechos de los ciudadanos se resentirían y padecerían una grave quiebra en su efectividad y satisfacción, ya que la actuación de la persona y su defensa frente a los posibles abusos pasan por el conocimiento veraz de las circunstancias relativas no sólo a la obtención y tratamiento de los datos, sino también de las que se refieren a los ficheros, sus titulares y las finalidades de aquéllos; informaciones precisas para que el interesado pueda contrastar y evaluar la incidencia y alcance que en sus derechos y libertades fundamentales va a tener el tratamiento automatizado de datos personales.

Esta obligación de publicidad, a veces, se consagra como "*principio de transparencia*", debiendo el archivo informar, además de los datos identificatorios de sus actividades, el sistema y los procedimientos que aplicará para el tratamiento de datos personales.

363.2. La publicidad se convierte en notificación expresa, como "deber de información individual", cuando se vayan a solicitar a la persona datos que puedan ser objeto de posteriores procesos.

La obligación se cumple con el pedido de colaboración expreso, dando noticias suficientes e inequívocas sobre los motivos para los cuales se requieren los datos personales, sin ocultar la finalidad y destino que a ellos se aplicarán.

En *España*, la ley se preocupa en afirmar el objeto de la información que debe darse al individuo, comenzando por la indicación sobre si es o no obligatoria su respuesta, las consecuencias de la obtención de datos y, en su caso, los inconvenientes que tendría por el silencio dispuesto. También, deberán darse a conocer los derechos de acceso, rectificación y supresión, así como la identidad y dirección del responsable del archivo.

En *México*, el aviso de privacidad está regulado en los artículos 16 y 17 estableciendo requisitos mínimos y la obligación de ponerlo a disposición de los titulares, a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, respectivamente. El artículo 18 prevé que cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el cambio en el aviso de privacidad, exceptuándose de este supuesto, cuando el tratamiento sea con fines históricos, estadísticos o científicos. El párrafo tercero de la norma dispone que cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados, en consideración al número de titulares, o a la antigüedad de los datos, previa autorización del IFAIPD, el responsable podrá instrumentar medidas compensatorias.

En Argentina, se establece en el artículo 6º:

> Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: *a)* La finalidad para la que serán tratados y quienes pueden ser sus destinatarios o clase de destinatarios; *b)* La existencia del archivo, registro o banco de datos, electrónico o de cualquier tipo de que se trate y la identidad y domicilio de su responsable; *c)* El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; *d)* Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; *e)* La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

363.3. Cuando los datos se requieran a través de encuestas, cuestionarios preimpresos, opinión casual requerida, cupones de sorteo, y otras modalidades que especifican el destino para el cual los datos se aportan, la información suficiente ha de estar en la misma propuesta.

Sin embargo, el desvío de los datos hacia otras fuentes, o bien para darles un tratamiento diferente, hace responsable directamente a quien los solicita y archiva, por haber violado el deber de confidencialidad naturalmente contenido al tiempo de la voluntaria prestación.

En síntesis, las obligaciones emergentes del derecho a la información son esencialmente dos: la primera pone énfasis en el deber del archivo de dar a conocer sus actividades y responsables; la segunda, consiste en notificar expresamente a la persona concernida sobre las razones y destinos que se hará con sus datos personales, a los fines de que éste otorgue o no su expreso consentimiento.

Para Estadella Yuste el titular del fichero está obligado a:

> *a)* que la recolección y operaciones automatizadas se hagan de conformidad con finalidades legítimas y aceptadas socialmente; *b)* que se respeten las limitaciones cuantitativas y temporales en la recolección y almacenamiento de datos; *c)* que se observen los requisitos de la calidad de la información personal; *d)* que se especifiquen los propósitos para los cuales se crea el fichero; *e)* que se adopten medidas de seguridad necesarias que protejan los intereses y derechos de las personas respecto de los datos personales que les afecten. La segunda clase de obligaciones tiene un carácter más específico, procedente de los derechos individuales reconocidos a los afectados, y relacionados con las disposiciones legales nacionales sobre protección de datos. El titular del fichero debe: *a)* informar al afectado sobre los datos que son objeto de registro, de la finalidad del archivo, de la identidad del titular y su localización; *b)* comunicar el contenido de los datos que son objeto procesamiento automático, de almacenamiento, o de transmisión internacional, mediante una copia o fotocopia de los datos; *c)* rectificar, cancelar, borrar o bloquear los datos que a instancia de la persona concernida son inexactos o no se ajustan a las disposiciones normativas sobre protección de datos; *d)* cumplir los requisitos sobre inscripción de ficheros, notificar a la autoridad nacional sobre un cambio de domicilio o de titular de fichero, solicitar la licencia para la transmisión internacional de datos, en los casos que proceda según las disposiciones nacionales; *e)* garantizar que en las transmisiones internacionales de datos no se intente violentar los principios básicos de protección y que

el destinatario de ellos, utilizará los datos personales transmisitos en forma adecuada; *f)* solicitar permiso a la autoridad nacional para el cambio de finalidad de ficheros; *g)* adoptar códigos de conducta interno que sean fiel reflejo de los principios básicos de protección de datos.[232]

364. Responsabilidades derivadas de la violación de la seguridad

364.1. Esta es una obligación para el archivo y un principio de legalidad para sus actos. Las medidas de seguridad que todo archivo debe tener, es un deber inexcusable que no debieran requerir de leyes o directivas "marco", toda vez que se trata de justificar con plenitud la custodia del valor más importante que registran: los datos personales. Sin embargo, es reconfortante ver la manera como se ocupan los países para encontrar niveles de protección equiparables a los que pueden adoptar lugares donde la contaminación informática es arrolladora.

Claro está que las diferencias han de ser atendibles, pero nunca la obligación de asegurar, sin burocracias, los procedimientos que garanticen el acceso, y con ello, el secreto y la confidencialidad del registro.

364.2. La seguridad no solo quiere la atención sobre la seguridad *técnica* (*v. gr.:* para impedir la filtración, intrusión, destrucción, etc. de la base de datos) y *personal* (*v. gr.:* obligando al personal que trabaje con los datos a suscribir un compromiso de confidencialidad), sino también provocar la confianza de las personas físicas y jurídicas, con la esperanza de fomentar el uso de estas herramientas de la informática que provocan un sistema de negociación y comercio distinto y de gran desarrollo.

El 26 de noviembre de 1992, el Consejo de la Organización para la Cooperación y el Desarrollo Económico (OCDE) adoptó una importante Recomendación relativa a las Líneas directrices para la Seguridad de los Sistemas de Información. En ella, el Consejo recomienda a los países miembros: Establecer medidas, prácticas y procedimientos que traduzcan los principios relativos a la seguridad de los sistemas de información enunciados en las Líneas directrices que figuran en el Anexo a la presente Recomendación y de la que forman parte integral; procurar que la puesta en práctica de las Líneas directrices sea acompañada de consultas, de coordinación y cooperación, y especialmente de colaboración internacional, con vistas a la elaboración de normas, medidas, prácticas y procedimientos compatibles para directrices; Dar una amplia difusión a los principios enunciados en las Líneas directrices; Reexaminar las Líneas directrices cada cinco años con vistas a mejorar la cooperación internacional en cuestiones relativas a la seguridad de los sistemas de información.

364.3. La recomendación anotada propone trabajar sobre principios especiales para la seguridad, provocando responsabilidades cuando ellas se violentan.

El *principio general de responsabilidad*, supone que las atribuciones y encargos de los propietarios, suministradores y utilizadores de sistemas de información y demás agentes afectados debieran explicitarse.

---

[232] ESTADELLA YUSTE, ob. cit., p. 236.

El *principio de sensibilización* promueve suscitar la confianza con respecto a los sistemas de información, con el fin de que los propietarios, suministradores y utilizadores de sistemas de información y demás agentes posean un conocimiento apropiado e informado suficientemente sobre medidas, prácticas y procedimientos que afectan a la seguridad de los sistemas de información. Todo ello, de manera sencilla y compatible con el mantenimiento de la seguridad.

El llamado *principio de ética*, persigue que los sistemas de información suministren y apliquen reglas de comportamiento para que la seguridad puesta en práctica respete los derechos e intereses legítimos de terceros.

El *principio de pluridisciplinariedad* es otro de los creados, y se fundamenta en decir que las medidas, prácticas y procedimientos dirigidos a la seguridad de los sistemas de información deberían tener en cuenta y atender todas las consideraciones y todos los puntos de vista oportunos, ya sean técnicos o administrativos, que afecten a la organización, la explotación, el comercio, la educación o el derecho.

El *principio de proporcionalidad* se relaciona con los niveles, costes, medidas, prácticas y procedimientos de seguridad que deberían ser apropiados y proporcionados al valor y al grado de dependencia respecto de los sistemas de información, así como a la gravedad, a la probabilidad y a la amplitud de los eventuales perjuicios, teniendo en cuenta que las necesidades en materia de seguridad varían según los sistemas de información.

Luego el *principio de integración* quiere que la seguridad de los sistemas de información esté coordinada y armonizada entre sí y con las demás medidas, prácticas y procedimientos de la organización, de modo que se cree un dispositivo de seguridad coherente.

El *principio de oportunidad* pretende que los agentes públicos y privados, tanto en el plano nacional como en el internacional, actúen en el momento oportuno de manera coordinada con el fin de impedir los ataques a la seguridad de los sistemas de información.

El *principio de reevaluación* se razona sobre la seguridad de los sistemas de información y el análisis periódico que debe gozar, dado que los sistemas de información y las exigencias en materia de seguridad varían a lo largo del tiempo.

En todos ellos priva el denominado *principio de democracia*, por el cual la seguridad de los sistemas de información ha de ser compatible con la utilización y la circulación legítima de los datos y las informaciones en una sociedad libre.

364.4. Las consecuencias de violar el principio de seguridad se pueden dar cuando se viola, intencionalmente o no, la confiabilidad técnica del archivo, registro, base o banco de datos personales, y se altera la confidencialidad y secreto de los datos personales archivados.

También cuando los datos se desvían, en el sentido de estar cedidos a personas no autorizadas, sin interesar el destino que ellas le asignen. De darse este supuesto, tanto el usuario como el titular y el responsable del fichero están alcanzados por el deber de reparación y son solidariamente responsables con el cesionario.

La adulteración de datos tiene consecuencias penales, de modo que se reprime la inserción de datos falsos en un archivo, sin importar la finalidad que porte esa acción. Ello así porqué de atender el móvil debiera perseguirse el daño al tercero, mientras que la ley castiga a quien provoca la ilegalidad de la base de datos al crearle un sistema de información que no son ciertos.

Asimismo quien consulta datos sin consentimiento o autorización del titular, comete la acción de penetrar una base de datos confidenciales y privados que se castiga por la inmiscusión clandestina.

364.5. Cuando hay tratamiento prohibido, o no autorizado también hay responsabilidad, de manera que si el acto de procesar datos resulta efectuado por un archivo, registro, base o banco de datos registrado, la autoridad de control podrá actuar en el ámbito de sus competencias específicas; mientras que si se trata de otros ficheros, la responsabilidad civil y penal deberá ser determinada por el juez competente, previa denuncia.

Finalmente, es responsable quien guarda datos destinados a ser informados, en archivos inseguros. Pero ¿qué ocurre si, a pesar de la prohibición, se archivan datos personales en ficheros poco confiables?, ¿qué sucede si este tratamiento de información fue autorizado expresamente por el afectado? ¿cuáles son las consecuencias?

Hay que recordar que la obligación de seguridad pesa sobre el responsable y/o el usuario del archivo, de modo tal que será este quien ha de responder en casos donde se manifieste y pruebe la violación al principio.

Sin embargo, si el titular de los datos, debidamente informado, inclusive en los aspectos técnicos de la base de datos, consiente el almacenamiento y la cesión a sabiendas de la poca confiabilidad que el archivo merece, la cuestión cambia de tornas, porqué nadie podrá cuestionar aquello que con sus propios actos provoca. Esto es: si pretende hacer responsable al titular o usuario del archivo, registro o banco de datos por cualquiera de las afectaciones previstas en la ley (adulteración, pérdida, consulta o tratamiento no autorizado, desvíos de información, confidencialidad vulnerada, filtración de la base de datos), no tendrá más derechos que los de poner en conocimiento de la autoridad de control a los fines de la vigilancia que éste organismo debe cumplir en la preservación del principio de seguridad; mientras que el tema de la responsabilidad emergente quedará para la interpretación judicial.

365. Obligaciones propias del archivo

365.1. Observamos en el *principio de corrección* el deber de los archivos de mantener actualizada la información contenida; obligación que se mantiene entre los acciones que deben implementarse en esta parte, con la diferencia que ahora hay que especificar la forma como se cumple.

La exactitud de la información depende del modelo que genera la tarea de acopio y los sistemas de procesamiento de datos. Implica la necesidad de auditorías permanentes sobre los mecanismos y la facilidad que se ha de otorgar al afectado para que, a través de su propia disposición, coopere con la actualización correspondiente.

365.2. De igual manera, la finalidad del archivo se relaciona y proyecta entre las obligaciones a ejecutar, porqué una vez que el informe ha cumplido la razón de su almacenamiento, debe eliminarse sin necesidad que el interesado (afectado) lo peticione. Si este lo planteara obraría dentro de la garantía constitucional de *habeas data*. La supresión de oficio del dato caduco es una obligación emergente del deber de mantener actuales los archivos.

> Adviértase —dice Herrán Ortiz— la relatividad de esta obligación en tanto que se permite la conservación de los datos cuando se realizan operaciones de disociación de los datos respecto a su titular. Pugna con la idea misma del respeto a la finalidad la conservación de los datos personales cuando su utilización responde a fines diferentes, o incluso incompatibles con el que motivó su obtención; y en nada desmerece a dicha observación, el hecho de que el legislador español haya previsto la disociación de los datos respecto del titular, ya que ninguna garantía ofrece esta obligación a la vista de los avances que la tecnología proporciona a quienes de ella se benefician.[233]

La cancelación de datos puede tener otras variables que se actúan por decisión del afectado, mientras que la obligación establecida en este campo se refiere solamente al dato que ha perdido la causa para su archivo.

365.3 En la ley Argentina también se tuvo en cuenta el problema de la falsificación de los datos. En el artículo 32 (Sanciones penales) se prevé la incorporación al Código Penal de una norma (art. 117 bis) por la que se establece que:

> 1º) Será reprimido con la pena de prisión de un mes a dos años el que insertare o hiciere insertar a sabiendas datos falsos en un archivo de datos personales; 2º) La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales; 3º) La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona; 4º) Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo de la condena.

El sistema tiene prevista una escala de ilicitudes: La primera es la simple modificación del dato personal insertando información inexacta que vulnera el perfil almacenado aportando con ello una imagen distorsionada de la persona. Si ello provoca al afectado un daño, la escala penal punitiva aumenta, y cuando el agregado fuere hecho por funcionario público en ejercicio de sus funciones (por ejemplo, el Director o Responsable del Banco de Datos) se aplica la accesoria de inhabilitación para el desempeño de cargos públicos por el doble tiempo de la condena que se fije.

366. La reparación del daño

366.1. La reparación por uso ilegítimo, abusivo o arbitrario del dato personal no tiene un régimen diferente al que establecen las normas sustanciales. El *daño* se debe alegar y probar, para obtener el derecho a la indemnización. Sin embargo, la novedad

---

[233] HERRÁN ORTIZ, ob. cit., p. 189.

está en que la ley argentina "presume el perjuicio sufrido", encadenando la culpa de manera directa e inmediata.

En efecto, dice el art. 46:

> En los supuestos en que se demande judicialmente el resarcimiento de los daños ocasionados, la existencia de perjuicio se presumirá siempre que se acredite la violación o intromisión ilegítima en los derechos reconocidos por esta ley. La indemnización se extenderá al daño moral que se valorará atendiendo a las circunstancias del caso y a la gravedad de la lesión efectivamente producida. La condena podrá incluir la difusión y/o publicación de la sentencia por los medios que resulten necesarios para la adecuada compensación del perjuicio causado. La indemnización nunca será inferior a $ 5.000.

366.2. La obligación económica que tratamos no se vincula con la condena hipotética que surge de una sentencia judicial, sino con un derecho autónomo que nace de la misma ley reglamentaria de tratamiento de datos.

La ley española dice en el:

> ART. 18.—*"Tutela de los derechos"*. 1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine. 2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación. 3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses. 4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.
>
> ART. 19.—"Derecho a indemnización". 1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.
>
> 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

366.3. La penalidad actúa como sanción a las infracciones que puedan ocurrir sobre las reglas, principios y derechos que se establecen en la Constitución y por vía reglamentaria.

En particular, se considera que incurren en falta los archivos que no realizan los registros en forma estricta, o no informan con fehaciencia y certeza a la persona; o desplazan hacia el futuro los procedimientos de seguridad, o sean éstos insuficientes o irregulares; o violan el secreto y confidencialidad de los datos que no están autorizados a divulgar, ceder o transmitir a terceros.

Sin perjuicio de las acciones que cupieren al particular, el órgano de control hará responsable al archivo en cualquiera de las infracciones advertidas, y lo obligará a cumplir con penalidades distintas (*Cfr*. art. 31 de la ley argentina).

366.4. Finalmente, la obligación económica que determina el resarcimiento que cuenta como derecho el afectado, en nuestro parecer, no necesita daño efectivamente sufrido, debiendo el interesado demostrar únicamente el incumplimiento del banco de datos con las reglas y principios que preservan la tutela de la intimidad.

¿Es este un sistema de responsabilidad objetiva? Se pregunta Herrán Ortiz:

> […] no parece que pueda decirse tanto; en otras palabras, cierto es que el responsable del fichero representa una figura jurídica en la Lortad a quien se imponen las consecuencias del incumplimiento de las normas; pero también es verdad que esta circunstancia en ocasiones se ve alterada en determinados supuestos. En efecto, cuando el incumplimiento en las obligaciones procede de un defectuoso cuidado en el sistema de seguridad, cuando el responsable del fichero no haya empleado la diligencia exigible a su condición y cualidad profesional para evitar los perjuicios y así se demuestre, ninguna responsabilidad podrá exigírsele, si bien se le impone la carga de la prueba. Bien es verdad que en los demás supuestos, tales como la obtención indebida de datos personales, tratamiento ilícito y cesión de los datos, impedimento al ejercicio de los derechos de las personas, o incumplimiento de las obligaciones en relación con la actualización, rectificación o cancelación, la responsabilidad se exige al responsable del fichero, y sólo a él, sea o no quien realizó la actuación infractora, aunque nada excluye que luego éste repita contra quien materialmente causó el perjuicio.[234]

[234] HERRÁN ORTIZ, ob. cit., p. 266.

Sección 9ª Derechos de los titulares de archivos y de las personas concernidas en ellos

367. Derechos del archivo

367.1. Los derechos de los titulares o administradores del archivo se reflejan en distintas exigencias que pueden requerir para el cumplimiento de la finalidad que persiguen.

Es decir, son derechos que reposan en la eficacia que se busca conseguir para los archivos, registros o bancos de datos, y en particular, versan sobre el acceso a la información que almacenan, y la colaboración que pueden exhortar a quienes consulten; también, en la etapa de tratamiento, propiamente dicho, donde han de resolver algunos problemas derivados de la exclusión de datos registrables; y en el ciclo de cesión o transferencia, que presenta un marco un tanto difuso frente a la ausencia de normas que consideren el tratamiento de los datos personales.

En suma, son los derechos emergentes de las tres etapas: recolección, tratamiento y cesión de los datos personales.

367.2. El *derecho a conocer los datos personales* se posiciona en primera línea. La finalidad del archivo se cumple si la base informativa lograda es autosuficiente y precisa. Para ello, es menester legitimar la búsqueda y tratamiento de los datos a partir del reconocimiento legal que las leyes prometen.

Esto supone que la actividad pueda ser ejercida con libertad, aceptando las restricciones emergentes de los principios, particularmente respecto a la pertinencia y proporcionalidad de la información colectada.

En *España* se denomina esta potestad como "*derecho a la información*", lo que parece confuso frente al derecho de la sociedad que tiene el mismo nominativo. Preferimos aceptar un derecho a conocer los datos y establecer alguna distancia según la información se tome directamente de la persona, o a través de mecanismos indirectos que obliguen a dar mayor seguridad a la tutela del derecho a la intimidad.

Dice Puccinelli que:

> los especialistas en derecho informático sostienen que la mayor parte de los datos son vacantes y, por tanto, accesibles a todos, en un Estado de derecho en el cual se reconoce el pluralismo de la información y la libre investigación científica. Estiman, asimismo, que el derecho a la información permitiría recolectar los datos vacantes (o públicos) para crear

> libremente el bien "información" e incluso, cuando se tratara de información privada, daría derecho a obtener el acceso libre e igual a tal información desde que ella fuese hecha pública.[235]

Actualmente existe este temperamento por el cual se acepta el derecho a que la información personal se confiera voluntariamente o se exija por los medios legales especialmente previstos al efecto.

367.3. La jurisprudencia argentina ha dicho que el derecho a exigir la confidencialidad de los datos no se extiende a aquella información de alcance comercial o financiero, pues la misma, por su carácter, está destinada a divulgarse entre todas las entidades financieras del país tal como lo prevé la Circular OPASI 2 del Banco Central.

Por eso están fuera de la exigencia del consentimiento, los datos que revistan estas características. La ley 25.326 dice en el art. 5 inciso 2º que:

> No será necesario el consentimiento cuando: *a)* Los datos se obtengan de fuentes de acceso público irrestricto; *b)* se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; *c)* se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; *d)* deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; *e)* se trate de datos que tengan fines estadísticos a los que se les hubiera aplicado una operación de disociación; *f)* se trate de información proveniente de operaciones comerciales o financieras que realicen los socios de asociaciones empresarias de informaciones comerciales, sin fines de lucro, con la condición de que esa información se utilice exclusivamente entre los socios de tales asociaciones.

En cambio, diríamos que otros datos no pueden lograrse ni exigirse si no es manifestado libremente por el interesado, tal como ocurre con los datos sensibles, o cuando se pretende la información a través de medidas cautelares, de hecho improcedentes.

Por eso se afirma que [...] "no es procedente la acción de *habeas data* para tomar conocimiento de los datos insertos en una historia clínica mediante la obtención de una fotocopia de la misma ante la negativa del sanatorio que la conserva en su poder".[236]

367.4. Otro de los derechos que tiene quien registra en archivos datos personales es el *tratamiento* de ellos, propiamente dicho.

La tarea de procesar información no es sencilla y como tal se debe especificar. Así lo han hecho buena parte de las leyes de tratamiento de datos cuando afirman que esta labor comprende las operaciones efectuadas, en todo o en parte, con ayuda de medios automatizados que facilitan la búsqueda, localización y depósito, a los

---

[235] PUCCINELLI, *El Habeas Data en Indoiberoamérica*, en "El Amparo Constitucional, perspectivas y modalidades", cit., p. 228.

[236] CNCiv., Sala C, 1995/07/06, El Derecho 165-255.

que se aplican operaciones lógicas o aritméticas, o de ambas en su caso, para interconectar información, modificar, borrar, recuperar y difundir a terceros el fruto generado.

El artículo 2 de la ley Argentina, define al tratamiento de datos, como aquellas operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

367.5. El tratamiento ocupa varias secuencias, o en otros términos, se compone de etapas que se reconocen inescindibles a los fines previstos para la creación del archivo.

A partir del banco de datos que se origina (compuesto básicamente de una red central de proceso, un ordenador con su teclado y pantalla, los soportes o memorias donde se registran los datos, el sistema operativo, los programas de aplicación, un módem de comunicaciones y otros periféricos adicionales), comienza una tarea bastante compleja para almacenar información de todo tipo y procesarla para los fines previstos en la creación de la base.

Cuando esa información sea personal, el derecho que tiene reconocido el archivo para colectarla, se encuentra limitado porqué existen datos que no pueden registrarse por diversas situaciones (Por ejemplo, sensibilidad de la información; seguridad militar; secreto de Estado o profesional; etc.).

De igual modo, la colección de datos puede servir para elaborar perfiles o preferencias de alguien, pero ello no somete al individuo, quien tiene derecho a su propia realidad.

367.6. Una vez que se realiza el tratamiento, comienza la etapa de transferencia de datos que tiene, en los hechos, la mayor importancia porque refleja las razones por las que el archivo se creó. Pueden ser beneficios científicos, culturales o económicos, pero en cada uno, el derecho a dar a conocer a otros el producto del tratamiento de datos está implícito en el reconocimiento original.

No interesa si la información se vende, cede o intercambia a un particular o se difunde públicamente, el principio es la libertad de transferencia, con algunas restricciones más estrictas que las observadas al tiempo de la registración.

> En tren de analizar las excepciones —agrega Puccinelli— a la regla del libre expendio, debemos remitirnos: *a)* a toda aquella información que está prohibido almacenar (*v. gr.:* conducta sexual; *b)* a aquélla registrable pero que sólo puede ser utilizada por determinados sujetos habilitados para ello (*v. gr.:* el juez penal que investiga una estafa), y *c)* a aquella que, en principio, no debiera ser proporcionada (*v. gr.:* listado de enfermos de SIDA remitidos a los fines estadísticos).[237]

---

[237] PUCCINELLI, "El *Habeas Data* en Indoiberoamérica", en *El Amparo Constitucional, perspectivas y modalidades*, cit., p. 229.

El derecho tiene base constitucional, en la garantía de ejercer toda actividad lícita, de modo que si tiene el archivo autorización para funcionar, debidamente conferida, no pueden encontrarse más obstáculos que los legalmente establecidos, para la cesión de datos a terceros.

368. Los códigos éticos

368.1. La necesidad de principios deontológicos establecidos en un código tipo, es una necesidad inevitable en el uso por otros de datos personales. La inmiscusión en la intimidad es inevitable desde múltiples formas y variadas expresiones. Se convive con la tecnología, la hemos aceptado, y casi sin darnos cuenta, nos sometimos a ella perdiendo individualidad.

La proliferación de bancos de datos, multiplicados al infinito desde la aparición de Internet, moviliza cotidianamente datos personales que se registran y procesan para un sin fin de razones.

Por ello, surge este anhelo internacional de contar con normas éticas que guían las conductas de los usuarios y titulares de los archivos.

De ello se ocupa el artículo 30 de la ley 25.326 de Argentina:

> 1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.
>
> 2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

368.2. En particular, se ha continuado la consigna emitida en Europa por la Directiva 95/46 CE, que dice, en el art. 27 que:

> 1) Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva; 2) Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales. Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes; 3) Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el

Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo.

369. Derechos del titular de los datos

369.1. ¿Quién es el titular de los datos? La protección que a la intimidad se confiere, en miras a evitar que la intromisión informática complique la vida privada de las personas, supone pensar que estamos frente a un derecho personalísimo que solamente le corresponde al individuo afectado por el almacenamiento, conservación y transferencia de sus datos personales.

No es simple ocultar la facilidad como se pueden interceptar los datos en la red, ni eludir los desvíos que ellos pueden sufrir en su tránsito para ser leídos por personas no autorizadas. Por eso, interrogarse quien es el dueño de la información tiene su sentido, mucho más si quedan señalados los problemas de la seguridad en Internet, que podrían sintetizarse básicamente en dos sub categorías de conflictos:

1. los referidos a los riesgos a los que se ve expuesto un servidor Web, como por ejemplo, la exposición de documentos a terceras personas.

2. Los que se vinculan con la protección de las comunicaciones de los usuarios, ante el riesgo de la interrupción y captura de datos personales (información crítica) como tarjetas de crédito, cuentas bancarias, etc.

369.2. De este modo, se tomaría a la noción de derecho subjetivo como base de la acción y, ante una hipotética demanda, habría que demostrar la relación existente entre la titularidad de quien propone la pretensión, con el perjuicio efectivamente sufrido. Asimismo, se tendría que verificar la relación causal y el derecho a las medidas que solicita.

Sin embargo, la explicación que precede no es absolutamente cierta. En efecto, la titularidad de los datos contrae algunas dificultades de intelección, porqué una cuestión son los derechos que tiene la persona afectada por el tratamiento de sus datos personales, y otra es la legitimación procesal que se debe acreditar en el proceso constitucional de *habeas data*.

Inclusive, hay quienes sostienen que una vez que los datos llegan y se incorporan a la base ocurre una suerte de legítima apropiación que le asigna la titularidad sobre ellas al responsable del archivo. La idea se basa en que existe un derecho a la información diferente al de titularidad sobre los datos.

Dado que alguna doctrina sostiene que podría ser ejercido una suerte de derecho de propiedad sobre los datos —dice Puccinelli—, cabría entonces distinguir entre el derecho a la información y el derecho sobre la información recabada. La posición que recurre al concepto de propiedad sobre los datos plantea ciertos debates nada pacíficos en la doctrina entre quienes sostienen la propiedad colectiva de toda información con independencia de su fuente y aquellos que, por el contrario, entienden que en los supuestos en que a partir de determinados datos y por el obrar de alguien, se logra generar determinada informa-

ción, a quien la generó se le debe reconocer su derecho de propiedad sobre ella, salvo en el caso de los datos personales, que pertenecerían a aquel a quien se refieren.[238]

369.3. El siguiente paso para reconocer la pertenencia del derecho a la denominada "autodeterminación informativa", consiste en tomar los derechos que se tutelan por esta novedosa posición y advertir el alcance que ellos tienen.

Estadella Yuste dice que la noción de datos puede conducir a falsas apariencias respecto de su contenido, ya que no va destinada a proteger los datos *per se*, sino a una parte del derecho a la intimidad individual.[239]

De este modo, se podrá constatar que la protección dispensada no es estrictamente a los datos sino a la persona, y particularmente, a su vida privada e intimidad.

Luego, cada etapa del proceso que va desde la localización de las fuentes de información hasta la transferencia de los datos, instala exigencias diferentes que tienen mucho que ver con las propias decisiones o autodeterminación (manifestación de voluntad del interesado) impuesta por quien ofrece información personal a un archivo.

La guarda de los datos, por ejemplo, es sin duda alguna responsabilidad del archivo; como lo es también la seguridad que aplica al secreto recibido y a la efectividad de las eventuales transferencias. Aquí, los datos son de alguien a quien se conoce, informa y ha prestado autorización; mientras que el acto pleno de la información ofrecida es del titular del archivo.

Son derechos distintos, es verdad, y deben tener consideraciones diferentes. Una cosa será la protección al dueño de los datos para evitar la ofensa o lesión a su intimidad y demás derechos vinculados (identidad, honor, reputación, etc.); y otras las garantías que debe contar el titular del archivo para poder ejercer con plenitud su derecho a la información, a comerciar lícitamente, etc.

369.4. Cuando se relaciona el derecho a tener protección de los datos personales con el derecho a la intimidad, se refleja una visión individual que asienta en un concepto civilista de la garantía. Pero cuando en la misma dimensión se cubren los derechos colectivos que persiguen evitar el abuso en el almacenamiento, recolección y procesamiento de datos personales, la intimidad queda en un segundo plano porqué el derecho garantizado adquiere alcance social.

> El Tribunal Constitucional alemán ha entendido que el principio liminar del ordenamiento jurídico establecido en su país, es el valor y la dignidad de la persona que actúa con libre autodeterminación al formar parte de una sociedad libre. De esa dignidad y libertad, entendida como libre autodeterminación, deriva la facultad de la persona de "deducir básicamente por sí misma cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida"; por lo que el Tribunal interpreta —en la deducción que hace Fappiano— que es contrario a esa facultad un orden social y un orden jurídico que hiciese posible al primero, en que el ciudadano ya no pudiera saber quién, qué, y cuándo y con

---

[238] PUCCINELLI, "El *Habeas Data* en Indoiberoamérica", en *El Amparo Constitucional, perspectivas y modalidades*, cit., p. 231.

[239] ESTADELLA YUSTE, ob. cit., p. 273.

> qué motivo sabe algo sobre él…Esto no solo menoscabaría las oportunidades del desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos.[240]

La dificultad de encuadrar como derecho subjetivo (propio e intransferible) a la noción de privacidad que pervive en el concepto de datos personales, está en que no se puede reparar el daño con la sola concesión de una indemnización reparatoria. La invasión a la intimidad se relaciona con las posibilidades reales que se tengan para controlarla, de manera que, los derechos emergentes de la protección de datos no pueden ser atendidos únicamente desde la visión economicista que mida el daño con la vara del resarcimiento. Es necesario que la protección del derecho se plantee como un problema social.

> La protección del derecho a la intimidad contra el uso de un tratamiento automatizado de datos personales no se plantea exclusivamente a consecuencia de problemas individuales, sino que también expresa conflictos que incluyen a todos los individuos de la comunidad internacional. Por eso —dice Estadella Yuste— la idea de que la persona titular de los datos –el afectado- tiene interés, como parte de un grupo, en controlar el tratamiento automatizado de datos es reciente, ya que no aparece así en la denominada "primera generación" de las leyes protectoras de datos, orientadas exclusivamente a la protección de la persona como entidad individual.[241]

369.5. La socialización del derecho puede ampliar las fronteras tradicionales de la legitimación procesal, y por eso es la diferencia entre derecho subjetivo y representación del interés a defender; es evidente que la afectación de la privacidad por cualquier medio, además de lo que pertenece a los datos en sí mismos, se puede exigir no sólo por el afectado, sino por otras personas que con iguales motivos persigan una decisión judicial al respecto.

No obstante, si la noción de autodeterminación informativa se restringe como derecho personalísimo, la defensa del honor, la imagen, o la intimidad en un amplio sentido, únicamente se podrá concretar por el afectado.

> El bien jurídico intimidad de ser tratado como un derecho exclusivamente individual puede dejar afuera del ámbito de defensa constitucional —al parecer de Perez Luño— los aspectos sociales y colectivos de las informaciones que directamente les afectan. De otro lado, dado que en la sociedad moderna la capacidad de actuación política se halla íntimamente relacionada con el acceso y control de la información, un equilibrio sociopolítico exige que se garantice a los grupos sociales formas de participación en los materiales archivados en los bancos de datos.[242]

---

[240] FAPPIANO, Oscar Luján, "*Habeas data*: Una aproximación a su problemática y a su posible solución normativa", en *"Liber Amicorum" Héctor Fix Zamudio*, volumen 1, Secretaría de la Corte Interamericana de Derechos Humanos, San José, Costa Rica, 1998.

[241] ESTADELLA YUSTE, ob. cit., p. 271.

[242] PÉREZ LUÑO, Antonio E., *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 1991 (4ª ed.), pp. 66 y ss.

369.6. La perspectiva anterior puede variar si el derecho se presenta desde los intereses que tutela. Es decir, si en lugar de ver a la persona que lleva la pretensión se observa el contenido del derecho que para sí reclama.

Esta cuestión es esencial en el análisis del *habeas data*, porqué la garantía constitucional se puede encontrar alterada por una caprichosa definición procesal que exija la relación directa entre quien pide y el daño producido (por ejemplo, cuando se requiere ilegalidad o ilegitimidad en el acto cuestionado y el actor únicamente solicita acceso al banco de datos); cuando en realidad, la lesión al derecho de la intimidad tiene varias manifestaciones, algunas de las cuales no reconoce un afectado directo porqué el gravamen asienta a toda la sociedad.

Muchas Constituciones del mundo han incorporado el derecho a la intimidad, el honor y la imagen como derechos del hombre; de este modo, se persigue establecer una igualdad de trato y consideración que evite diferencias escandalosas entre el significado que unos y otros puedan dar a cada uno de los intereses.

369.7. En relación estricta a los datos personales, debe aplicarse esta inteligencia porqué la intromisión a la vida privada se realiza en el preciso momento que alguien usa o conoce información personal que nos concierne, adquiriendo un conocimiento que pudo estar reservado, secreto o ser confidencial.

Esa información adquirida, cuando lo es de manera ilegítima, representa una injerencia en la vida privada, familiar o doméstica; constituye un atentado a la libertad individual cuando se usa para descalificar u ofender, o asignar conductas que lesionan el honor personal; asimismo, puede considerarse que es un hostigamiento, una vigilancia perturbadora, y en definitiva, una actitud hostil contra la reserva de los comportamientos individuales.

Cada caso es una proyección a defender, una hipótesis de cómo se afecta el derecho a través de la penetración y divulgación de los datos personales.

> Por tanto, tal como afirma Perez Luño, se trata en suma de comprobar en qué casos la *privacy* puede operar como coartada para burlar una política social avanzada, o en qué supuestos puede servir de freno ante determinadas formas de control o discriminación social o política. Pero en lo que interesa distinguir es que las cuestiones sobre las que gravita la disciplina jurídica de la intimidad han perdido su carácter exclusivo individual y privado, para asumir progresivamente una significación pública y colectiva. El problema del suministro de datos personales a la administración es evidente que atañe a los individuos, pero también a toda la sociedad, e incluso puede afirmarse que atañe a los individuos en cuanto pertenecen a un grupo social.[243]

Si no se considera dicho carácter social del derecho para centrar su tutela en la defensa exclusiva del derecho personalísimo, es evidente que se deja sin defensa a las personas jurídicas, porqué al referirse a las personas individuales se establece que el derecho a la protección de la intimidad y, en esencia, de los datos, corresponde a la persona humana; dejando en todo caso la tutela a la información de las empresas a la normativa específica que cada ordenamiento mantenga.

---

[243] PÉREZ LUÑO, ob. cit., p. 34.

369.8. La progresión del derecho a partir de la interpretación judicial y doctrinaria ha puesto de relieve el difícil encuadre que tiene el criterio tradicional entre derecho positivo y derecho natural. Dicho en otros términos, no siempre las cosas se presentan como polaridades entre el derecho subjetivo, individual y concreto, frente al derecho social, difuso y abstracto.

No es bueno creer que la mejor defensa parte de las garantías individuales que tenga una persona porqué desde ellas irradia la fuerza normativa hacia los demás; como tampoco lo es pensar que si la sociedad se defiende con las armas de la ley, no es posible creer en el hombre indefenso.

Una posición intermedia deja en la persona la disponibilidad de actuar con libertad y criterio, poniendo en claro que, en materia de protección de datos, nadie mejor que el afectado para promover, de acuerdo con sus propios sentimientos y convicciones, la defensa de su vida privada.

La posición se refleja en muchas de las legislaciones sobre protección de datos, las cuales ponen énfasis en la autonomía de la voluntad individual para autorizar la guarda, almacenamiento y transferencia de información que concierne a las personas físicas o jurídicas.

> Resumiendo se puede decir —concluye Estadella Yuste— que en un primer momento los instrumentos internacionales de derechos humanos no recogían expresamente el derecho a la protección de datos o autodeterminación informativa, sino tan sólo un derecho "a la vida privada" o a la intimidad personal. Posteriormente éste se ha ido desarrollando y paulatinamente se han adoptado otros instrumentos internacionales reconociendo el derecho a la protección de datos. Ello es importante porqué, si la protección de datos sólo se hubiera plasmado en leyes de ámbito nacional, habría sido más difícil que la comunidad internacional lo considerara como un derecho individual.[244]

369.9. La dificultad puede estar en las limitaciones que se pretendan derivar de ese acto voluntario como una proyección de la doctrina de los actos propios, que en nuestro parecer no puede ser tan inflexible porqué desnaturaliza el derecho central a proteger. De aplicar el temperamento cualquier autorización abriría una carta de crédito al archivo evitando el control externo si el afectado no efectúa una pretensión concreta.

La defensa de los datos no tiene una visión estática simplificada en el interés particular; todo lo contrario, la función dinámica que adquiere se toma del modo como actúan los archivos y registros de información personal, los que habilitan actuar en dimensiones diversas, ya sea para tutelar el interés concreto, como para descubrir el control externo que se merece.

> Esta posición ha penetrado en los últimos años en la doctrina europea y reviste una importancia prioritaria para delimitar conceptualmente el contenido del derecho a la intimidad y su alcance en la sociedad tecnológicamente avanzada. En suma, se trata de insistir —afirma Perez Luño— que en nuestra época resulta insuficiente concebir la inti-

---

[244] ESTADELLA YUSTE, ob. cit., p. 199.

midad como un derecho garantista (*status* negativo) de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla, al propio tiempo, como un derecho activo de control (*status* positivo) sobre el flujo de informaciones que afectan a cada sujeto.[245]

370. Las garantías procesales en la protección de datos

370.1. De lo que llevamos diciendo se puede deducir que la herramienta procesal destinada a proteger los datos personales es el *habeas data*. Su implementación depende del marco donde se encuentre, sea la Constitución, la ley o el desarrollo jurisprudencial de los procesos constitucionales.

Ahora bien, esa garantía tiene una finalidad específica; no se trata de resolver con ella un impedimento para negar información personal o suprimir aquella que estuviera registrada en un banco de datos; sino de permitir que sea el propio interesado quien decida el destino de esa información y su permanencia en la base creada.

A partir de esa libertad puede, siguiendo un orden lógico en las pretensiones, *perseguir el acceso* a la fuente de información que lo concierne; y después, una vez verificado el registro personal de sus datos, disponer el control sobre ellos, ya sea para mantenerlos actualizados, reemplazarlos con los que sean exactos y veraces, solicitar la confidencialidad estricta de la información privada, o bien, plantear la supresión por alguna de las razones que enseguida se verán.

370.2. *Derecho de información.* Hablamos aquí de un derecho distinto a la información que se le debe proporcionar al sujeto que admite incorporar sus datos a un archivo con el fin de darles un tratamiento automatizado. También difiere de aquél derecho a la exactitud que planteamos como garantías para el usuario.

El derecho a la información que se instala entre las garantías del *habeas data*, no piensa en el carácter individual sino en el alcance general que tiene "toda persona" para solicitar información sobre la existencia de bancos de datos, sus finalidades y la identidad de sus responsables.

La ley argentina establece en el artículo 13 (Derecho a la información) que: "Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o banco de datos personales, sus finalidades y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita".

Tal como se orienta en el derecho comparado esa idea de amplia circulación de los datos, el derecho a la información se presenta como una garantía de la publicidad de los actos que lleven a cabo los archivos.

En *Bolivia* basta con la mera sospecha de estar afectado para dar derecho a toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten

[245] PÉREZ LUÑO, ob. cit., p. 67.

su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de *habeas data* ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya.

En *Brasil* se concede para asegurar el conocimiento de informaciones relativas a la persona del solicitante contenidas en registros o bancos de datos, de entidades gubernamentales o de carácter público.

En *Chile*, la ley 19.628 dispone que toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen. En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos.

En *Colombia* la información personal recolectada o suministrada de conformidad con lo dispuesto en la ley a los operadores que haga parte del banco de datos que administra, podrá ser entregada de manera verbal, escrita, o puesta a disposición de las siguientes personas en los términos que la norma dispone.

En *Ecuador* también se afianza desde la Constitución el deber informativo al conceder a toda persona el 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.

En *Paraguay* la ley 1682 dice que toda persona podrá acceder a la información y a los datos que sobre sí misma, sobre su cónyuge, sobre personas que acredite se hallen bajo su tutela o curatela, o sobre sus bienes, obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial, así como conocer el uso que se haga de los mismos o su finalidad.

En *Uruguay*, la ley establece en el art. 13 el principio general que otorga derecho de información frente a la recolección de datos, los que se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca.

Finalmente en *México* recordemos el aviso de privacidad (art. 16) de la ley federal que establece el deber de informar, cuanto menos: La identidad y domicilio del responsable que los recaba; las finalidades del tratamiento de datos; las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos; los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición; y en su caso, las transferencias de datos que se efectúen, y el procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en la ley. En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

Quizás fuera mejor establecer como deber de los bancos de datos producir periódicamente un informe, antes que dejar en la iniciativa de las partes el control eventual de la transparencia en el tratamiento de datos personales. Así lo hacen algunas legislaciones (*v. gr.:* Portugal, Gran Bretaña, Suiza, Noruega, entre otros), donde se destaca la ley finlandesa que impone al responsable la elaboración de una lista de ficheros de personas que deben estar a disposición del público.

La finalidad del derecho a la información no consiste únicamente en saber quienes son los titulares ni cuantos bancos de datos existen; la garantía proyecta un control directo sobre el tratamiento que se efectúa sobre la información que a la persona le atribuyen. De este modo, cuando se pretenda deducir una calidad particular, una cualidad determinada, un perfil o personalidad de alguien, a partir de los datos que el archivo hubiere procesado, la conclusión será nula por estar ausente el derecho del afectado a conocer el informe que le concierne de manera tan directa.

Esta elaboración es común para ciertas decisiones judiciales o en algunos actos administrativos que adoptan un criterio a partir de la valoración lograda del tratamiento automatizado de datos personales; y se observa agudamente en los servicios informatizados de información crediticia que suelen elaborar un perfil de la persona a partir del cumplimiento de sus obligaciones patrimoniales.

> En Argentina país hubo un panorama similar desde la sanción de la reforma constitucional que trajo la garantía del *habeas data* pero acotada a la iniciativa de parte interesada. Ello no obsta a que se pueda exigir la transparencia de los archivos, sobre todo los de carácter público, que tienen una obligación inmediata con el ciudadano.
>
> Ahora bien, este derecho no debe confundirse con el derecho de acceso a la documentación administrativa; pese a que tiene una evidente vinculación con algunos derechos fundamentales como el derecho a la participación en los asuntos públicos, o el derecho a comunicar y recibir libremente información auténtica, o el más próximo que lo relaciona con el derecho a la tutela judicial efectiva. Sin perjuicio de esta vinculación, dice Peñarrubia Iza, el derecho de acceso a la documentación administrativa es un derecho constitucional, pero no un derecho fundamental, en cuanto no está ubicado sistemáticamente entre los derechos fundamentales. Para convertirse en un derecho subjetivo, basta con el reconocimiento expreso que hace la Constitución, si bien el mismo precepto que menciona este derecho se remite a las leyes, lo cual significa que hay un principio de reserva de ley para delimitar este derecho, es decir, que el modo concreto de ejercicio, la legitimación y cualesquiera otros aspectos, sobre todo en lo que respecta a los límites, han de ser establecidos legalmente.[246]

En síntesis, el derecho a la información es una garantía general para la publicidad de los actos de tratamientos de datos personales que efectúen los archivos. La regla mínima es difundir el nombre y los responsables de cada banco de datos, y las extensiones radican en las consecuencias que pueda tener la información aportada sin dicho conocimiento general.

370.3. El derecho de información se desgrana en garantías específicas que constituyen el corazón de la protección de datos. Son los derechos al acceso a las bases de datos para tomar conocimiento de los datos que obran registrados, y en su caso, para ejercitar otros derechos que se denominan de control, que consisten

---

[246] Peñarrubia Iza, Joaquín María, *El derecho de acceso a los archivos y a los documentos de la Administración Militar*, Cívitas, Madrid, 1999, pp. 69 y ss.

en requerir la actualización de la información inexacta; la rectificación de la que fuera errónea; pedir la supresión del dato caduco o solicitar la confidencialidad de cierta información.

Esta obligación de publicidad insiste en difundir la actividad vinculada al tratamiento de datos personales. Por eso, la ley 25.326 (Argentina) no sólo piensa en las personas (físicas y jurídicas) ofreciéndoles una herramienta directa de protección a sus datos y garantizando el derecho a la intimidad y el honor de las mismas, sino, además, diseña un sistema progresivo para el desarrollo de los sistemas informáticos, el comercio electrónico, la comunicación abierta por medios modernos de telecomunicaciones, la difusión de Internet y sus ventajas, y todos los mecanismos que laboran con información personal, necesaria e imperiosa para la efectividad de sus tareas, procurando *fomentar credibilidad y confianza, como una suerte de patentamiento a la seguridad de que los datos personales que ingresen en un sistema automatizado, no serán fuentes de abuso ni desnaturalización*.

370.4. Asimismo, el deber de información individual se cumple con el requerimiento de colaboración al titular de los datos, debiéndose comunicar inequívocamente los motivos para los que se piden datos personales, sin ocultar la finalidad y destino que a ellos se aplicarán.

En España, la ley se preocupa en afirmar el objeto de la información que debe darse al individuo, comenzando por la indicación sobre si es o no obligatoria su respuesta, las consecuencias de la obtención de datos y, en su caso, los inconvenientes que tendría por el silencio dispuesto. También, deberán darse a conocer los derechos de acceso, rectificación y supresión, así como la identidad y dirección del responsable del archivo.

Para Estadella Yuste el titular del fichero está obligado a:

> *a)* que la recolección y operaciones automatizadas se hagan de conformidad con finalidades legítimas y aceptadas socialmente; *b)* que se respeten las limitaciones cuantitativas y temporales en la recolección y almacenamiento de datos; *c)* que se observen los requisitos de la calidad de la información personal; *d)* que se especifiquen los propósitos para los cuales se crea el fichero; *e)* que se adopten medidas de seguridad necesarias que protejan los intereses y derechos de las personas respecto de los datos personales que les afecten. La segunda clase de obligaciones tiene un carácter más específico, procedente de los derechos individuales reconocidos a los afectados, y relacionados con las disposiciones legales nacionales sobre protección de datos. El titular del fichero debe: *a)* informar al afectado sobre los datos que son objeto de registro, de la finalidad del archivo, de la identidad del titular y su localización; *b)* comunicar el contenido de los datos que son objeto procesamiento automático, de almacenamiento, o de transmisión internacional, mediante una copia o fotocopia de los datos; *c)* rectificar, cancelar, borrar o bloquear los datos que a instancia de la persona concernida son inexactos o no se ajustan a las disposiciones normativas sobre protección de datos; *d)* cumplir los requisitos sobre inscripción de ficheros, notificar a la autoridad nacional sobre un cambio de domicilio o de titular de fichero, solicitar la licencia para la transmisión internacional de datos, en los casos que proceda según las disposiciones nacionales; *e)* garantizar que en las transmisiones internacionales de datos no se intente violentar los principios básicos de protección y que el

destinatario de ellos, utilizará los datos personales transmitidos en forma adecuada; *f)* solicitar permiso a la autoridad nacional para el cambio de finalidad de ficheros; *g)* adoptar códigos de conducta interno que sean fiel reflejo de los principios básicos de protección de datos.[247]

370.5. La información se debe prestar al tiempo de pedir los datos personales, de modo tal que la forma como ella se ofrezca, va a depender de la manera como se practique el requerimiento.

Sin embargo, esta obligación legal no se instala únicamente en el momento de la recolección, porque el tratamiento de datos —que es el objeto de tutela— comienza con el almacenamiento y continúa con las siguientes hasta la cesión local e internacional.

En este sentido, si un fichero no informó oportunamente deberá hacerlo antes de la cesión, como mínimo, pues de otro modo violaría las disposiciones legales.

Ahora bien, si el archivo público o privado que obtiene información personal está liberado de requerir el consentimiento *expreso* e *informado*, por encontrarse entre las situaciones legalmente exceptuadas (*v. gr.:* información crediticia; con fines de publicidad, o relativos a encuestas, según las legislaciones comparadas), el deber de información no los alcanza íntegramente, pero la ley no abandona a las personas en el juego de equilibrios, porque para cada caso determina posibilidades alternas que protegen los derechos de los posibles afectados.

370.6. La información a prestar no debe ser asociada al consentimiento como resultado. Con esto se quiere expresar que los archivos, registros, base o banco de datos, públicos o privados, que actualmente funcionen, y aquéllos que vayan a crearse con finalidades específicas, podrán suministrar la comunicación informada a las personas contenidas mediante cualquiera de los mecanismos fehacientes que se autoriza: por escrito, medios electrónicos, telefónicos, de imagen, u otros medios idóneos al fin que deben alcanzar.

El consentimiento es el medio a conseguir, pero no legitima la ausencia de información previa.

Las obligaciones mínimas de información, sin perjuicio de la forma como se debe hacer, son las siguientes:

a) Objeto y destinatarios: la finalidad del archivo debe coincidir con lo registrado, e informar al requerido para qué se quieren los datos (*v. gr.:* participación en un concurso), y a quienes se aportará esa información personal (destino), sin necesidad de que éstos sean individualizados, en la medida que se puede simplemente indicar la "clase" de destinatarios.

Hay supuestos que establecen la prohibición de almacenar cierta categoría de datos (por ejemplo, datos sensibles), aunque se autoriza a algunas entidades a proceder a la formación de archivos con una finalidad específica como es llevar el re-

[247] ESTADELLA YUSTE, ob. cit., p. 199.

gistro de sus miembros (iglesia católica, asociaciones religiosas, organizaciones políticas o sindicales). Queda en claro que, estas bases de datos tienen por única finalidad un control interno de administración, y no se pueden transferir a otros sin violar las disposiciones legales. Sin embargo, algún dato sensible (*v. gr.:* pertenencia gremial) se puede transferir a los fines de realizar una oferta de bienes y servicios, y siempre que ello no cause discriminación, y también hay datos compilados en archivos públicos de acceso irrestricto que se transfieren a organismos privados sin conocimiento del afectado y, obviamente, sin información posible sobre finalidades y destino.

370.7. Es preciso señalar al requerido si está obligado (por ley) o no a prestar sus datos personales, condición que únicamente está prevista para el caso de peticiones directas.

Señala Padilla que:

> las exigencias de esta cláusula solamente encuentran sentido cuando la recolección de datos debe hacerse de modo directo, persona a persona diríamos, a fin de resguardar la exigencia del consentimiento del interesado y para que éste conozca su situación jurídica ante la solicitud que se le pide llenar. No es aplicable, por ello, a datos obtenidos de archivos públicos y de otras fuentes. Sin embargo, ha de tenerse muy en cuenta que cuando los incisos c) y d) se refieren a "datos", obviamente no pueden ser aquellos que al siguiente precepto, en su inciso primero, califica como "sensibles".[248]

Este dilema sobre el *carácter obligatorio o facultativo* en la aportación de la información personal que se solicita, y en especial, cuando se trata de datos sensibles, lleva a cuestionar la polaridad manifiesta que expresa. A veces, una encuesta puede ser de respuesta obligatoria (por ejemplo, el Censo Poblacional), otras meramente facultativa (*v. gr.:* encuesta de opinión), y la consecuencia de no reportar en una u otra quedar librada a la apreciación judicial.

Por ejemplo, si en el primer caso alguien se ve obligado a responder por imperio de las normas, hay que recordar que el derecho a la autodeterminación informativa nace, precisamente, de un fallo del Tribunal Constitucional alemán que consideró violatorio de la intimidad personal el tener que responder a un cuestionario que revelaba facetas de la personalidad privativas del derecho a tener una vida privada.

> El Tribunal señaló que el principio básico del ordenamiento jurídico establecido por la Ley Fundamental es el valor y la dignidad de la persona que actúa con libre autodeterminación al formar parte de una sociedad libre. De la dignidad y libertad, entendida como libre autodeterminación deriva la facultad de la persona de decidir básicamente por sí misma cuando y dentro de qué límites procede revelar situaciones referentes a su vida privada. Por ello el tribunal entendió —según palabras de Bergel— que sería contrario a dicha facultad de autodeterminación un orden social y un orden jurídico que hiciese posible al primero, que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué

---

[248] PADILLA, Miguel M., *Bancos de datos y acción de habeas data*, Abeledo Perrot, Buenos Aires, 2001, p. 65.

> motivo se sabe algo sobre él...esto no sólo menoscabaría las oportunidades de desarrollo de la persona individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos.

En otras, si se revelan datos sensibles ante un interrogatorio informal, las consecuencias del uso ilegítimo de esa información, voluntariamente aportada, quedará librada a la apreciación judicial (en cuanto a la tipicidad que cabe acordar al ilícito).

370.8. Otra faceta de la información a proporcionar son las consecuencias, donde se encuentran tres posibilidades: a) *cuando los datos se facilitan voluntariamente*; b) *cuando se niega el reporte*, y c) *cuando se otorga información inexacta*.

En el primer supuesto, se debe dar a conocer el uso que tendrán los datos personales, y los alcances (a quienes llegará la información) y efectos (para que fines se piden). Por ejemplo: solicitados datos personales orientados a revelar la opinión política o partidaria (dato sensible), se deberá expresar quien los solicita y para qué los necesita (*v. gr.:* enviar fichas de afiliación).

Frente al segundo supuesto, la negativa a responder puede traer consecuencias legales (en el caso que sea obligatoria la respuesta) o la pérdida de ocasionales beneficios (cuando la respuesta no es obligatoria).

El tercero, es un caso más grave, porqué el afectado podría encontrarse incurso en penalidades como las que agrega el nuevo artículo 117 bis del Código Penal Argentino (*el que insertara o hiciere insertar a sabiendas datos falsos en un archivo de datos personales*), o en menor medida, perder las facultades de gratuidad en la corrección (art. 19) por aplicación de la teoría de los propios actos (nadie puede alegar su propia torpeza y pretender iguales beneficios que respecto al que obra de manera diligente y responsable).

371. Derecho de acceso

371.1. El derecho a solicitar y obtener información de un archivo o registro, para saber si el mismo contiene o no, información personal que a alguien concierne, constituye el fundamento esencial del *habeas data*.

Es el derecho de entrada a los bancos de datos y la garantía principal que tiene la persona para conocer qué información existe sobre ella.

Falcón explica la faz procesal de este derecho, sosteniendo que:

> comprende dos pretensiones sucesivas y secuenciales, una subsidiaria de la otra. La primera de información y la segunda de conocimiento y ejecución…Como se ve, se trata de un proceso complejo, con inversión sucesiva de pretensiones. Así la presentación, que puede ser planteada por vía de proceso sumarísimo o similar expedito, llamado en algunos ordenamientos extraordinario y aun plenario rapidísimo, debe contener una pretensión primaria destinada a que se informe al juzgado de los datos registrados por el Estado (en sí o en cualquiera de las reparticiones), instituciones o particulares referentes al actor, la finalidad de los mismos y en su caso las medidas a tomar sobre dichos datos.

> Dichas medidas se pueden pedir en ese mismo acto (de modo directo o cautelar) si se conocen o presumen, o reservar esta segunda petición para el momento en que se haya contestado el informe. No obstante los contenidos de la petición inicial, no limitan la segunda petición a la luz del informe presentado. La primera etapa del procedimiento entonces será de naturaleza informativa y voluntaria, la segunda podrá tener el carácter de contenciosa.[249]

De alguna manera, como antes se dijo, es la libertad de requerir que "se traigan los datos", cual si fuera la acción exhibitoria propia del *habeas corpus*. Aun cuando es preciso destacar que el acceso no se dirige justamente a los datos sino al archivo que los contiene, y por ello las posibilidades de lograr el control varían con la forma como se presenta el pedido.

371.2. El acceso será directo cuando la información se pueda lograr por la simple consulta al banco de datos, y éste la evacue por un medio escrito o la deje disponible en un medio electrónico por el cual se pueda lograr una rápida visualización.

En cambio, si el requerimiento necesita de la colaboración judicial, se deben adoptar los recaudos típicos de las formalidades para demandar, teniendo en cuenta que se trata de un proceso constitucional que no podrá ser anulado por el principio de legalidad instrumental.

La idea no es poner exigencias previas que hagan vulnerable el derecho de acceso, tales como los recaudos de legitimación o personalidad procesal, sino en su lugar, tener por suficiente la acreditación de identidad que efectúe la persona afectada o aquella que demuestre un interés legítimo para realizar el requerimiento.

Dice Herrán Ortiz que:

> el derecho de acceso presenta en la ley española una amplia variedad de posibilidades, que pueden ser resumidas en la siguiente idea: lo verdaderamente trascendente es que el afectado tenga constancia de la información relativa a sus datos personales registrados, de un modo claro, completo y exacto, de suerte que se procure al afectado el conocimiento de aquellos aspectos fundamentales del tratamiento automatizado de sus datos, para poder ejercitar una defensa de sus derechos con ciertas garantías jurídicas.[250]

Es importante destacar que el derecho de acceso no le corresponde únicamente al particular afectado por la información almacenada en un banco de datos sino a toda persona que acredite un interés legítimo para actuar.

371.3. Uno de los problemas habituales en la garantía ofrecida está en resolver si el acceso supone visualizar directamente el banco de datos, con lo cual el derecho de entrada podría suponer estar en el mismo sitio donde se produce el tratamiento de los datos (y conseguir en ese acto la revelación).

Sin embargo, de esta manera se violaría la seguridad que los archivos deben preservar, razón que sugiere que el derecho de acceso se resuelva a través de la información que se debe brindar.

---

[249] FALCÓN, Enrique M., *Habeas Data*, Abeledo Perrot, Buenos Aires, 1996, p. 32.

[250] HERRÁN ORTIZ, ob. cit., p. 233.

La ley argentina establece en el artículo 14 inciso 2 que: "El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de *habeas data* prevista en esta ley".

Además, es conveniente agregar que el derecho de acceso a la información no supone otro derecho similar como es acceder a la documentación del Estado.

> Nos referimos a los supuestos especiales de aquellos datos personales que se almacenan para fines administrativos, que deben ser objeto de registro permanente (*v. gr.:* bancos de datos de las fuerzas armadas; fuerzas de seguridad; organismos policiales; servicios de inteligencia), o bien, proporcionan estos archivos información a las autoridades administrativas o judiciales en virtud de una autorización legal precedente.

El artículo 23.2 de la ley de *habeas data* argentina dispone que:

> El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

371.4. Otra cuestión que debe ser analizada es la radicación extranjera del banco de datos, porqué las distancias pueden solapar el derecho general de información que tienen todas las personas; como también dificultar el encuentro con la base originaria de la información personal.

Cuando se desconoce de qué fuente proviene el uso de los datos individuales, el derecho de acceso se puede encaminar a través de los organismos de control locales, para que sean éstos quienes asuman el derecho del afectado. Así podría quedar resuelto un problema común como es negar el derecho de acceso por considerar que la información personal recogida no es objeto de la petición, ya que el fichero donde está almacenado no es de carácter nominativo, sino mixto.

No se trata de una sustitución, propiamente dicha, porqué el interesado mantiene la potestad de insistencia ante quien se obliga por sus datos. Quizás el mayor problema podría surgir de aquellos países que no cuenten con ley de protección de datos, a los que puede aplicarse el principio de la "protección equivalente", y negar el acceso basados en el fundamento del trato igualitario que recoge el principio citado.

371.5. También hay que aclarar que el derecho de acceso se tiene a partir del mismo momento que ingresan al archivo, sin importar si los datos personales fueron o no motivo de tratamiento automatizado.

> ¿A partir de qué momento los datos personales pueden ser objeto del derecho de acceso? Se pregunta Estadella Yuste. ¿Pueden incluirse los datos registrados provisionalmente?, o bien ¿debe ejercerse este derecho en los datos personales que ya han sido objeto de operaciones automatizadas?, ¿puede ejercitarse el derecho de acceso sobre los datos al-

macenados?. Entiendo —agrega— que en los dos primeros casos es posible ejercer el derecho de acceso; sin embargo, en el supuesto de información almacenada cuyos nexos de identificación ya han sido eliminados, se podría aceptar la negación del titular del fichero para el derecho de acceso, siempre que éste garantice que los datos serán borrados del sistema una vez cumplida la finalidad del fichero.[251]

371.6. De acuerdo con la finalidad que la petición de acceso persiga, el derecho concreta modalidades implícitas en la garantía a preservar. Es decir, el derecho de acceder a los bancos de datos supone que se especifique para qué se quiere entrar en ellos y qué es lo que se quiere conocer.

A veces la información pretende saber el contenido de la información personal almacenada; en otras, además, se plantea inquirir el medio por donde se obtuvieron los datos; también es posible reclamar para qué y para quien se realizó el registro; y con menor intensidad, indagar los medios utilizados para alcanzar la finalidad para la cual la información ha sido recogida.

> Cada una de estas pretensiones ha llevado a Sagüés, a presentar una clasificación en el *habeas data*, nominando subtipos específicos: a) *exhibitorio*, que consiste en saber qué se registró; b) *finalista*, que procura indagar además para qué y para quién se realizó el registro; c) *autoral*, cuyo propósito es inquirir acerca de quien obtuvo los datos que obran en el registro.[252]

Por su parte Puccinelli, agrega:

> *a)* aquel que tiene por objeto indagar sobre la existencia y localización de bancos y bases de datos que existe en algunos países, y que tiene como objetivo final el garantizar el ejercicio de los derechos de aquellos que se hallen potencialmente afectados, estableciendo la obligatoriedad de inscribir a las bases y bancos de datos en un registro especial que puede ser objeto de consulta; y *b)* aquel que puede utilizar quienes pretenden acceder a la información pública, que funciona cuando no se les permite el acceso a ella sin la debida justificación (obligación legal de reserva, motivos de seguridad del Estado, etc.), y que, aunque para nosotros es otra versión principal, denominada "*habeas data* impropio", se puede englobar en la clasificación de Sagüés.[253]

371.7. El derecho a la información se puede recabar por etapas: *a)* cuando no sabe si está registrado, primero formulará el pedido a la autoridad de control si ella existe en la reglamentación local, o directamente ante el juez cuando se hizo un planteo estéril ante el responsable; informado, concretará la acción consecuente ante los ficheros en los cuales presume se encuentra afectado; *b)* si conoce al archivo al que prestó consentimiento, la petición se hará en forma directa; *c)* si no tiene certeza sobre la base de datos, pero presume que en ella se encuentra, podrá peticionar ante la misma cumpliendo los requisitos formales correspondientes.

---

[251] ESTADELLA YUSTE, ob. cit., p. 290.

[252] SAGÜÉS, Néstor Pedro, *Subtipos de habeas data*, Jurisprudencia Argentina del 20/12/95. Buenos Aires.

[253] PUCCINELLI, "El *Habeas Data* en Indoiberoamérica", en *El Amparo Constitucional, perspectivas y modalidades*, cit., p. 288.

La pretensión informativa se podrá plantear sobre cualquiera de las cuestiones que han sido reglamentadas, esto es:

- Conocer si está en el archivo.
- Conocer los datos que de él se tienen archivados.
- Saber de quién se obtuvieron los datos, cuando no fuera él mismo quien voluntariamente los aportó.
- Saber por qué medios de almacenó la información personal que le incumbe.
- Ser informado sobre las finalidades que tiene el fichero respecto con sus datos.
- Ser informado sobre el destino (lugares o personas) hacia donde irá esa información.
- Ser informado sobre el cumplimiento por el archivo de los principios establecidos, y en particular, si está registrado, y cuáles son los sistemas de seguridad con que protege las bases de datos.

372. El derecho a controlar los archivos

372.1. La base del derecho a la protección de datos personales está en el libre consentimiento que pueda dar quien sea requerido a esos efectos, y en el control que *a posteriori* se pueda ejercer.

Esta vigilancia apunta hacia dos objetos precisos. Controlar al archivo autorizado para que cumpla la finalidad oportunamente expuesta al requerir la autorización; y verificar la actualidad de los datos para que no se ofrezca información obsoleta, equívoca o inexacta.

En ambos casos rige el principio de "calidad de los datos", que como se recordará, establece los deberes que tiene el registro en cuanto a la adecuación, pertinencia y congruencia del almacenamiento con los datos autorizados que se van compilando de la persona concernida.

> Es necesario aclarar que el deber de actualización de los datos es del archivo y no de la persona afectada, incurriendo en negligencia el responsable que no cumpla con esa obligación de veracidad. Al respecto, ha señalado Orozco Pardo que la ley impone al titular del fichero: mantener los datos exactos y al día; rectificándolos de oficio, sustituyéndolos por los correspondientes datos rectificados y completos, sin que sea necesario que ello se solicite. Los datos deben cancelarse de oficio cuando ya no sean pertinentes o necesarios para la finalidad con que se recogieron, mientras tanto, deben estar almacenados de forma que posibiliten el ejercicio de los derechos de los afectados.[254]

La vigilancia es un poder del afectado para controlar directamente al registro, pero se debe diferenciar del control externo que los bancos de datos tienen en los organismos que cada legislación suele crear al efecto.

372.2. En Europa se ha generalizado en la oficina del "Supervisor de Protección de Datos", la asistencia para que los derechos de acceso y control se cumplan por

---

[254] Orozco Pardo, *Los derechos de las personas en la Lortad,* cit., p. 156

las instituciones y los organismos de la Comunidad, en colaboración con los responsables de la protección de datos que han sido nombrados en cada una de las instituciones y los organismos comunitarios.

Las funciones del organismo conciernen el examen e investigación de las reclamaciones presentadas por personas cuyos datos son objeto de tratamiento en instituciones y organismos europeos, incluidos los miembros del personal de la administración de la Unión Europea; la realización de investigaciones y de inspecciones *in situ*, tanto por iniciativa propia como a raíz de una reclamación.

El Supervisor es competente para controlar las actividades de 1as instituciones y los organismos de la Comunidad y para asesorarles. Dentro de los Estados miembros, este tipo de funciones son competencia de las autoridades nacionales de protección de datos y, en algunos países, también de las autoridades regionales. Sus funciones suelen abarcar en general también el tratamiento de datos por entidades del sector privado.

Además, coopera con las autoridades nacionales, por ejemplo en el marco del Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, también conocido como "*Grupo de Trabajo del artículo 29*". Sin embargo, el organismo no es jerárquicamente superior a las autoridades nacionales o regionales.

372.3. En la lista de los derechos de control se alinean los siguientes:

a) *Derecho a la rectificación del dato*

Ante la obligación del archivo de mantener actuales los datos, se instala el derecho de la persona para requerir que se rectifique la información inexacta. No estamos hablando aquí del dato falso o que se aplique con fines discriminatorios, sino de la información errónea, es decir, la que una vez transmitida provoca un dato incierto por ser ajeno a la r realidad. Por ejemplo, si una persona figura como deudora de un crédito que pagó con posterioridad al registro, esa información es atrasada, y el deber de corrección es del archivo —de oficio, o a requerimiento expreso del interesado—.

En doctrina suele llamarse a este tipo de actuación como *habeas data rectificador* o *correctivo*.

> El objetivo de este tipo de *habeas data* —dice Puccinelli— es el de corregir o sanear informaciones falsas, aunque también podría abarcar a las inexactas o imprecisas, respecto de las cuales es factible solicitar determinadas precisiones terminológicas, especialmente cuando los datos son registrados de manera ambigua o pueden dar lugar a más de una interpretación (*v. gr.:* si una información proveniente de un sistema que suministra datos acerca de la factibilidad de otorgar créditos dentro de una Cámara comercial determinada, estableciese que tal persona es un "deudor inhabilitado" y ello obedeciese a que se encuentra inhabilitado para operar con el sistema, pero que no es un inhabilitado en términos jurídicos).[255]

---

[255] PUCCINELLI, "El *Habeas Data* en Indoiberoamérica", en *El Amparo Constitucional, perspectivas y modalidades*, cit., p. 290.

Se rectifica un dato cuando el que se tiene no es correcto, entendiendo como tal a la información incompleta, es decir, la verdad que registra puede ser parcial, y para revestir de integridad la información, necesitar de complementos que el archivo no haya recabado.

Esta característica de las bases de datos, pone en dudas si el deber de mantener actualizada la información es del titular de la base que opera con datos personales; o en su caso, si queda en la iniciativa del interesado la posibilidad de corrección.

En los artículos 4 inciso 5º relacionado con el 16 inciso 1º de la ley argentina, se observa que, aun reconociendo el deber de almacenar y mantener información exacta y actualizarla ("en caso de que ello fuera necesario") permanentemente, también es cierto que la auténtica posibilidad de corregir el dato erróneo o incompleto queda en manos del interesado, o de quienes actúen por cuenta o interés de los acreedores del afectado (en el caso de información de cumplimiento o incumplimiento de obligaciones patrimoniales).

De esta manera, la persona física o jurídica dispone de una garantía de protección de sus datos obligando a los archivos, registros, bases o bancos de datos a mantener, de modo constante, la actualidad de la información que disponen; pero este deber no puede llegar a límites irrazonables respecto a quién está obligado a responder a la consigna de permanente actualización, en la medida que la expresión "en caso de que ello fuera necesario" depende de la información que ofrezca el interesado para variar el dato consignado; o la base de datos conozca de la inexactitud de la información de que se trate.

> Se registra el caso de una base de datos condenada por no haber actualizado la información en ella contenida. La sentencia sostuvo que "cabe responsabilizar a la entidad operadora de un banco de datos que, habiendo tomado conocimiento del error en virtud del cual se había incorporado al actor dentro de la base de datos del Banco Central no procedió a borrarlo de sus respectivos registros, pues no existe norma alguna que le impidiera dejar sin efecto tal incorporación…Habiendo quedado demostrado que el actor ha sido erróneamente incluido en la base de datos del Banco Central; sin que esta obligación pueda verse condicionada al cumplimiento de ciertos requisitos contenidos en una disposición interna de aquél que no ha sido aun publicada en el Boletín Oficial, pues no se trata de una norma vigente en los términos del art. 3º del Código Civil. Tanto más que, en el caso, el demandante ni siquiera operaba con el banco que le comunicó la errónea información a la entidad de contralor…Si bien es cierto que, en el caso, el banco que le comunicó al Banco Central la errónea información respecto del actor que provocó la inclusión de este dentro del registro de deudores del sistema crediticio, no tiene la obligación de borrarlo de ninguna base de datos propia, también lo es que los aquí codemandados Banco Central y Organización Veraz S.A. sólo podían desafectarlo de sus registros una vez que se les hubiese informado el error cometido, por lo cual, la mencionada entidad bancaria deberá ser responsabilizada por no haber realizado oportunamente tal notificación…Dada la ligereza y la falta de prudencia con que se opera en orden a la información pública que se brinda a través de las bases de datos, y habida cuenta de los perjuicios que con ello se puede provocar a los ciudadanos, que no pueden justificarse en función de la mayor agilidad que tal operatoria puede reportar para el comercio, resulta necesario que este hecho sea puesto en conocimiento del Honorable Congreso de la

> Nación a fin de que en ejercicio de su propia competencia adopte las medidas legislativas que estime corresponder.[256]

En la sistemática dispuesta por la ley, el dato que se pretende *rectificar* en realidad se suprime y sustituye por el dato correcto. Si existen dudas sobre la veracidad de la información, la rectificación puede quedar a la espera de una decisión judicial sobre ella; mientras que si es la misma base de datos la que considera, de oficio, la rectificación, ante la duda debe suprimir sin sustituir. El dato que se pretende completar corresponde a un problema de actualización.

Por eso señala Gils Carbó que:

> el dato es incompleto cuando la omisión de algún detalle modifica de manera relevante el sentido de la información. Esta hipótesis no está prevista en la ley, pero puede asimilarse a la inexactitud o al error, y también a la actualización, aunque se distingue de ella porque cuando se trata de actualizar un dato la omisión tiene un contenido específico temporal o cronológico.

La rectificación cambia la información archivada, mientras que con la actualización se integra o complementa.

b) *Derecho a la actualización*

También es posible encontrar informaciones incompletas que dibujan un perfil insuficiente y afectan el derecho a la verdad. En este caso, se debe incorporar al archivo la información parcialmente omitida.

> Un dato puede ser incompleto cuando no tiene toda la información necesaria. Otra cuestión diferente —dice Fappiano— es que los datos de una persona estén desactualizados. Por eso una de las obligaciones que tiene el titular o responsable del registro o banco de datos es llevarlos con toda precisión, pertinencia, perfección y actualidad; para lo cual está obligado a realizar todos los esfuerzos que sean razonables.[257]

La puesta al día trabaja sobre el dato insuficiente, llamado también, dato inexacto o incompleto. No es información real para el tiempo donde se produce y por Eso la finalidad es actualizar el registro. La actualización de los datos pretende agregar información, antes que rectificar la existente; por eso, la doctrina divide o clasifica esta modalidad como *habeas data aditivo* segmentado en subtipos *actualizador* (que persigue renovar el dato caduco), e *inclusorio* (incorporar al registro más información).

> Enseña Puccinelli —siguiendo a Sagüés— que este tipo de *habeas data* procura agregar más datos a los que figuran en el registro respectivo, y puede ser utilizado, por ejemplo, para obligar a un banco de datos comerciales a colocar que una deuda asentada ha sido refinanciada, o que se es deudor como garante de una obligación contraída por un tercero cuyo monto ha sido controvertido judicialmente. En él confluyen dos versiones distintas:

---

[256] CNContenciosoadministrativa, Sala I, 1999/04/21, "*Finoli, Leonardo Luis c/ Banco Central de la República Argentina y otros s/ habeas data*", El Derecho, del 21/10/99.

[257] FAPPIANO, ob. cit., *passim*.

se puede utilizar tanto para actualizar datos vetustos, como para incluir en un registro a quien fue omitido.[258]

c) *Derecho a la confidencialidad de los datos*

La autorización del titular para que los datos sean utilizados con la finalidad que el archivo le informa y en la medida del consentimiento prestado para su transferencia, implica que algunos datos pueden ser restringidos en cuanto a la libre difusión y cesión.

Como regla, los datos sensibles no se pueden circular sin permiso expreso, pero hay otros datos que se pueden mantener en confidencia dentro del registro, y sólo posibles de cesión cuando el titular lo autoriza.

La reserva que estudiamos en el parágrafo 4.6 muestra algunos ejemplos de este tipo de *habeas data*, que algunos de los autores más prestigiados de la ciencia procesal constitucional definen como *habeas data reservador.*

d) *Derecho al silencio y al olvido mediante la cancelación del dato*

Una cosa es ocultar información archivada en virtud del acuerdo de confidencialidad con la persona concernida; y otra distinta, otorgarle un derecho a silenciar toda difusión que se tenga sobre la vida privada cuando el conocimiento se obtiene de los agentes que intervienen el proceso de tratamiento.

Esto es consecuencia del deber de secreto y confidencialidad que los registros deben preservar. La violación o amenaza que potencialmente exista, la controla el afectado a través del proceso de *habeas data*.

Asimismo, cuando el dato ha cumplido la finalidad para la cual se archivó, aparecen dos consecuencias que se traducen en derechos y deberes de la persona y el banco de datos, respectivamente.

El derecho se fundamenta en la potestad de reclamar la eliminación de toda información que violente la esfera de privacidad personal cuyo almacenamiento no fuera autorizado. También, el poder de exclusión o supresión permite demandar la cancelación del dato que se ha tornado impertinente o ha devenido innecesario.

Los derechos al silencio y al olvido se recogen de la ley de tratamiento de datos española que obliga a las personas que intervienen en cualquier fase del tratamiento de datos a mantener reservada la información que adquieren en ocasión del trabajo. Se trata por tanto —afirma Orozco Pardo— de la situación en que la existencia y contenido de los datos debe quedar dentro del ámbito funcional y finalidad del fichero para el que fueron recabados evitando el "rumor informático" (derecho al silencio) y del derecho a que, de oficio, el titular o responsable cancele o destruya los datos personales cuando se den alguno de los supuestos antes citados, sin que tenga que mediar previamente el ejercicio del derecho de cancelación (derecho al olvido).[259]

---

[258] PUCCINELLI, "El *Habeas data* en Indoiberoamérica", en *El Amparo Constitucional, perspectivas y modalidades*, cit., p. 291.

[259] OROZCO PARDO, ob. cit., p. 156.

El deber, por su parte, es del titular del archivo, quien debe eliminar la información personal compilada que ha perdido interés, actualidad o sentido para el objeto inicialmente guardado.

El afectado, si considera que los datos carecen de pertinencia o devienen inadecuados, puede ejercer el derecho de cancelación o bloqueo de transmisión, propiciando en el pedido al registro que se borren todos los datos innecesarios.

Para Sagüés, este tipo de *habeas data* se denomina *exclutorio* o *cancelatorio*, interpretando que la eliminación procede en los casos en los cuales se trate de datos sensibles, aunque no existe una regla fija acerca de verificar cuándo procede esta vía constitucional.[260] Puccinelli, por su parte, agrega que es factible incluir en esta versión a otra clase de datos que, sin resultar sensibles, de todas formas no puede ser almacenada por cualquier registro (como ocurre, *v.gr.*, con las fórmulas de determinadas sustancias), pues aunque alguno las podrá contener de manera reservada, en los casos en que no se trata de un registro habilitado para ello, no bastará con infidenciarla, sino que es imprescindible su eliminación.[261]

373. Excepciones al derecho de acceso, rectificación y supresión

373.1. En líneas generales el derecho de control sobre los archivos y los datos personales se restringe en contadas ocasiones. Las veces que así ocurre se fundamentan en cuestiones de seguridad nacional, orden público, razones morales y políticas, sin perjuicio de los derechos y acciones que a terceros les corresponde cuando están afectados sus intereses legítimos.

En la ley argentina nacional se establecen como excepciones las siguientes (art. 17):

1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

Es importante agregar que la obstaculización al derecho de acceso es considerada falta grave del titular o usuario del archivo.

---

[260] SAGÜÉS, Néstor Pedro, *Subtipos de habeas data*, passim.

[261] PUCCINELLI, "El *Habeas data* en Indoiberoamérica", en *El Amparo Constitucional, perspectivas y modalidades*, cit., p. 289.

373.2. Las excepciones que la ley argentina crea al derecho que tienen las personas físicas y jurídicas para controlar las bases de datos que los afectan, se pueden considerar, mínimamente, violatorias del sentido fundamental que contiene la protección de datos personales.

El primer gran error es otorgar a los archivos públicos una suerte de patente de corso por la cual resultan únicos autorizados para denegar el acceso, la rectificación o la supresión, con el solo recaudo de emitir una decisión fundada. No tienen igual derecho de oposición los archivos privados, quienes en todo caso, deberán recurrir a las medidas cautelares ante la justicia, con el fin de evitar una contestación negativa que, eventualmente, los haría pasibles de sanción por la autoridad de control.

Decir que es para proteger a la Nación, el orden y la seguridad públicos; o para interceder como defensores de los derechos e intereses de terceros, son términos de una vaguedad muy grande, y por tanto exceden la discrecionalidad hipotética a tolerar.

Es evidente que tal grado de indeterminación es incompatible con el fin de fácil acceso y rapidez en el control sobre las bases o bancos de información personal, sin perjuicio de anular una disposición constitucional que persigue justamente lo contrario.

El Tribunal Constitucional español ha declarado la inconstitucionalidad de este precepto incluido en la ley 15/1999. Ha dicho:

> Como en otra ocasión hemos aseverado, los motivos de limitación adolecen de tal grado de indeterminación que deja excesivo campo de maniobra a la discrecionalidad administrativa, incompatible con las exigencias de la reserva legal en cuanto constituye una cesión en blanco del poder normativo que defrauda la reserva de ley. Además, al no hacer referencia alguna a los presupuestos y condiciones de la restricción, resulta insuficiente para determinar si la decisión administrativa es o no el fruto previsible de la razonable aplicación de lo dispuesto por el legislador (SSTC 101/1991, FJ 3 y 49/1999, FJ 4). De suerte que la misma falta evidente de certeza y previsibilidad del límite que el art. 24.2 LOPD impone al derecho fundamental a la protección de los datos personales (art. 18.4 CE), y la circunstancia de que, además, se trate de un límite cuya fijación y aplicación no viene precisada en la LOPD, sino que se abandona a la entera discreción de la Administración Pública responsable del fichero en cuestión, aboca a la estimación en este punto del recurso interpuesto por el Defensor del Pueblo al resultar vulnerados los arts. 18.4 y 53.1 CE.

373.3. La constitucionalidad de esta medida restrictiva debiera estar sustentada en otros principios, antes que en la sola decisión de la Administración Pública. Ni es suficiente que la ley apodere a ésta para que precise en cada caso sus límites, ni siquiera para asegurar finalidades tan genéricas como las establecidas. Es cierto que ellas pueden existir y ser razonablemente interpuestas como obstáculos al progreso del control sobre los archivos; pero también lo es que la cláusula es contradictoria con los principios que la Constitución sustenta y la ley consagra entre sus preceptos.

En todo caso, debiera ser el legislador quien determine cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales

y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales.

> Reafirma el Tribunal Constitucional español, en la sentencia antes comentada, que si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional.
>
> Ahora bien, aun habiendo llegado a esta conclusión no es ocioso señalar, de un lado, que el derecho a consentir la recogida y el tratamiento de los datos personales (art. 6 LOPD) no implica en modo alguno consentir la cesión de tales datos a terceros, pues constituye una facultad específica que también forma parte del contenido del derecho fundamental a la protección de tales datos. Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatibles con éstos (art. 4.2 LOPD) supone una nueva posesión y uso que requiere el consentimiento del interesado. Una facultad que sólo cabe limitar en atención a derechos y bienes de relevancia constitucional y, por tanto, esté justificada, sea proporcionada y, además, se establezca por Ley, pues el derecho fundamental a la protección de datos personales no admite otros límites... (*El fallo* in extenso *se encuentra publicado en el Suplemento de Derecho Constitucional de la Revista La Ley, del 15 de junio de 2001*).

373.4. El artículo 17 señalado, que también es fuente de otras legislaciones, contiene las siguientes causas de justificación para denegar el acceso o cualquiera de las acciones de control sobre las bases de datos públicos:

a) Defensa de la Nación

b) Defensa del orden

c) Defensa de la seguridad pública

d) Protección de los derechos e intereses de terceros

e) Cuando se obstaculice una actuación judicial o administrativa en curso que investigue sobre el cumplimiento de obligaciones tributarias o previsionales

f) Cuando impida el desarrollo de actividades de control de la salud

g) Cuando obstaculice el control del medio ambiente

h) Cuando impida o genere dificultades en la investigación de delitos penales

i) Cuando impida o genere dificultades en la verificación de infracciones administrativas.

Estas defensas exclusivas coinciden parcialmente con las establecidas en el artículo 24 (Otras excepciones a los derechos de los afectados) que tiene la Ley 15/1999 del 13 de diciembre, española, que ha sido declarado inconstitucional por el fallo recién mencionado. *Allí se indica que:*

> 1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas. 2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

Las excepciones se vinculan con los incisos 1º y 2º de la norma, y más allá de los reparos que tuvo la redacción definitiva en oportunidad de su debate parlamentario, es preciso señalar la operatividad de cada situación contemplada.

a) *Defensa de la Nación*: Por defender de la Nación se entienden las actividades que realizan las Fuerzas Armadas para proteger al Estado en caso de agresión interna o externa; también, cuando la soberanía está cuestionada o se provocan amenazas que impiden el ejercicio de los derechos fundamentales de los habitantes.

Parece, en consecuencia, de una latitud muy grande sopesar el argumento de la defensa nacional cuando se trata del uso de datos personales. Eventualmente, podría darse el caso de alguien que reclamara la confidencialidad de información por vulnerar un derecho que le es propio y encuentra afectado su honor e intimidad, y provocar con ese ejercicio, una alteración en la seguridad de los habitantes; pero dicho reclamo debiera, en su caso, articularse con lo dispuesto en el artículo 23 inciso 2º, el cual involucra a los archivos con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, entre otros organismos del Estado. En tal sentido, denegar el acceso, como cualquiera de las acciones de control debiera, en todo caso,

quedar al amparo de los jueces, los que están facultados para resolver con adecuada ponderación de las circunstancias.

Por otra parte, una medida así, excede la discrecionalidad y provoca una desigualdad en el trato respecto a los demás archivos, y en particular, a los privados destinados a dar información.

b) *Defensa del orden*: El orden es un concepto muy vago, en razón de comprender múltiples matices y posibilidades de proyección. Respecto al cuadro de especificaciones que tiene el artículo 17, el orden referido pareciera ser el que puede resultar afectado para la administración interna del Estado, ya sea para cuestiones sociales como económicas.

De así resultar se contrapone con el secreto fiscal dispuesto en el artículo 101 de la Ley 11.683 (Argentina), reserva que se extiende a toda la documentación que se expone incluyendo los papeles privados de los que el Fisco toma conocimiento, sea por requerimiento o declaración voluntaria.

Evidentemente, al levantarse el secreto fiscal sobre este tipo de actos de confidencialidad, se pretende establecer una especie de sanción al renuente o al incumplidor con la presentación de las declaraciones juradas correspondientes a obligaciones tributarias, lo que es absolutamente inconstitucional.

Sin embargo, es manifiesta la intención de los organismos recaudadores —algunas veces concretada— de informar los sumarios o investigaciones que se practican a quienes pueden haber violado el deber de decir verdad en las declaraciones de impuestos. La exposición como vergüenza pública afecta la intimidad, sin perjuicio de otros intereses afectados.

Planteadas ambas situaciones, es posible que se fomente la ambigüedad normativa, obligando a intervenciones judiciales esclarecedoras, como medio de lograr el justo equilibrio de la ley.

Entra dentro del análisis que se efectúa, las comunicaciones que realiza el Fisco al Banco Central sobre supuestas deudas, que aun sin estar firmes por ser litigiosas, se comunican como si fueran tales; así como los potenciales incumplimientos de la seguridad social. Hace un tiempo el Fisco remitía una nota a los bancos con los que operaba el contribuyente o responsable en los términos del artículo 12 de la Ley 14.449 y de la Circular 1703 del BCRA, a los fines de inhabilitarlo para conseguir créditos de parte de la institución bancaria.

c) *Seguridad Pública*: Los datos personales considerados en la seguridad pública, que hipotéticamente no se podrían revelar a través del derecho de acceso, o proceder a modificarlos o suprimirlos en orden a cualquiera de las acciones de control, no serían aquellos vinculados con la prevención y represión del delito pues a estos se refiere más adelante el inciso en estudio.

Por tanto, hay que sostener que dicha norma solo completa e integra un cuadro ejemplificativo de situaciones de excepción, o en algunos casos insiste con las especificaciones para dejar en claro cuantas son las veces y los casos de los que se pueden valer los archivos públicos para no actuar conforme lo plantea el requirente afectado.

No hay que olvidar lo establecido en el párrafo final del artículo 23 inciso 2º de la Ley 25.326 de Argentina, cuando especifica que "los archivos (con fines de defensa nacional o de seguridad pública) deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad".

Por tanto, resta a la autoridad de control dar cumplimiento con esta necesaria clasificación que propicia evitar excesos o arbitrariedades en las causas de exclusión.

Ha dicho Gils Carbó que:

> la dificultad de delinear un límite para la aplicación de estas causales de excepción al reconocimiento de derechos individuales es evidente, pues se trata de conceptos jurídicos indeterminados. Además, en materia de acceso y rectificación de los datos resulta difícil encontrar reglas generales y simples, que a su vez no vayan seguidas de múltiples excepciones y de la necesidad de ponderar en cada caso las circunstancias de hecho. Pues si bien existen principios básicos que delimitan cuáles son los derechos del titular y las correlativas obligaciones del responsable del registro, de la naturaleza de los intereses en juego dependerá que se reconozca prevalencia a uno sobre otro. La simple curiosidad puede bastar para justificar el acceso a un registro público administrativo, mas no para acceder a un registro de los servicios de inteligencia. Estos se ubican en el plano de la máxima reserva junto con las bases de datos de las fuerzas de seguridad y las afectadas a la defensa nacional, debido a la relevante función que cumplen en las investigaciones para la persecución del terrorismo y el crimen organizado. Es que el secreto impuesto por estas razones, es oponible aun al titular de los datos afectados por las informaciones que contengan los registros, pues está justificado en el resguardo de los intereses superiores del Estado.[262]

d) *Protección de los derechos e intereses de terceros*: El derecho de acceso puede llevar al archivo público a tener que exponer sus registros de forma tal que con la apertura ponga a disposición del requirente información que no le concierne por referir a terceros.

Si además vulnera la confidencialidad de esa información almacenada, está en su derecho negar el derecho reclamado, dando las razones y justificativos para la denegación. No obstante, no es la solución que en otros lugares se realiza frente a situaciones como estas. En Estados Unidos, por ejemplo, un organismo debe eliminar detalles de identificación personal, para prevenir una invasión a la privacidad, siempre que pone a disposición o publica una opinión, hace una declaración política, o realiza una interpretación o un manual o instrucción al personal.

En cada caso se debe explicar completamente y por escrito la justificación de la eliminación, obligando al archivo a tener un resumen de cada oportunidad que lo practica. Cada organismo debe oportunamente publicar trimestralmente o con más frecuencia y distribuir (por venta o de cualquier otro modo) copias de estos informes, que se presentan como índices o suplementos.

En la práctica, la protección del derecho o intereses de terceros, mejor puede practicarse si es un Juez quien lo decide.

---

[262] Gils Carbó, ob. cit., p. 237.

Gils Carbó explica que:

> la protección de derechos e intereses de terceros constituye una excepción al derecho de acceso a los registros de datos que rige tanto para el sector público (art. 17.1) como para el privado (art. 15.2 "*in fine*") y se presenta con relación a los documentos que se conocen como *doblemente nominativos*. Las doctrina se refiere a *documentos nominativos*, para designar a los que contienen una apreciación o juicio de valor sobre una persona nominalmente designada o fácilmente identificable, incluyendo informaciones de orden personal o relativas al comportamiento y cuya divulgación podría causar un perjuicio, *v.gr.* un informe social, una evaluación laboral, un diagnóstico médico, etc. Son documentos que contienen datos personales y que, además, tienen entidad para afectar los intereses o derechos del titular de aquéllos, lo que los ubica dentro de una categoría especial en un régimen de tutela. Los *documentos* son *doblemente nominativos* cuando además de contener informaciones sobre una persona, por ejemplo, está identificado el autor de esas opiniones, de modo que hay más de un sujeto comprometido en la publicidad o consulta de los datos, cuyo interés es también digno de protección.[263]

También en aras de esta defensa hacia el interés de terceros está la Ley 24.766 sobre confidencialidad de la información que esté legítimamente bajo control de una persona y se divulgue sin su consentimiento de manera contraria a los usos comerciales honestos.

e) *Obstáculos en una actuación judicial o administrativa:* La excepción tiene dos requisitos: *1)* que se trate de investigaciones en curso; y *2)* que sean sumarios administrativos o expedientes penales relativos al *cumplimiento de obligaciones tributarias o previsionales*.

Esta disposición se relaciona con los *artículos 7º inciso 4º* (que le permite al Estado proceder al tratamiento de datos personales relativos a antecedentes penales o contravencionales), *20* (en cuanto le impide al juez o a la autoridad administrativa a resolver sobre la información contenida en una base de datos personales que definan el perfil o la personalidad del afectado), y *23* (en los casos de archivos del Estado de consulta permanente por ser necesarios para la gestión administrativa).

Pero además, este artículo 17 inciso 2º autoriza operar con la excepción a magistrados y funcionarios administrativos cuando la acción de *habeas data* provoque "obstáculos en las actuaciones", o la "investigación de delitos penales o la verificación de infracciones administrativas".

El simple enunciado potencial de "provocar obstáculos" dicho al principio, como el agregado de afectar la investigación o la verificación (que para el caso es lo mismo), son exageraciones al poder discrecional del Estado, y debieran dejarse en manos de los jueces, únicamente.

> En Estados Unidos, la excepción se plantea para los datos mantenidos por una agencia o componente de la misma que realice como función principal cualquier actividad relacionada con el cumplimiento de las leyes penales, incluyendo los esfuerzos de la Policía para prevenir, controlar, o reducir el crimen o para apresar criminales, y las actividades

[263] GILS CARBÓ, ob. cit., p. 238.

de los abogados, tribunales, correccionales y autoridades de sentencias de libertad condicional, y que consista en: (a) información compilada con el propósito de identificar transgresores penales o supuestos transgresores y consistente solo en la identificación de datos y notaciones de arrestos, la naturaleza y tipo de cargos penales, sentencias, reclusión, liberación, y condición de libertad bajo palabra o condicional; (b) información compilada para una investigación penal, incluyendo declaraciones de informantes y detectives, y asociados con un individuo identificable; o (c) informes identificables para un individuo compilado en cualquier etapa del proceso de cumplimiento de las leyes penales desde arresto o acusación hasta liberación de supervisión.

La decisión de excluir la respuesta debe ser fundada y notificada expresamente al requirente.

f) *Impedimentos para el desarrollo de actividades de control de la salud*: El "desarrollo de funciones de control de salud" puede tener dos lecturas. Desde una primera visión, se ocupa del derecho de negar al paciente o afectado el derecho de interferir en una investigación que se viene practicando, cumpliendo rigurosamente el requisito de disociación entre datos personales e información consecuente (*cfr.* arts. 5 inciso *d)*, 8, 9 inciso 2°, 11 inciso 3° apartados *d)* y *e)* y 12 inciso 2 apartado *b)*). Por otra vertiente, analiza el derecho del Estado de negar el acceso, la rectificación, la actualización o la supresión de aquellos datos que se necesitan para administrar y regular cuestiones atinentes a la salud de la población (*v. gr.:* no se puede cancelar de un archivo público el dato que registra la evolución de una enfermedad, para observar a partir del mismo, si se trata de epidemia, brote epidémico, o casos aislados).

Es recurrente, en esta consideración, recordar que el uso de los datos médicos requiere disociación o anonimato para al tratamiento del afectado. La información es imprescindible, no solamente para la asistencia clínica, sino también, y quizá en mayor medida, para la gestión sanitaria y la salud pública.

En principio, los datos médicos deben ser recogidos y procesados sólo por profesionales sanitarios o por individuos u órganos que trabajen en representación de profesionales sanitarios. Los individuos u órganos que trabajen en representación de profesionales sanitarios recogiendo y procesando datos médicos deben estar sujetos a las mismas normas de confidencialidad que pesan sobre los profesionales sanitarios o a normas de confidencialidad comparables.

Los administradores de archivos que no son profesionales sanitarios sólo deben recoger y procesar datos médicos cuando estén sujetos a normas de confidencialidad comparables a las que pesan sobre el profesional sanitario o a medidas de seguridad igualmente eficaces proporcionadas por la ley nacional.

En particular, salvo que la ley nacional proporcione otras medidas de salvaguardia, los datos médicos sólo pueden comunicarse a una persona sujeta a las normas de confidencialidad que pesan sobre un profesional sanitario o a normas de confidencialidad comparables, y que acate las normas de esta recomendación.

La exclusión prevista tiene en cuenta, antes que la revelación de datos personales, la afectación posible de acciones comunitarias. Porqué los datos médicos, en sí mismos, se pueden comunicar cuando son relevantes para la prevención de un pe-

ligro real o la represión de un delito específico; o existe otro interés público importante; o es necesario a la protección de los derechos y las libertades de otros; o la comunicación es permitida por la ley con fines de:

- protección del sujeto de los datos o de un pariente en línea genética;
- salvaguarda de intereses vitales del afectado o de una tercera persona;
- el cumplimiento de obligaciones contractuales específicas;
- el establecimiento, ejercicio o defensa de una reclamación legal.

El artículo 8.1 (Recomendación 81 sobre datos médicos, ya transcripta) dice que:

> Se permitirá a toda persona el acceso a sus datos médicos, ya directamente o a través de un profesional sanitario o, si lo permite la ley nacional, a través de una persona designada por el titular de los datos. La información debe ser facilitada de modo inteligible.
>
> 8.2. El acceso a los datos médicos puede ser denegado, limitado o rechazado sólo si lo prevé la ley y si:
>
> *a)* constituye una medida necesaria en una sociedad democrática por su interés en proteger la seguridad del Estado, la seguridad pública o la represión de crímenes; o
>
> *b)* el conocimiento de la información es probable que cause un serio daño a la salud del afectado; o
>
> *c)* la información sobre el afectado revela también información sobre terceros o, respecto a los datos genéticos, si esta información es probable que cause un serio daño a un pariente consanguíneo o uterino o a una persona que tiene un vínculo directo en línea germinal; o
>
> *d)* los datos son empleados para fines de investigación científica o estadística y se aprecia con nitidez que no hay riesgo alguno de violación de la intimidad del afectado, especialmente el de usar los datos en decisiones o medidas que afecten a un individuo en particular.

g) *Control del medio ambiente:* Con idéntico alcance se persigue evitar que la política de protección al medio ambiente, y el derecho que tiene toda persona a la salud en un medio ecológicamente equilibrado, quede anulado por proteccionismos individuales que, otorgando acceso a fuentes de información pública, revelen actividades o políticas estratégicas del Estado.

De igual modo, si el derecho de control individual sobre las bases de datos se concede y, con ello, se afecta la confidencialidad de medidas tendientes a concretar acciones de control público, o en su caso, la eliminación de datos supondría alterar dichas acciones, la norma autoriza a no responder invocando la excepción articulada.

h) *Dificultades en la investigación de delitos penales:* Como se observó esta calidad de apreciación subjetiva queda en poder del juez. La norma indica que no basta la existencia de una investigación para que se configure esta causal sino que, además, la comunicación de los datos debe interferir o retrasar el trámite. Lo más adecuado sería que el funcionario o magistrado instructor del procedimiento sea el que decida sobre la procedencia de la petición, ya que es quien estará en mejores condiciones de emitir un juicio de esa naturaleza.

En cambio, la ley no ha hecho diferencias respecto al tipo de investigación penal en curso, porqué si la causa involucra intereses de terceros la limitación al derecho de acceso y control podría ser temporal; esto es, que perdure en tanto no se pueda admitir el derecho sin afectar al sumario propiamente dicho. Mientras que si el delito o la persecución penal vinculara a funcionarios a agentes de la administración pública, la prohibición de acceso tendría que tener un carácter más permanente, porqué la investigación no se agota con el encuentro de sujetos a condenar.

i) *Dificultades en la verificación de infracciones administrativas*: A esta condición se le pueden extender las anteriores conclusiones; sin perjuicio de ello, se nos ocurre que solamente mediante la acción de supresión de los datos personales almacenados se podría afectar la verificación de una infracción administrativa, teniendo en cuenta que no consideramos de esta calidad a los delitos de orden tributario.

Tanto como en el caso anterior, se debe exigir la acreditación del interés a quien reclama, y resolver frente a esta situación si corresponde obrar la excepción que la ley dispensa.

Sección 10ª Protección procesal y *habeas data*

374. Requisitos generales

374.1. Los requisitos para entrar en los bancos de datos se clasifican por el lugar, el tiempo y la forma como se debe realizar. En nuestra opinión, primero se debe emplazar al titular o responsable del archivo para que otorgue el derecho de acceso y permita el ejercicio activo de las acciones de control; sin embargo, no todas las legislaciones coinciden al punto que otras atienden al *habeas data* como una vía directamente judicial.

Observemos con los ejemplos que venimos trayendo:

En *Bolivia* se puede interponer el recurso de *habeas data* ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección del afectado.

En *Brasil* la vía es electiva. Puede ser judicial directa o preferir quien reclama el procedimiento secreto que puede ser, asimismo, administrativo o jurisdiccional.

Chile claramente establece el reclamo administrativo previo y si el responsable del registro o banco de datos personales no responde la solicitud de información, modificación, bloqueo, cancelación o eliminación pretendida, se puede deducir, dentro de los dos días hábiles siguientes, la acción de *habeas data*.

En *Colombia* se denomina acción de *habeas data* tanto al reclamo previo como al mecanismo procesal constitucional. De allí que se permita ejercer ambos procesos (*habeas data* y petición), en forma directa o a través de los operadores que creó la ley estatutaria, conforme lo previsto en los procedimientos de consultas y reclamos.

> El derecho lo tienen los titulares de la información o sus causahabientes, quienes podrán consultar la información personal del titular, que repose en cualquier banco de datos, sea este del sector público o privado. El operador deberá suministrar a estos, debidamente identificados, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular. La petición o consulta de información se formulará verbalmente, por escrito, o por cualquier canal de comunicación, siempre y cuando se mantenga evidencia de la consulta por medios técnicos. El trámite de reclamos, establece que los titulares de la información o sus causahabientes que consideren que la información contenida en su registro individual en un banco de datos debe ser objeto de corrección o actualización podrán presentar un reclamo ante el operador, el cual será tramitado bajo las siguientes reglas: 1) La petición o reclamo se formulará mediante escrito dirigido al operador del banco de datos, con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y si fuere el caso, acompañando los documentos de soporte que se quieran hacer valer. En caso de que el escrito resulte incompleto,

se deberá oficiar al interesado para que subsane las fallas. Transcurrido un mes desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de la reclamación o petición. 2) Una vez recibido la petición o reclamo completo el operador incluirá en el registro individual en un término no mayor a dos (2) días hábiles una leyenda que diga "reclamo en trámite" y la naturaleza del mismo. Dicha información deberá mantenerse hasta que el reclamo sea decidido y deberá incluirse en la información que se suministra a los usuarios. 3) El término máximo para atender la petición o reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender la petición dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

En *Ecuador* igualmente se participa de la doble vía. A toda persona se le reconoce el derecho a conocer de los titulares o responsables de archivos de datos personales, que se proporcione información suficiente y completa sobre la finalidad, origen y destino de los datos almacenados. Y en su caso, la acción de *habeas data* tendrá como fin garantizar dicho derecho de acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes sobre sí misma, que estén en poder de entidades públicas o privadas, cualquiera sea el soporte donde se encuentren (art. 49, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional).

Paraguay genera un procedimiento administrativo previo que se sostiene en el derecho de toda persona para acceder a la información y a los datos que sobre sí misma, sobre su cónyuge, sobre personas que acredite se hallen bajo su tutela o curatela, o sobre sus bienes, obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial, así como conocer el uso que se haga de los mismos o su finalidad.

Si los reclamos extrajudiciales no fueran atendidos sin razón o sin base legal, se aplicará a la entidad reacia al cumplimiento de sus obligaciones una multa. El juzgado ordenará que se efectúen las rectificaciones o supresiones que correspondan, y podrá ordenar también que la sentencia definitiva sea publicada en forma total, parcial o resumida, a costa del responsable. Será competente para la aplicación de las multas el juzgado en lo civil y comercial, en trámite sumario.

La Ley 26.301 de *Perú* establece que la garantía constitucional de la acción de *habeas data* de que trata el inciso 3 del Artículo 200 de la Constitución Política del Estado se tramitará, ante el juez de primera instancia en lo civil de turno del lugar en donde tiene su domicilio el demandante, o donde se encuentran ubicados los archivos mecánicos, telemáticos, magnéticos, informáticos o similares, o en el que corresponda al domicilio del demandado, sea esta persona natural o jurídica, pública o privada, a elección del demandante. Si la afectación de derechos se origina en archivos judiciales, sean jurisdiccionales, funcionales o administrativos, cualquiera sea la forma o medio en que éstos estén almacenados, guardados o contenidos, conocerá de la demanda la Sala Civil de turno de la Corte Superior de Justicia respectiva, la que encargará a un juez de primera instancia en lo civil su trámite. El fallo

en primera instancia, en este caso, será pronunciado por la Sala Civil que conoce de la demanda. Este mismo precepto regirá para los archivos funcionales o administrativos del Ministerio Público.

Uruguay dispone en el artículo 37 de la ley 18331 la acción de *habeas data* diciendo que: "Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y, en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización, a exigir su rectificación, inclusión, supresión o lo que entienda corresponder". Es decir que la norma establece cada uno de los subtipos de *habeas data* analizadas.

No obstante case advertir que la disposición no inhabilita el reclamo administrativo previo que se puede ejercer como derecho a la información; como tampoco inhibe la promoción de una demanda de amparo.

En *Venezuela,* el artículo 28 de la Constitución también consagra el derecho de toda persona de acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas, quedando a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley. La norma, por tanto, consagra dos derechos distintos, sobre los cuales la Sala Constitucional en sentencia de 23 de agosto de 2000 (Caso: *Veedores de UCAB*) expresó en materia de derecho de acceso:

> el artículo 28 separa el acceso a la información y a los datos, del acceso a documentos que contengan información, la cual debe ser puntual, sobre cualquier tópico, sean o no dichos documentos soportes de bases de datos, que tengan interés para las comunidades o grupos. El acceso a estos documentos es distinto al de las bases de datos, de cualquier tipo. Se trata de acceder a documentos en sentido amplio, escritos o meramente representativos (de allí que la norma expresa que son documentos de cualquier naturaleza), que por alguna razón contienen información de interés para el grupo, o para la comunidad. Tal interés debe ser decidido por el juez, para ordenar su exhibición, por lo que debe ser alegado, no bastando la subjetiva apreciación del actor en ese sentido.

Estos derechos de *habeas data*, por otra parte, son también distintos al derecho garantizado en el artículo 143 de la misma Constitución que tienen todos los ciudadanos a ser informados oportuna y verazmente por la Administración Pública, sobre el estado de las actuaciones en que estén directamente interesados, y a conocer las resoluciones definitivas que se adopten sobre el particular. Asimismo, consagra la norma el derecho de acceso a los archivos y registros administrativos, sin perjuicio de los límites aceptables dentro de una sociedad democrática en materias relativas a seguridad interior y exterior, a investigación criminal y a la intimidad de la vida privada, de conformidad con la ley que regule la materia de clasificación de documentos de contenido confidencial o secreto. La norma prohíbe, en todo caso, la censura a los funcionarios públicos en relación a lo que informen sobre asuntos bajo su responsabilidad.

En cuanto al derecho de *habeas data* que consagra el artículo 28 de la Constitución, la Sala Constitucional del Tribunal Supremo de Justicia en su sentencia Nº 1050 dd

el 23 de agosto de 2000 (caso: *Ruth Capriles y otros*), determinó que se trata de un "derecho de las personas a conocer la información que sobre ellas, hayan sido compiladas por otras" consecuencia del hecho de que "tanto el Estado, como los particulares, mediante diversas formas de compilación de datos: manuales, computarizados, etc., registran y almacenan datos e informaciones sobre las personas o sobre sus bienes, y en vista que tal recopilación puede afectar la vida privada, la intimidad, el honor, la reputación, la vida económica y otros valores constitucionales de las personas naturales o jurídicas, la Constitución, para controlar tales registros, otorga varios derechos a la ciudadanía que aparecen recogidos en el artículo 28 citado.[264]

Finalmente en *México,* la ley federal es clara al establecer que el reclamo es netamente administrativo debiendo recurrirse ante el Instituto Federal de Acceso a la Información y Protección de Datos, a que hace referencia la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

El art. 22 de la norma citada dice:

> […] Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.

Por su parte, el artículo 23 dice: "Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento".

374.2. Cuando son reclamaciones administrativas directamente opuestas ante el responsable de la base de datos, el *lugar* donde plantear la pretensión es ante el titular del registro o archivo que tiene los datos personales del interesado.

La categoría de la información personal puede eludir el derecho de acceso, por ejemplo, en los casos de hospitales y demás instituciones sanitarias —públicas o privadas—, la recolección de datos se ampara por el secreto profesional. De similar envergadura es la prohibición de acceso a los archivos de datos sensibles que únicamente se admiten crear cuando median razones de interés general, autorizadas por la ley. También, como vimos, algunas legislaciones protegen a los archivos públicos impidiendo que se plantee ante ellos este tipo de reclamaciones.

374.3. La intervención de un tercero en el tratamiento de los datos implica obligarlo solidariamente con el titular del archivo, de manera que corresponde tener en cuenta el domicilio del cesionario, a los fines de deducir el reclamo administrativo.

---

[264] BREWER CARÍAS, *El proceso constitucional de las accciones de habeas data en Venezuela*, cit., pp. 146 y ss.

Si el banco de datos no informa de conformidad con lo requerido, el lugar donde presentar el *habeas data* es el del órgano de control que la ley establezca, o el del juez donde se encuentre la base comprometida, salvo que la propia reglamentación establezca una jurisdicción especial, como es el caso señalado de Bolivia y Perú.

374.4. El *tiempo* para formular el pedido, siguiendo el derecho comparado, oscila entre intervalos de seis a doce meses.

En Argentina el derecho de acceso sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis (6) meses, salvo que se acredite un interés legítimo al afecto.

> España, por su parte, está dicho en términos similares que el derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes. La periodicidad para el ejercicio del derecho de acceso es un criterio que llega de las normas europeas, especialmente del Convenio 108 y de la Directiva 95/46/CE, aunque ninguna de ellas establece un tiempo determinado sino la elasticidad del período prudente y razonable, para admitir una cobertura amplia.

Estos son plazos continuos, en el sentido que no tienen términos de prescripción sino pausas o treguas entre las veces que se pueden suscitar. El cómputo se inicia en cualquier momento cuando no se tiene conocimiento efectivo y solo se persigue el derecho de acceso; a diferencia de otras situaciones donde se informa a la persona concernida (*v. gr.:* aviso de privacidad de México; notificación individual en Argentina u otras legislaciones; edictos o comunicaciones masivas, etc.) y se cuenta desde allí el lapso para pedir.

La pauta general es la toma de conocimiento de la posible afectación, y los períodos cambian según se conozca o no al archivo donde plantear los derechos. Por eso, para formular el interés de lograr la información planteada comienza desde la incorporación de los datos al archivo, o desde el momento en que el afectado presume que sus datos se encuentran en un determinado archivo. A partir de allí rige el derecho de acceso e información, sin que ello suponga un plazo de caducidad.

En Argentina el período de seis meses comentado es por el beneficio de gratuidad, por eso, no se quiere significar que no existan períodos establecidos para el derecho de acceso, sino consideraciones de naturaleza económica, las que de ser establecidas, deberán autorizarse por la autoridad de control. No obstante, no se puede formular más de una petición cada seis meses, salvo que se justifique plenamente el interés en hacerlo.

374.5. La *forma* de concretar el derecho está liberada de requisitos formales. Rige el principio de libertad sin solemnidades, aunque habitualmente los órganos de control presentan formularios que facilitan la fundamentación del planteo.

En Argentina el párrafo segundo del artículo 15 de la reglamentación indica que: "La Dirección Nacional de Protección de Datos Personales elaborará un formulario que facilite el derecho de acceso de los interesados".

De igual manera, cuando se trate de archivos públicos de fácil acceso o destinados a la difusión pública (*v. gr.:* Banco Central de la República Argentina), se podrán establecer modalidades especiales, aunque sin diferencias en la informalidad del requerimiento. También el afectado puede optar por otros medios de intimación fehaciente como: *a)* carta documento; *b)* carta con aviso de entrega; *c)* telegrama; o bien, utilizar los medios técnicos que se dispongan (página en Internet; servicios on line; atención al consumidor; líneas telefónicas, siempre y cuando el interesado acredite la recepción del reclamo).

> ¿Puede ser formulada verbalmente la petición de acceso? Interroga Gils Carbó. Respondiendo que, la ley no indica nada, por lo tanto la petición verbal es aceptable y debe ser atendida sin formalidades. Si hay dudas sobre la accesibilidad del documento, el responsable del registro podrá requerir una petición formal para dejar constancia del acceso.[265]

Asimismo, quien requiera el acceso, tiene derecho a solicitar y obtener información de sus datos de carácter personal incluidos en ficheros automatizados, a través de cualquiera de los siguientes medios (siempre que la configuración o implantación material del fichero lo permita):

- Visualización en pantalla
- Escrito, copia o fotocopia remitida por correo a su domicilio, o retirado en el domicilio del requerido.
- Copia enviada por facsímil
- Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

En cualquier caso, la presentación debe completar los datos siguientes: *a)* nombre y apellido del interesado; *b)* fotocopia del documento de identidad, y en los casos que se admita la representación, el instrumento que lo acredite; *c)* petición clara y fundada sobre el alcance que tiene su pretensión; *d)* denunciar el domicilio a efectos de notificaciones o comunicaciones pertinentes, y *e)* todo otro dato disponible en el archivo requerido que sea útil para establecer, sin error posible, la identidad del titular que solicita el acceso a sus datos.

En conclusión, como dice la ley española, el derecho de acceso se configura con un contenido amplio, pues debe establecerse la facultad de la persona de requerir que se ponga en su conocimiento la existencia de datos personales que lo individualicen o lo hagan individualizable en registros y/o sistemas electrónicos, bases de datos, ficheros automatizados o sobre los que exista previsión de que vayan a ser automatizados. Para que ello resulte efectivo, deberá poder obtener dicha información por el medio que prefiera (dentro de determinados límites): soporte electrónico, papel, visualización en pantallas o cualquier otro medio como la consulta a través de una red de comunicación. Ello requiere la implementación de un sistema poco gra-

---

[265] GILS CARBÓ, ob. cit., p. 274.

voso (no obsta a ello que se cobre una tasa por consulta) en todas aquellas instancias públicas y privadas que tengan acceso a la citada información.

375. La legitimación procesal activa en el *habeas data*

375.1. España es uno de los países más avanzados en la defensa y protección de los derechos sobre los datos personales. La creación de una "Agencia de Protección de Datos" ha permitido elaborar una serie de reglas técnicas que actúan a modo de orientadores para el ejercicio de los derechos.

La petición de acceso a los archivos, así como los de rectificación y cancelación de datos son derechos de carácter personalísimos, condición que determina que sólo puedan ser ejercidos por el afectado frente al responsable del fichero.

Este debe acreditar su identidad frente al sujeto reclamado. Podrá, no obstante, actuar a través de mandatario cuando se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que el representante legal acredite tal condición.

La ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

La pretensión deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero y contendrá:

a) Nombre y apellido del interesado acreditado con la fotocopia del documento nacional de identidad y, en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación. La fotocopia del documento nacional de identidad podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.

b) Petición clara y fundada.

c) Domicilio a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos que respalden la pretensión.

e) El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

El reclamo siempre es gratuito, tanto para el derecho de acceso como para la rectificación, actualización o supresión de datos personales.

375.2. Esta limitación que tiene el modelo español, aunque haya sido fuente de muchas leyes latinoamericanas, no ha tenido pleno seguimiento, en la medida que hay países como Argentina que habilitan y expanden la legitimación procesal, y otros que la restringen aun más, como el caso de México que la relaciona los datos protegidos con la vida humana, de modo que muerta la persona cesa la protección legal.

Pero hay también otra división que atiende la legitimación para obrar según el objeto que se pretenda. Diferentes son los requisitos si uno persigue el "derecho de acceso" a las fuentes de información; o se quiere un "control sobre la base de datos", o es otra la intención.

La línea expansiva atiende al derecho de "autodeterminación informativa" como una garantía de protección que es posible de transmitir a herederos y cesionarios, donde se reproduce la idea de conservar el derecho a una imagen sin máculas por información posterior a la desaparición de la persona física o jurídica.

La posición restricta, en cambio, lo considera como un medio procesal para proteger la intimidad de las personas que posibilita el acceso del interesado a los archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos —sean estos públicos o privados— que contengan datos referentes a su persona en procura de obtener conocimiento de tal información y poder así asegurar su exactitud, o rectificarla en caso de inexactitud o falsedad. Lo que intenta esta figura es evitar situaciones de afectación directa.

375.3. Asimismo las leyes suelen diferenciar entre personas físicas que pueden reclamar y personas jurídicas que logran hacerlo cuando cumplen ciertas condiciones. Por ejemplo, en Argentina la ley 25.326, habla de "toda persona" y "personas de existencia ideal" derivándose que ambos tienen legitimación para obrar.

Después, con el fallo dictado en la causa "*Halabi*".[266] dio permiso a la acción de clase, alegando que, si la regla general en materia de legitimación es la representación por el afectado, cuando se trata de derechos de incidencia colectiva que tienen por objeto bienes colectivos (art. 43 de la Constitución Nacional), ellos se pueden defender por el Defensor del Pueblo de la Nación, las asociaciones que concentran el interés colectivo y también por uno de los afectados.

> En estos supuestos existen dos elementos de calificación que resultan prevalentes. En primer lugar, la petición debe tener por objeto la tutela de un bien colectivo, lo que ocurre cuando éste pertenece a toda la comunidad, siendo indivisible y no admitiendo exclusión alguna. Por esta razón sólo se concede una legitimación extraordinaria para reforzar su protección, pero en ningún caso existe un derecho de apropiación individual sobre el bien ya que no se hallan en juego derechos subjetivos. No se trata solamente de la existencia de pluralidad de sujetos, sino de un bien que, como el ambiente, es de naturaleza colectiva. Es necesario precisar que estos bienes no tienen por titulares a una pluralidad indeterminada de personas, ya que ello implicaría que si se determinara el sujeto en el proceso éste sería el titular, lo cual no es admisible. Tampoco hay una comunidad en sentido técnico, ya que ello importaría la posibilidad de peticionar la extinción del régimen de cotitularidad. Estos bienes no pertenecen a la esfera individual sino social y no son divisibles en modo alguno. En segundo lugar, la pretensión debe ser focalizada en la incidencia colectiva del derecho. Ello es así porque la lesión a este tipo de bienes puede tener una repercusión sobre el patrimonio individual, como sucede en el caso del daño ambiental, pero esta última acción corresponde a su titular y resulta concurrente con la primera.

De tal manera, cuando se ejercita en forma individual una pretensión procesal para la prevención o reparación del perjuicio causado a un bien colectivo, se obtiene

---

[266] CS, 2009/02/24, Fallos, 332:111.

una decisión cuyos efectos repercuten sobre el objeto de la *causa petendi*, pero no hay beneficio directo para el individuo que ostenta la legitimación.

En este tipo de supuestos, la prueba de la causa o controversia se halla relacionada con una lesión a derechos sobre el bien colectivo y no sobre el patrimonio del peticionante o de quienes éste representa. Puede afirmarse, pues, —dice la Corte Suprema de Justicia de la Nación Argentina— que la tutela de los derechos de incidencia colectiva sobre bienes colectivos corresponde al Defensor del Pueblo, a las asociaciones y a los afectados, y que ella debe ser diferenciada de la protección de los bienes individuales, sean patrimoniales o no, para los cuales hay una esfera de disponibilidad en cabeza de su titular.

375.4. La cuestión debe ser vista en cada país en particular. En *Bolivia,* la Constitución Política del Estado vigente antes de la última reforma, cambió el *nomen juris* del *habeas data* por el de *acción de protección de la privacidad*, pero no así su esencia tutelar.

Contempla algunos cambios específicos en cuanto a su redacción, en especial el art. 130.I, en el que se refiere a los casos de legitimación activa que si bien es muy similar al texto del art. 23.I de la constitución abrogada, tiene una diferencia notoria cuando afirma:

> …Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la acción de protección de privacidad.

De allí que se observa, en primer lugar, que se añaden a las personas colectivas como posibles legitimados activos, o futuros accionantes, concibiendo que las personas colectivas también tienen acceso a los derechos reconocidos, que son: derecho a la intimidad, a la privacidad, honra, propia imagen y dignidad.

En consecuencia, se entiende que al reconocer como probables demandantes a personas colectivas, se refiere a aquellas de orden público como privado, pero con algunas diferencias en cuanto a los derechos tutelados para éstas; es decir, que las personas colectivas no podrán aducir la vulneración de su derecho a la intimidad personal y familiar, que son derechos fundamentales de índole personal, pero si podrían denunciar la vulneración de sus derechos a la imagen, y reputación.

Los derechos, si bien no está expresamente proclamado en el catálogo previsto por el art. 7 de la Constitución, sí lo está en los arts. 12 de la Declaración Universal de Derechos Humanos; 5 de la Declaración Americana de Derechos y Deberes del Hombre; 17 del Pacto Internacional de Derechos Civiles y Políticos; y 11 de la Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica, que son fuentes de la constitución política.

Otra diferencia consiste en la inclusión de la letra “o” en las siguiente frases: “Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida

de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la acción de protección de privacidad"; la letra "o", según el Diccionario de la Real Academia de la Lengua Española, tiene tres diferentes significados: En primer lugar puede denotar diferencia, separación o alternativa entre dos o más personas, cosas o ideas, cuando es utilizada como una conjunción disyuntiva (Antonio o Francisco); en su segundo significado puede ser utilizado ante cada uno de dos o más términos contrapuestos (blanco o negro); en su tercera acepción denota equivalencia significando "o sea, o lo que es lo mismo", acepción que este Tribunal adoptará para interpretar la parte final del art. 130.I, debido a que el sentido en esta ultima frase tiene como objetivo el definir una idea común y no denotar diferencias o ideas contrapuestas; por lo que el objeto de este artículo no cambia en cuanto a lo que estaba prescrito en la Constitución abrogada.

En suma, la acción de protección de privacidad tiene las mismas características que tenía el recurso del *habeas data* previsto en la constitución abrogada, por lo que se hace necesario establecer si la jurisprudencia del Tribunal Constitucional emanada de la interpretación de la naturaleza jurídica y objeto de protección de esta acción tutelar es o no compatible con el nuevo emplazamiento y aplicable dentro del nuevo marco constitucional.

En tal sentido, partiendo de los conceptos referidos, se puede inferir que el *habeas data* es una garantía constitucional por lo mismo se constituye en una acción jurisdiccional de carácter tutelar que forma parte de los procesos constitucionales previstos en el sistema de control de la constitucionalidad. Es una vía procesal de carácter instrumental para la defensa de un derecho humano como es el derecho a la autodeterminación informática.

Como una acción tutelar, el *habeas data* sólo se activa a través de la legitimación activa restringida, la que es reconocida a la persona afectada, que puede ser natural o jurídica. En consecuencia, no admite una activación por la vía de acción popular, es decir, no se reconoce la legitimación activa amplia.

Se ha dicho que:

> […] La legitimación activa del *habeas data* recae en la persona natural o jurídica -aunque el precepto constitucional no lo determina de esa manera en forma expresa, se entiende que dentro de la protección de este recurso se puede y debe abarcar tanto a las personas físicas como a las jurídicas, de quienes también se pueden registrar datos e informaciones- respecto de la cual la entidad pública o privada haya obtenido y tenga registrados datos e informaciones que le interesen a aquella conocer, aclarar, rectificar, modificar, o eliminar, y que no haya tenido respuesta favorable por la citada entidad para lograr esos extremos (TC de Bolivia, sentencia 027 del 3 de mayo de 2010).

375.5. En *Brasil*, el derecho es en apariencia amplio cuando se lee que puede ejercerlo cualquier nacional o extranjero residente; más apenas se lo ve en funcionamiento la restricción es inmediata porque se considera que es un derecho perso-

nalísimo que no debe confundirse con la amplitud que se concede para un derecho similar pero asimétrico, como es el derecho a la información.

La demanda se plantea contra el propietario del banco de datos, sin aclarar si ocupa a registros públicos y privados, o solo a los primeros. Toda pretensión se debe llevar con abogado.

375.6. En *Chile* cualquier persona afectada, y en consecuencia, también los herederos y causahabientes, pueden reclamar en los términos de la ley 19.628, al responsable del registro o banco de datos, que puede ser una persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.

El artículo 23 deja en claro que, la persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez.

El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

375.7. En *Colombia,* la ley alcanza a las bases de datos públicas como privadas, sin que se afecten aquellas que tienen por finalidad resguardar con la información almacenada, la seguridad del Estado y el orden interno.

Los registros públicos a cargo de las cámaras de comercio se rigen exclusivamente por las normas y principios consagrados en las normas especiales que las regulan y también quedan exceptuados aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales.

El artículo 15 de la Constitución reconoce, entre otros, el derecho de *habeas data*, entendido éste como la facultad que tienen las personas de "conocer, actualizar y rectificar las informaciones que se hayan registrado sobre ellas en bancos de datos y en archivos de entidades públicas y privadas". Es, además, un derecho fundamental autónomo que busca equilibrar las condiciones entre el sujeto de quien se informa y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo.

En estas condiciones, el *habeas data* se concibe como un derecho de doble vía, pues si bien es cierto que los usuarios pueden conocer, actualizar y rectificar las informaciones que de ellos se tiene sobre el cumplimiento de sus obligaciones, también lo

es que las instituciones y el resto de la sociedad tienen derecho a conocer la solvencia económica de sus clientes, más aún por tratarse de asuntos de interés general.

En otras palabras, supone la facultad de "conocer e incidir sobre el contenido y la difusión personal que se encuentra archivada en bancos de datos" y, paralelamente, significa que esa información debe ajustarse a ciertas exigencias mínimas.

Ahora bien, en paralelo con esta amplitud de encuadre, surge la necesidad de atender aquellos aspectos que se relacionan con los datos en sí mismo respecto de aquellos que, aplicados en una base de información, afectan la honra y el buen nombre de las personas.

Tal cuestión pone dudas sobre el derecho de impugnación, pues si queda asentado como un derecho personalísimo, solo el afectado tendría legitimación; mientras que si el control es para que se cumplan los principios de la protección de datos personales, el reclamo tiene mayores incumbencias.

La veracidad implica una correspondencia entre el registro efectuado y las condiciones empíricas del sujeto pasivo. La imparcialidad supone que ninguno de los intervinientes en el proceso de suministrar, registrar y divulgar la información, persiga un fin ilegítimo, ya sea par obtener provecho indebido o para causar un agravio injustificado a otra persona. Por último, cuando se exige información completa y suficiente, quiere advertirse sobre la necesidad de dinamizar el proceso cognoscitivo para evitar que la información se reciba en forma sesgada o sugestiva.

La Corte Constitucional ha dicho que el derecho de *habeas data* adquiere relevancia en el ámbito de las relaciones comerciales y financieras. Las entidades bancarias y las centrales de información desempeñan aquí un papel central, las primeras al momento de reportar la situación de sus clientes; las otras, en el registro, actualización y divulgación de la información. Cualquier anomalía, por pequeña que parezca, puede afectar gravemente los derechos no solo de un cliente o de un deudor, sino de todo aquel que pretenda hacer uso de los datos puestos a su disposición, más aún tratándose de personas que se encuentran en situación de indefensión.

Tal emplazamiento significa que el perjudicado tiene derecho de acceso y control, pero ¿qué pasa después de la muerte de la persona?

Es evidente que el deceso no impide que se informe el comportamiento financiero del pasado, el que puede continuar divulgado de manera indefinida a través de una base de datos. La difusión de este tipo de información afecta el buen nombre y la memoria de quien aparece reportado como deudor incumplido después de su fallecimiento, pero igualmente lesiona la intimidad y la buena reputación de su familia, ya no sólo por ver expuesta de manera indefinida una información negativa sobre uno de sus miembros, que ya no está ahí para defenderse de ella, sino en la medida en que tales datos puedan llegar a ser utilizados para elaborar el perfil de riesgo crediticio de los herederos de la persona que permanece o es reportada tras su muerte como deudora.

Ello en tanto la información que se tenga sobre las deudas insolutas de una persona fallecida, puede influir en el juicio que se haga acerca de la solvencia económica y la capacidad de pago de quienes están llamados a sucederla en sus derechos y

obligaciones. En consecuencia, la legitimación de los herederos y causahabientes se suma a la del afectado, quienes pueden a través de la tutela, perseguir la rectificación de la información que causaba agravio a la intimidad y honra de la persona y a la de su familia.

En definitiva, aún cuando los datos relativos al historial crediticio de una persona no forman parte de la esfera más íntima de la vida privada, sino que aluden a un aspecto importante de su interacción social, no por ello dejan de estar protegidos por el derecho a la intimidad, de modo tal que es, en principio, cada persona la única facultada para decidir a quiénes y con qué alcance revela su situación financiera. Tal reserva sólo puede levantarse cuando el Estado ejerce su potestad inquisitiva en el trámite de las investigaciones que constitucional y legalmente le corresponde adelantar o, en el ámbito de las bases de datos crediticias, cuando el propio individuo ha autorizado de manera expresa ser reportado a ellas y sólo para los fines que justifican la existencia de dichas centrales de información. Así las cosas, cuando una persona establece con otra una relación crediticia, la parte acreedora adquiere el derecho a obtener el pago de su crédito, pero no a dar a conocer, salvo que medie consentimiento expreso, la condición de deudor de su contraparte; tal información, pese a enmarcarse en el ámbito de una relación jurídica entre particulares, aún forma parte de la vida privada del deudor.[267]

375.8. Veamos cuál es la situación en *Ecuador*. Toda persona, según el art. 94 de la Constitución Política de la República, 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 propósito. Teniendo como base este derecho consagrado en la Constitución, puede solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación, anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.

El objeto del *habeas data* es proteger el buen nombre, honor, dignidad, buena fama de la persona, y de sus bienes. Concede el derecho a conocer los documentos, bancos de datos o informes que existan sobre su persona o bienes. Y concede, finalmente el derecho a solicitar al funcionario correspondiente, la actualización, rectificación, eliminación o anulación si fueren erróneos o cuando afectaren ilegítimamente sus derechos. Mas no puede servir como diligencia preparatoria para la iniciación de un proceso, o para la anulación o eliminación de una obligación, o para afectar el sigilo profesional, o para obstruir la acción de la justicia, o para conocer documentos que sean catalogados como de seguridad nacional, o para eliminar datos o informes que deben mantenerse en archivos públicos o privados.

Cuando se trata de fuentes de información comercial, los clientes de los burós y cualquier otra persona que por diversas causas lleguen a tener acceso a reportes emitidos por esas bases (incluyendo a funcionarios, empleados, agentes, entre otros), deberán obligatoriamente guardar confidencialidad sobre la información contenida en ellos, siendo prohibido utilizarla para fines distintos del análisis de riesgo crediticio.

---

[267] Corte Constitucional, expediente T – 1628346, del 27 de septiembre de 2007.

Quien empleare o divulgare indebidamente la información contenida en un reporte de crédito o alterare la información proporcionada por la fuente, estará sujeto a las sanciones establecidas en el artículo 201 del Código Penal, sin perjuicio de las acciones y responsabilidades civiles a las que hubiere lugar.

375.9. En *Paraguay* se aplica un principio inverso. Si todas las personas pueden tener archivos con datos personales para uso particular, cuando ellos se difunden o comunican a terceros, cualquiera sea el afectado o concernido, y haya o no daño cierto, cuentan con legitimación para denunciar el desvío legal. De allí que el campo operativo es limitado.

En *Perú*, también se prevé una legitimación activa restringida para la interposición del *habeas data*; es decir, únicamente tiene legitimación el afectado, en razón de que nadie más que el propio interesado —se dice— puede saber si se le transgrede su derecho constitucional. Ello se puede advertir del contenido de los arts. 61 al 65 previstos en el Código Procesal Constitucional del Perú, promulgado mediante Ley 28.237, el 31 de mayo de 2004.

375.10. La ley *uruguaya* establece en el art. 14 (derecho de acceso), la posibilidad de todo titular de datos personales, que previamente acredite su identificación con el documento de identidad o poder respectivo, para obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico.

Cuando se trate de datos de personas fallecidas, el ejercicio del derecho al cual refiere este artículo, corresponderá a cualesquiera de sus sucesores universales, cuyo carácter se acreditará por la sentencia de declaratoria de herederos.

En cuanto al derecho de rectificación, actualización, inclusión o supresión, le corresponde a toda persona física o jurídica que puede solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular.

El responsable de la base de datos o del tratamiento deberá proceder a realizar la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin en un plazo máximo de cinco (5) días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar de las razones por las que estime no corresponde.

El incumplimiento de esta obligación por parte del responsable de la base de datos o del tratamiento o el vencimiento del plazo, habilitará al titular del dato a promover la acción de *habeas data* prevista en la ley.

375.11. En cambio, cuando se trata de ejercer acciones de control, debemos identificar cada una de ellas para derivar la legitimación correspondiente.

Si el caso fuera *conocer la información*, los probables intereses serían: *a)* saber sobre la formación y existencia de los bancos de datos; *b)* tomar conocimiento del

acopio informativo personal que se tenga, y *c)* la finalidad o destino que tienen esos registros.

La norma constitucional, como se dijo, vincula el conocimiento con la finalidad de ellos, circunstancia que demuestra la necesidad de acreditar algo más que un interés sobre los archivos, debiendo el demandante fundamentar las razones que entiende lo habilitan para ser informado de las fuentes y los objetivos que con los datos levantados se persigue.

El derecho a saber su incorporación en una base de datos, ocupa también a dar noticia permanente sobre la permanencia.

La forma como se conocen los datos puede ser voluntaria, en cuyo caso estamos fuera del marco que precisa el *habeas data*; o provocada, a través de las acciones judiciales pertinentes que al efecto se encaminen.

La información directa se brinda a través de la consulta en los ficheros, o visualizándolos si estos fueran telemáticos o informáticos. En cambio, es indirecta cuando se obtiene mediante escrito, copias, fotocopias u otro medio similar que no requiera el uso de dispositivos mecánicos específicos.

Para Velázquez Bautista:

> la ejecución del derecho de acceso conlleva una serie de exigencias o deberes, que realizan tanto el titular de la base de datos como el del derecho. Es la obligación de comunicar los datos encontrados al titular del derecho de acceso, comunicación que, según especifican las leyes de protección de datos, deber realizarse en forma comprensible, es decir, de manera que pueda entenderse.[268]

El libre ingreso a los archivos informáticos o manuales puede limitarse cuando existan situaciones de reserva o secreto, o la difusión provoque inseguridad en las instituciones o, el mismo Estado atraviese por circunstancias de excepción (estado de sitio, por ejemplo).

375.12. Si la pretensión fuera de *control sobre las bases de datos*, la cuestión reconoce variantes. Desde la óptica de las acciones tendientes a dar eficacia al control, las pretensiones se desglosan.

La necesidad de saber sobre datos personales que se ingresan en bancos de información públicos o privados constituye un aspecto del derecho a la información que no puede ser contrariado sin dar excepciones válidas o razonables.

Es el derecho de acceso que señalamos en el punto anterior, el cual se puede incoar ante el archivo, es decir, directamente al registro que lo contiene, y facultativamente, a través del *habeas data*, ante la renuencia de los organismos a suministrar la información que se pide, o por intentar el reclamo como acción directa.

En algunas legislaciones, el impedimento o la obstaculización del ejercicio al derecho de acceso o la negativa a facilitar los datos que se solicitan, son causales graves que pueden llevar a la sanción de los funcionarios, o a cancelar la autorización para tener sistemas informáticos de almacenamiento.

---

[268] VELAZQUEZ BAUTISTA, ob. cit., p. 166.

375.13. La facultad de requerir la *cancelación o la corrección* de los datos inexactos, otorga el denominado derecho al olvido, esto es, el principio a tenor del cual ciertas informaciones (*v. gr.:* antecedentes penales prescriptos) deben ser eliminadas de los archivos transcurrido un determinado espacio de tiempo desde el momento en que acaeció el hecho a que se refieren, para evitar que el individuo quede prisionero de su pasado.

La corrección de los archivos puede efectuarse por el mismo sistema que los contiene, sea ya por la aclaración que formule el individuo, o por la información corroborada por la base de datos.

Estos organismos de registración, públicos o privados, generalmente pueden oponerse a las rectificaciones cuando ellas se promueven por quienes no son directamente interesados; excepción hecha de las pretensiones sostenidas por personas que invoquen un legítimo interés y la conservación de los datos les provocare riesgos o daños inminentes.

375.14. En cambio, si la idea es *actualizar los datos registrados*, debe acreditarse la inutilidad de los trámites administrativos dirigidos a obtener el pedido. De otro modo se llevan a la justicia cuestiones de naturaleza administrativa que harían de la función jurisdiccional un auténtico notariado.

Un supuesto más a considerar es el *derecho de rectificación o respuesta* con relación al *habeas data*.

El derecho a réplica, también conocido como derecho de rectificación y respuesta, que no se encuentra aun legislado en el ordenamiento positivo, tiene no obstante, plena captación a través del "bloque de constitucionalidad" que significan los tratados incorporados en el artículo 75 inciso 22. Particularmente, la Convención Americana sobre Derechos Humanos norma en el art. 14 que:

> Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.

La dimensión del problema se vincula con la difusión que pueden hacer los medios de prensa, de datos que conozcan sobre ciertas personas y los reproduzcan en una nota periodística, causándoles perjuicios.

El artículo 43 de la Constitución Nacional Argentina, y el agregado final que tiene el artículo 1º de la ley 25.326, disponen que "no podrá afectarse el secreto de las fuentes de información periodística", dejando en claro que el *habeas data* no se puede utilizar como remedio alternativo para el derecho de réplica.

En los hechos la norma le otorga a la prensa, *lato sensu*, la posibilidad de escudarse tras este derecho al secreto profesional, evitando revelar las fuentes donde obtuvo los datos que publica o difunde.

Pero el sujeto interesado debe tener, entonces, una vía útil y efectiva para conocer los registros que de él se tienen, así como para rectificarlos, actualizarlos o pedir su anulación.

Si no los tiene, existe una omisión inconstitucional.

La coincidencia entre las disposiciones aparece en la "información inexacta", pero la diferencia estriba en los motivos que acuden para fundar una u otra pretensión.

Mientras el derecho a réplica supone obtener un medio equivalente al que difunde o reproduce un dato equívoco que nos agravia para perseguir su correcta exposición; el derecho de rectificación presente en el *habeas data* concierne al derecho de acceso a los bancos de datos para lograr cualquiera de las pretensiones a que ya hicimos referencia.

> De esta manera, dice Velázquez Bautista, se configura el derecho de rectificación aplicado a los servicios de información electrónica como una garantía más, un plus, que coadyuvar a proteger los bienes involucrados en un tratamiento automatizado de datos de carácter personal, que pueden lesionarse con la difusión de datos inexactos a través de los servicios de información periodística, situación que ya se ha dado en la práctica.[269]

Para nosotros es preciso reconocer en el que peticiona algún derecho o interés vinculado con lo que está reclamando.

Por ejemplo, existe información totalmente privada que pertenece a la esfera de la intimidad y constituye un auténtico derecho al secreto absoluto. Esta, no puede ser difundida, aunque pudiera estar registrada (*v. gr.:* enfermedades psicosociales que informa una historia clínica). Mientras que otro tipo de registraciones eluden la condición de privacidad y se instalan en la dimensión de informaciones públicas que procuran una mejor administración del Estado (*v. gr.:* Registro Civil, Registros de la propiedad inmobiliaria o automotor, Policía Federal, Colegios, Universidades, Obras Sociales, Clubes, Compañías de Seguros, etc.), o el cumplimiento adecuado de ciertas obligaciones constitucionales (*v. gr.:* los registros en padrones).

Esta división pone de manifiesto que hay una esencial distinción entre el "titular" de los datos, y quienes los administran.

Bianchi explica que titular es el individuo porqué a él le corresponden y pertenecen; en tanto que los administradores son quienes poseen los bancos o registros que recopilan y ordenan tales datos.

> Estos últimos tienen cuatro obligaciones básicas: *a)* estar legitimados para haberlos obtenido; *b)* llevar un correcto registro, sin incurrir en falsedades, lo que incluye también su actualización; *c)* asegurar su confidencialidad y no proveer de información sino mediante autorización del titular o a requerimiento de autoridad competente; *d)* evitar su destrucción o deterioro.[270]

La distinción entre sujetos con legitimación activa y sujetos legitimados pasivamente es naturalmente obvia e imprescindible.

375.15. En conclusión:

a) En el "*habeas data*" destinado a *conocer la información* que se tiene registrada, la legitimación para obrar le corresponde a "toda persona", "todos los habitantes",

---

[269] VELAZQUEZ BAUTISTA, ob. cit., p. 166.

[270] BIANCHI, Alberto B., *Habeas data y derecho a la privacidad*, El Derecho, 161-866.

"todos los ciudadanos", o cualquiera otra persona física o jurídica (para utilizar algunas de las expresiones usadas en textos constitucionales o leyes reglamentarias) que proponga a un Juez el proceso.

Es un derecho a la información que no puede ser restringido por el "derecho subjetivo vulnerado" o el "interés legítimo a tutelar".

Esta libertad irrestricta proviene del carácter público que tiene la fuente informativa y de la condición expuesta de los datos (que en el caso se denominan "vacantes").

Ahora bien, como la norma constitucional relaciona el conocimiento con la finalidad del registro, es preciso que la persona que deduce la acción indique el motivo por el cual los solicita, para que una vez conocido, pueda concretar la supresión, rectificación, actualización o requerir la confidencialidad o reserva de aquellos.

Altmark y Molina Quiroga señalan que:

> la norma constitucional debió habilitar a toda persona a "tomar conocimiento de los datos a ella referidos y de su finalidad", y como consecuencia de este derecho establecer la vía procesal para hacerlo efectivo. Esperamos —agregan— que esta interpretación correctora sea en definitiva la que se imponga, ya que resultaría contradictorio que debiera acreditarse la existencia de "ilegalidad o arbitrariedad manifiesta" por parte del titular u operador del banco de datos para que se pueda ejercer los derechos de acceso a los datos de carácter personal.[271]

Elocuentemente se muestra de que manera la pretensión es compleja al fraccionar el objeto en dos motivos esenciales aunque dependiente el segundo del primero: *a)* conocer los datos o registros y, *b)* solicitar, en caso de información falsa o discriminatoria, alguna de las causas que posibilitan el *habeas data*.

No existirían problemas de intentar acciones independientes, pero como dijimos anteriormente, el Código procesal tiene otras vías para la pretensión, de modo que al proponer el *habeas data* como garantía subsidiaria, estaría postergada si el remedio propuesto en paralelo es más idóneo.

b) Si la intención fuese interponer *habeas data correctivo*, en cualquiera de sus posibilidades (rectificación o actualización), va de suyo que sólo quienes tengan el "interés" específico de la demanda tendrán legitimación procesal.

La noción de "interesado" expresa la idea según la cual, toda persona -física o jurídica- tiene un derecho subjetivo sobre la información relativa a sí misma, aun cuando tal información haya sido reunida por otras personas.

Desde luego, un *habeas data* puede ser mixto, en el sentido de comprender un objetivo simplemente exhibitorio, o pretender también actualizar, rectificar, reservar o excluir datos, concernientes a la información que obre en un registro.

En este cuadro se puede aceptar la legitimación para actuar de aquellos que continúen el interés procesal de la persona registrada, tales como los herederos forzosos (*v. gr.:* ascendientes y descendientes, los colaterales hasta un grado determinado, los afines y el cónyuge —salvo que estuviese divorciado).

---

[271] ALTMARK, *Molina Quiroga*, ob. cit., p. 67.

c) En el supuesto del *habeas data tendiente a lograr la confidencialidad*, reserva o directa exclusión de los datos registrados, se acentúa el carácter personalísimo y, por tanto, la necesidad de acreditar la relación procesal que se invoca.

Para iniciar la protección solicitada basta cumplir con los recaudos indicados en el párrafo anterior; pero lograr la sentencia favorable depende del tipo de registro que los contiene y del uso que de ellos se haga.

La finalidad del *habeas data* es impedir que en bancos o registro de datos se recopile información respecto de la persona titular del derecho que interpone el "amparo", cuando dicha información está referida a aspectos de su personalidad que estén directamente vinculados con su intimidad, no correspondiendo encontrarse a disposición del público o ser utilizados en su perjuicio por órganos públicos o entes privados, sin derecho alguno que sustente dicho uso.

Se trata, particularmente, de información relativa con la filiación política, las creencias religiosas, la militancia gremial, el desempeño en el ámbito laboral o académico, entre muchos otros objetivos.

La diferencia entre el secreto y la intimidad está presente en este capítulo. Obsérvese que quien deduce la demanda no es titular ni dueño del secreto que está registrado. Es el legitimado pasivo —el que opera el archivo— quien tiene el secreto, que al ponerlo en contacto con otros medios evita la ocultación y los expone ante otras personas, provocando, con ese acto de circulación, el perjuicio que habilita el *habeas data*.

También la amenaza de difusión permite la vía.

Por eso la intimidad le pertenece a un sujeto preciso y queda en él la reserva de sus derechos. En cambio, el secreto está proyectado a terceros que lo conocen y que se convierten en garantes de la confidencialidad.

A este respecto, dice Quintano que:

> la simple indiscreción no puede ser objeto de protección jurídica ni menos jurídico-penal, porque la criminalización de tal comportamiento daría al traste o dificultaría no pocos aspectos de la vida social. Lo que sí es claro es que no reviste tanta importancia saber si un secreto, para su titular, constituye realmente una materia digna de reserva, como saber si, efectivamente, ese secreto es digno de protegerse jurídicamente porque sea merecedor de tal protección. Naturalmente, siempre será digno de protección un secreto que, para la persona titular, sea digno de ella, habida cuenta de que la lesión produciría un perjuicio en la intimidad de dicha persona, si bien esta protección ya no alcanzaría la vía penal, sino la civil.[272]

376. La legitimación pasiva

376.1. Frente al derecho de las personas a conocer su inclusión en bancos de datos o cualquier archivo, se encuentra el derecho de los administradores o titulares de ellos, sean públicos o privados.

---

[272] QUINTANO RIPOLLÉS, Antonio, *Tratado de la parte especial de derecho penal,* editorial Madrid, 1972, pp. 155 y ss.

> Palazzi diferencia según se trate uno u otro registro, responsabilizando al funcionario que está a cargo del mismo cuando sea público; y al representante legal cuando sea privado. Puede suceder que el mantenimiento del registro o base de datos esté a cargo de un tercero especializado —caso de empresas de computación—, que puede llevar a integrar la litis con éste para que la resolución final le sea válidamente oponible, sobre todo en el caso de registros desactualizados o erróneos que hayan causado algún perjuicio económico o moral.[273]

Ellos tienen deberes que cumplir como es el derecho de acceso, pero también encuentran justificaciones para resistir las pretensiones, circunstancias que pone en cada modalidad de *habeas data*, variables en los legitimados pasivos correspondientes.

376.2. En Argentina el artículo 35 (Legitimación pasiva) especifica que: "La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes". Esta última condición: "destinados a proveer informes" limita notablemente el espectro de archivos incluidos.

En otros lugares el sujeto pasivo es quien tiene archivos con datos personales y no cumple con los imperativos conocidos como principios de "calidad de los datos" (*v. gr.:* Paraguay); también se restringe si son archivos públicos (México); o de información comercial (México), a diferencia de otros que los atrapan especialmente (*v. gr.:* Colombia).

376.3. Es verdad que todas las leyes comparadas producen un claro derecho de los registrados para reclamar acceso y control, pero está ausente en ellas resolver los problemas emergentes de la acumulación, tratamiento y distribución de los datos.

La condición para adquirir la calidad de sujeto pasivo depende de los datos almacenados y de la forma como se compilan. Una cosa es el archivo común que no tiene finalidades informativas, y otra muy distinta el registro ordenado y sistemático que tienen los bancos de datos.

La diferencia que se hace en Argentina entre "registros públicos y privados destinados a proveer información" es simplista, aunque efectiva a los efectos de lograr alguna precisión respecto a saber a quienes se puede demandar. Pero en los hechos, los registros públicos reconocen supuestos especiales, tales como los que menciona el artículo 23:

> 1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquéllos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.
>
> 2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o

---

[273] PALAZZI, Pablo, *El habeas data y el derecho al olvido,* en Jurisprudencia Argentina, semanario nº 6030 del 26 de marzo de 1997.

inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función del grado de fiabilidad.

3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

376.4. Inclusive, todos los ordenamientos jurídicos admiten la necesidad de establecer un cierto orden para clasificar los tipos de bancos de datos de acuerdo a la información que manejen y el destino que para ellos esté previsto.

Por ejemplo, la información sensible no se puede recolectar ni ser objeto de tratamiento, pero la iglesia católica, las asociaciones religiosas o las organizaciones políticas y sindicales pueden llevar un registro de sus miembros (art. 7 inciso 3º párr. final, ley argentina). Lo mismo cabe decir de los hospitales y demás instituciones sanitarias, públicas o privadas, y los profesionales vinculados a la ciencia médica que pueden recolectar y tratar los datos personales relativos a la salud física y mental de los pacientes que acudan a los mismos, o que estén o hubieren estado bajo tratamiento de aquéllos (art. 8, ley citada).

Los archivos privados, que no sean de estricto uso particular, tienen el mismo problema de adaptación a las reglas constitucionales. Así se observa en aquellos servicios destinados a la información crediticia, los que tienen fines publicitarios o estadísticos, entre otros.

Por ejemplo, se ha dicho que "los libros de comercio que posee un banco o entidad financiera no constituyen el supuesto constitucional de registros privados destinados a proveer informes" (*Cfr*. CNCom., Sala D, mayo 13/996 *in re* "Figueroa Hnos S.A. c/ Banco de la provincia de Santiago del Estero". Sin embargo, otros fallos opinan que "la vía del amparo informativo es el camino para ejercer la acción de *habeas data* a fin de que el Banco demandado corrija o suprima datos de sus registros y rectifique informes falsos que pudieran haberse proporcionado en su virtud".[274]

376.5. La información crediticia también juega la misma incertidumbre, porqué siendo bancos destinados a proveer información, algunos requieren para la procedencia del *habeas data* que los datos circulados sean falsos, erróneos, inexactos o discriminatorios, pues de otro modo, el archivo sólo cumple con la finalidad para la cual ha sido creado.

En síntesis, la calidad de sujeto pasivo del *habeas data*, con legitimación suficiente para actuar, solamente se obtiene del tipo de información que almacenan y del destino previsto para ellos.

Cuando la información no tiene fines informativos, la calidad procesal se difumina, aunque en todos los casos se deben resguardar el derecho de acceso para tomar conocimiento de los datos que a las personas interesadas concierne.

---

[274] Superior Tribunal de Justicia de Entre Ríos, sala 1ª penal, 1994/09/08, "*R.R.J.E., c/ Banco Francés del Río de la Plata*", ED, 164-413.

377. Los herederos y causahabientes

377.1. El problema de admitir la posibilidad de transmisión del derecho a proteger los datos personales de la persona fallecida, depende del criterio que se adopte para interpretar la vida privada tras la muerte de alguien. En México, como hemos dicho, la defensa de los datos personales se extingue con la desaparición física de la persona; no es igual en Argentina que le otorga derecho a los herederos y causahabientes.

De igual modo, si la tutela sobre la intimidad se establece como un derecho personalísimo, existirá la misma dificultad para admitir la demanda a través de una persona sucesora.

Para Estadella Yuste:

> *a priori* la respuesta debe ser negativa ya que no existe un derecho a la vida privada después de la muerte. Sin embargo, el caso es importante respecto a datos de carácter médico relativos a enfermedades hereditarias. Aunque en estos casos el argumento a favor del acceso por terceras personas es conveniente, porque el uso incorrecto de la información podría perjudicar la memoria o buen nombre del difunto.[275]

El caso es que la protección reglamentaria argentina admite la representación del derecho a través de los sucesores universales (*v. gr.:* arts. 14 inciso 4º y 34), lo cual no obsta a que se plantee la legitimidad de tal reconocimiento.

377.2. En realidad, el problema de la legitimación activa en los herederos no se puede analizar como si fuera una cuestión de resguardo a la vida privada del difunto, sino para observar cuales son los derechos *intuito personae* que tienen los sucesores universales.

> Bidart Campos explica que los muertos no prolongan los derechos que titularizaron en vida, ni siquiera como subsistentes en la memoria de sus deudos; los derechos de éstos podrán estar concatenados a los que fueron de la persona fallecida, pero serán derechos de quienes siguen viviendo, que se les reconocen en virtud del vínculo parental con el difunto.[276]

En efecto, el derecho de acceso es un derecho a estar informado. Es una garantía que no se puede limitar, pues para establecer presupuestos y condiciones están las modalidades que el *habeas data* plantea.

De todas maneras, cada pretensión de control sobre los bancos de datos (actualización, corrección, supresión o confidencialidad) permite extender la petición respectiva hacia otros campos de tutela, sin que ello signifique afectar el derecho subjetivo de quien fuera titular. Es decir, si los herederos plantean el acceso a los archivos y practicado verifican que los datos contenidos afectan la dignidad, el honor o la imagen del difunto, la pretensión que ellos deduzcan se podrá encarrilar por el

---

[275] ESTADELLA YUSTE, ob. cit., p. 273.

[276] BIDART CAMPOS, Germán J., *Tratado elemental de derecho constitucional argentino,* tomo VI, Ediar, Buenos Aires, 1995, pp. 123 y ss.

habeas data si es la vía idónea. Mientras que una demanda indemnizatoria, una reparación moral, un desagravio a la reputación o fama de la persona fallecida no se fundamenta en este proceso constitucional.

377.3. En este sentido, las leyes suelen dividir los caminos para la defensa de la intimidad, el honor y la imagen, evitando que se transite por el *habeas data*. El esquema no se toma de España que unifica el temperamento, debiéndose la diversidad a las propias reglas que nacen de los códigos civiles.

De allí que en Argentina, el *habeas data* se consagra en una causa judicial donde la defensa se hizo sobre una persona desaparecida sin que se encontraran obstáculos para ello.

> En la causa *Urteaga* se permitió que los parientes de un desaparecido, presuntamente muerto en las acciones militares sucedidas después de la revolución del 24 de marzo de 1976, pudieran demandar desde el *habeas data*, el conocimiento y la información que dispusieran los archivos militares sobre la citada persona.
>
> Comparte Bazán el fallo, agregando que el mismo resulta totalmente compatible con el derecho a la autodeterminación informativa que postula como bien protegible por medio del *habeas data*, pues el espectro de cobertura de aquel derecho incluye la posibilidad de conocer qué tipo de información (en este caso, perteneciente al hermano presuntamente fallecido del peticionario) existe en los archivos o bancos de datos (estatales, en este caso), para luego decidir someterla a un manto de confidencialidad o, a la inversa, hacerla pública.[277]

378. La representación y el mandato

378.1. La cuestión no es baladí porqué hay que recordar que la protección de los datos personales se concreta por etapas: una extrajudicial y otra, eventual e hipotética, judicial (*habeas data*, propiamente dicho).

Si la idea que pervive es tutelar la intimidad y evitar intromisiones indeseadas en la vida privada de las personas, la delegación hacia otros para conocer la información concernida puede resultar en sí misma contradictorio, al habilitar un acceso más a lo que se pretende conservar secreto o confidencial.

En nuestro parecer, el primer reclamo debe ser hecho por la persona afectada o que ostente un interés legítimo para ingresar al registro informativo, pudiendo discernir, en situaciones excepcionales —caso de incapacidad física o legal, impedimentos manifiestos, minoría de edad— la representación a un tercero. Este, a su vez, consigue legitimación por mandato, pero el acceso sólo podrá acordarse cuando actúe en interés y beneficio del afectado, y no para la satisfacción de intereses de terceros —padres, tutor, entre otros—.

> Esta es la conclusión de Estadella Yuste, quien agrega otro supuesto relacionado con la transferibilidad del título cuando un tercero pretende acceder al fichero en favor de una

---

[277] BAZÁN, Víctor, "El *habeas data* y sus particularidades frente al amparo", en *Revista de Derecho Procesal*, nº 4, Rubinzal Culzoni, Buenos Aires, 2000, pp. 215 y ss.

> persona que jurídica y físicamente es capaz, pero que por circunstancias especiales no puede ejercerlo. En este caso tampoco parecen existir disposiciones normativas que impidan el derecho de acceso a través de mandatario autorizado; no obstante siempre habrá que considerar lo previsto en las jurisdicciones nacionales, las cuales pueden determinar ciertas excepciones.[278]

378.2. En cambio, el acceso a la justicia requiere y exige patrocinio letrado, circunstancia que no cambia en los procesos constitucionales. Por eso, el planteo de *habeas data* supone, necesariamente, la deducción por abogado, calidad que cubre el recaudo de la representación legal.

Cabe aclarar que no todas las legislaciones coinciden en esta apreciación, porque algunos interpretan que la protección constitucional no exige asistencia letrada.

> Dice Velázquez Bautista que una situación diferente es aquella en la que el ordenamiento jurídico admite la posibilidad de actuar en nombre de otro, y ejercer el derecho de acceso mediante mandato, es decir, en nombre y por cuenta su titular. Ocasión en la que no se plantea que el titular se desprenda del derecho, sino, como tal, autoriza a otro para que acceda en su nombre. Esta opción debe establecerse con especial cuidado, especificando siempre quiénes son los que pueden actuar en este sentido. La primera cuestión que habría que plantear con respecto a lo anterior es en qué casos se podría proponer, así como quien, apoderado por el titular, en su nombre, accedería de forma efectiva a los datos. Esto podría contemplarse con ocasión de una enfermedad que conlleve la inmovilización permanente del paciente, una declaración de incapacidad, la desaparición del sujeto mientras transcurre el plazo legal que permite se proceda a la declaración de fallecimiento, etc. Estarán legitimados para acceder, según los casos, el calificado como tutor, el profesional del derecho al que se otorga el correspondiente poder, el padre, madre, cónyuge o hijos del desaparecido.[279]

378.3. Otro supuesto de legitimado pasivo que se demanda por representación son las personas jurídicas que titularizan (responsables) al archivo, registro, base o banco de datos.

En estos casos no hay problemas de acreditación pues basta con demostrar que la requerida no ha dado cumplimiento con las peticiones extracontenciosas (acceso y control) previamente interpuestas.

---

[278] ESTADELLA YUSTE, ob. cit., p. 274.

[279] VELAZQUEZ BAUTISTA, ob. cit., p. 166.

Sección 11ª ⋮ El *Habeas Data* en México

379. Antecedentes

379.1. En México, país federal, existen disposiciones especiales sobre protección de datos personales de manera reciente, aunque algunos estados federativos tienen legislaciones especiales de las que haremos referencia.

Antes de este desarrollo, el marco legal estuvo en la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* (en particular, el capítulo IV), y otras se desprenden de las normas infraconstitucionales que se incorporan al derecho interno.

La Convención Americana sobre Derechos Humanos, es una de ellas; dispone en el artículo 13 que: "Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole…", que lleva a sostener que:

> […] la libertad de expresión se concibe en un doble ámbito; por un lado la libertad para la expresión de ideas, y por otro el derecho a recibir información…El 30 de abril de 2002 el Congreso mexicano aprobó por unanimidad la nueva Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, la cual fue publicada en el *Diario Oficial de la Federación* el 11 de Junio del mismo año…La implementación y plena operación de la ley ha sido exitosa y los ciudadanos han podido no solo obtener información del quehacer gubernamental, sino que además han logrado tener acceso a su propia información.[280]

379.2. También se debe destacar la *Ley para regular las sociedades de información crediticia*, que dispone que ellas sólo podrán llevar a cabo las actividades necesarias para la realización de su objeto, incluyendo el servicio de calificación de créditos o de riesgos, el de verificación o confirmación de identidad o datos generales, así como las demás actividades análogas y conexas que autorice la Secretaría, oyendo la opinión del Banco de México y de la Comisión.

Las Sociedades, al ofrecer servicios de calificación de créditos o de riesgos a que se refiere el párrafo anterior, deberán considerar toda la información disponible en su base de datos sin discriminar la información proporcionada por cualquier usuario.

---

[280] Gómez Robledo, Alonso, Ornelas Núñez, Lina, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal,* UNAM, México, 2006, p. 4.

Se prevé expresamente el derecho del concernido en requerir acceso a las fuentes de información con el fin de consultar su historial crediticio, así como cuando envíen información relativa a la falta de pago puntual de cualquier obligación exigible.

Las Sociedades (buró de créditos) están sujetas a la inspección y vigilancia de la Comisión, a quien le deben suministrar la información y documentos que el Banco de México y la Comisión determinen mediante disposiciones de carácter general, con el fin de que cumplan con sus funciones, en términos de la ley que les corresponda.

Asimismo, tienen que proporcionar a dichas autoridades, en los plazos y a través de los medios que éstas establezcan, la información que requieran con el propósito de supervisión y divulgación estadística.

La base de datos de las Sociedades se integrará con la información sobre operaciones crediticias y otras de naturaleza análoga que le sea proporcionada por los Usuarios. Los usuarios que entreguen dicha información a las Sociedades deberán hacerlo de manera completa y veraz.

En caso de que la información proporcionada por el usuario sea relativa a una persona moral, deberá incluir a los accionistas o titulares de las partes sociales, según corresponda, que sean propietarios del 10% o más del capital social.

379.3. La *Ley General de Salud*, también contiene datos personales que se han de proteger, en cuanto refiere a la completa información que se debe dar al paciente y sus familiares, que por su naturaleza puede quedar inmersa dentro del ámbito de protección de los datos sensibles de carácter médico.

Finalmente, cabe agregar que existieron distintos proyectos presentados al Congreso de la Unión destinados específicamente a la protección de datos personales. Uno presentado por el diputado Jesús Martínez Álvarez (Convergencia), el 1º de diciembre de 2005; otro perteneciente al senador Antonio García Torres (PRI), del 2 de febrero de 2006; una más del diputado David Hernández (PRI), del 23 de febrero de 2006; y de la diputada Sheyla Fabiola Aragón Cortés (PAN) del 22 de marzo de 2006.[281]

379.4. Indirectamente hay normas federales que tienen algún derecho o principio de protección especial, como la *Ley de Información Estadística y Geografía*, (norma rectora del Instituto Nacional de Estadística Geografía e Informática), publicada en el *Diario Oficial de la Federación* el 30 de diciembre de 1980, que, en lo pertinente establece:[282]

- Que serán considerados como informantes (entre otras, las personas físicas y morales cuando les sean solicitados datos estadísticos y geográficos por las autoridades competentes);
- Que los datos que los informantes proporcionen con fines estadísticos serán manejados, para efectos de esta ley, bajo la observancia de los principios de

---

[281] Ver por todos: http:// www.senado.gob.mx/sgsp/gaceta; y http:// www.gaceta.diputados.gob.mx.

[282] Ver RAMÍREZ, Luis Manuel, "Protección Jurídica de Datos Personales. Situación en México", *Revista de Derecho Informático* (REDI), Alfa-Redi, diciembre 2001, núm. 41.

confidencialidad y reserva y no podrán comunicarse, en ningún caso, en forma nominativa o individualizada, ni harán prueba ante autoridad administrativa o fiscal, ni en juicio o fuera de el.

- Que la información estadística, a que se refiere dicha norma, sólo podrá proporcionarse a particulares, organismos o gobiernos extranjeros por conducto de la desaparecida Secretaria de Programación y Presupuesto (cuyas funciones fueron atraídas por la actual Secretaría de Hacienda y Crédito Público) o de las unidades que formen parte de los servicios nacionales, que hubieran sido autorizados por aquella, salvo la que en cumplimiento de otras disposiciones legales pueda proporcionarse.
- Que los informantes, podrán exigir, previa presentación de solicitud ante la misma autoridad que capturó la información registrada, que sean rectificados los datos que les conciernan, al demostrar que son inexactos, incompletos, equívocos u obsoletos, y denunciar ante las autoridades administrativas y judiciales todo hecho o circunstancia que demuestre que se ha desconocido el principio de confidencialidad de los datos o la reserva establecida por disposición expresa, en el ejercicio de las facultades que esta ley confiere a las unidades que integran los sistemas nacionales.
- Que para proteger los intereses del solicitante, cuando proceda, deberá entregársele un documento en donde se certifique el registro de la modificación o corrección.
- Que a las personas a quienes se les requieran datos estadísticos o geográficos deberán ser informadas de:
  - El carácter obligatorio o potestativo de sus respuestas;
  - Las consecuencias de la falsedad en sus respuestas a los cuestionarios que se les apliquen;
  - La posibilidad del ejercicio del derecho de rectificación;
  - La confidencialidad en la administración de la información estadística que proporcionen, y
  - La forma en que será divulgada o suministrada la información.
  - Cuales son los procedimientos y sanciones correspondientes a la infracción de las normas contenidas en esta ley.

379.5. En la *Ley Federal del Derecho de Autor*, se prevé la protección jurídica a las bases de datos, sin que la tutela alcance a los datos personales; pues en su caso, el acceso a información de carácter privado relativa a personas contenidas en los registros, así como la publicación, reproducción, divulgación, comunicación publica y transmisión de dicha información, requiere la autorización previa de las personas de que se trate.

Por último, la *Ley Federal de Protección al Consumidor,* reformada y adicionada por decreto publicado el 29 de mayo de 2001, en su artículo 76 *bis* fracciones I y II establece que el proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros provee-

dores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente; y que el proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos.[283]

380. Leyes de los Estados Federativos

380.1. El 21 de junio del año 2003, se publica en el periódico oficial del *Estado de Colima*, la primera Ley de Protección de Datos Personales. De ella se desprende el carácter de derecho humano fundamental que se reconoce a la preservación de información particular que esté registrada en cualquier soporte físico que permita su tratamiento, tanto por parte del sector público como privado dentro del Estado.

Se exceptúan de su aplicación: *a)* Los archivos mantenidos por personas físicas para actividades exclusivamente personales o domésticas; *b)* los archivos que sean

---

[283] RAMÍREZ, ob. cit., *passim*. Sostiene Aristeo García González que desde 1917, la Constitución Política de los Estados Unidos Mexicanos estableció derechos relativos a la libertad individual, de entre los que destacan la inviolabilidad de correspondencia y domicilio, y más adelante, el secreto a las comunicaciones privadas, que siendo derechos vinculados con la intimidad de la persona, que protegen ciertas áreas o espacios relativos a todo ser humano, no tuvo en cuenta —como fue obvio por el tiempo— el impacto tecnológico sobre las personas. No obstante, señala el autor que en materia de protección de datos personales, se han manifestado ciertas tutelas relacionadas pero en el ámbito sectorial (así destaca la ley Orgánica de la Administración Pública Federal [artículos 27 al 44], la ley de Información Estadística y Geográfica [artículos 32, 35, 39 al 47], el Código Fiscal de la Federación [artículos 30 y 69], la ley Orgánica de la Procuraduría General de la República [artículos 11 y 26], la ley Federal de Radio y Televisión [artículos 4, 6 y 58], ley Federal del Trabajo [artículo 544], la ley de Instituciones de Crédito [artículos 28, 117 y 118], el Código Federal de Procedimientos Penales [artículo 192], la ley de Población [artículos 98, 103-111 y 91], ley Federal contra la Delincuencia Organizada [artículos 15 al 28], y el Código Civil Federal [artículos 1916 y 1917].

El primer paso importante fue dado con la ley Federal de Transparencia y Acceso a la Información Pública en 2002, al establecer en su artículo 3, lo siguiente: [...] Para los efectos de esta Ley se entenderá por...[...] II. Datos personales: La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

Sin embargo, opina el profesor de Morelia [Michoacán] que dicha Ley hace sólo referencia a los datos personales sobre su uso y destino, por lo que en el caso del derecho a la intimidad es la exclusión de cierto tipo de datos que la persona quiere mantener reservada para sí misma. Lo que significa que la alusión que realiza la Ley de Acceso a la Información, en lo referente a los datos personales, es de forma y no de fondo. Por lo que podría considerarse que tanto el derecho a la intimidad como la protección de datos son derechos diversos.

En el año 2001 el primer proyecto de ley federal en esta materia, fue rechazado por el Pleno de la LVII Legislatura en diciembre de 2004. Quizás sea con el proyecto de reforma al artículo 16 de la Constitución de los Estados Unidos Mexicanos —siendo este el primer paso para alcanzar su consolidación— aprobada por el Senado —pendiente de aprobación por la Cámara de Diputados— cuando por fin vea la luz un nuevo derecho, el de toda persona a proteger sus datos personales.

considerados como clasificados por la ley; y *c)* los archivos establecidos para investigaciones penales. En este caso, el responsable del archivo deberá comunicar la existencia del mismo a la Comisión Estatal para el Acceso a la Información Pública, indicando sus características generales y su finalidad.

La Comisión Estatal para el Acceso a la información Pública, es la autoridad encargada de la aplicación del presente ordenamiento;

La norma creada sigue las líneas de la legislación española de 1999, que se advierte en los principios dispuestos en el artículo 4º que señalan:

> I. Sólo podrán obtenerse y ser sujetos de tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades expresas y legítimas para los que se hayan obtenido;
>
> II. No podrán usarse para actividades incompatibles a los propósitos para los que fueron obtenidos. No se considerará un uso incompatible el tratamiento posterior para fines estadísticos, históricos o científicos;
>
> III. Deberán ser correctos y actualizados, de modo que reflejen fielmente la situación del afectado;
>
> IV. No podrán ser guardados de modo que se identifique al interesado una vez que dejen de ser necesarios o pertinentes para la finalidad que les dio origen o haya concluido el plazo de conservación a que obliguen las leyes. Los reglamentos correspondientes indicarán de manera expresa los casos de excepción en que se autorice la conservación íntegra de ciertos datos, en virtud del valor histórico, estadístico o científico que pudieran tener;
>
> V. Deberá garantizarse el derecho de acceso por parte de los interesados para todos los archivos con datos que les correspondan;
>
> VI. Los datos deberán obtenerse en todos los casos por medios lícitos que garanticen el respeto a las garantías individuales y, especialmente, de los derechos al honor y a la intimidad de la persona a la que conciernen. No deberán obtenerse por medios fraudulentos, desleales, ilícitos o engañosos;
>
> VII. Previamente a su obtención, se deberá informar al interesado de manera completa y precisa sobre la existencia del archivo, su finalidad, el carácter obligatorio u optativo de la información que proporcione, las consecuencias del suministro de los datos o la negativa a hacerlo, la posibilidad de ejercer el derecho de acceso, rectificación, cancelación y oposición, así como la identidad y dirección del responsable del archivo;
>
> VIII. Cuando se obtengan por parte de terceros, el responsable del archivo, a través de los mecanismos que defina el reglamento correspondiente, dentro de los 60 días naturales siguientes notificará al interesado después de haber dado de alta los datos, a menos que exista legislación al respecto que indique otra medida o se trate de procesos para fines históricos, estadísticos o científicos, o cuando los datos provengan de fuentes accesibles al público;
>
> IX. Será necesario el consentimiento explícito e inequívoco del interesado para cualquier tratamiento de los datos de carácter personal. Se exceptúan los siguientes casos: *a)* Los previstos en la legislación; *b)* cuando impliquen datos obtenidos para la realización de las funciones propias de la administración pública en su ámbito de competencia; *c)* cuando se trate de los datos de las partes en contratos civiles, laborales, comerciales o administrativos; *d)* cuando se trate de datos disponibles en fuentes de acceso público; y *e)* cuando sean necesarios para el tratamiento médico del interesado.

X. El interesado podrá revocar el consentimiento mencionado en la fracción anterior, cuando exista una causa justificada y no tendrá efectos retroactivos;

XI. Los servidores públicos, profesionales, trabajadores y otras personas que por razón de sus actividades tengan acceso a archivos o datos de carácter personal, estarán obligados a mantener la confidencialidad de los mismos y a no darlos a conocer a terceros. Esta obligación subsistirá aun después de finalizar las relaciones que les dieron acceso a los datos. La contravención a esta disposición será sancionada de conformidad con la legislación penal; y

XII. Los datos personales relativos a la salud podrán ser operados por los profesionales e instituciones de acuerdo con la legislación sanitaria, pero conservando la confidencialidad de los mismos de acuerdo con la presente ley.

De igual modo, la reglamentación impone al responsable del archivo el deber de seguridad en el tratamiento y en la cesión de datos personales.

La importancia de la ley está en que pone claramente el lugar que le corresponde a la vía procesal de *habeas data*, que se instala como un derecho para solicitar y obtener gratuitamente información de sus datos de carácter personal y del origen de esos datos.

La persona no tiene exigencias rituales que cumplir, pues cuando se ve sometida a decisiones con efectos jurídicos o que le afecte, que se hayan basado exclusivamente en datos de carácter personal destinados a evaluar determinados aspectos de su personalidad, tiene abierto el proceso constitucional; donde inclusive, puede recibir una indemnización proporcional al daño o lesión ocasionada en sus bienes o derechos.

La ley, que es muy buena, comenzó a regir el 2 de marzo del año 2004.

380.2. En el *Distrito Federal* también rige una Ley de Protección de Datos, considerada de orden público e interés general, que tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los entes públicos.

Están alcanzados por la norma los archivos que poseen: La Asamblea Legislativa; el Tribunal Superior de Justicia; el Tribunal de lo Contencioso Administrativo; el Tribunal Electoral; el Instituto Electoral; la Comisión de Derechos Humanos; la Junta de Conciliación y Arbitraje; la Jefatura de Gobierno; las dependencias, órganos desconcentrados, órganos político administrativos y entidades de la Administración Pública; los Órganos Autónomos por ley; los partidos políticos, asociaciones y agrupaciones políticas; así como aquellos que la legislación local reconozca como de interés público y ejerzan gasto público; y los entes equivalentes a personas jurídicas de derecho público o privado, ya sea que en ejercicio de sus actividades actúen en auxilio de los órganos antes citados o ejerzan gasto público.

Siguiendo el modelo de otras legislaciones europeas, se explica el significado de los términos que ocupa la ley y se establecen los principios aplicables: a) *Licitud*, que consiste en que la posesión y tratamiento de sistemas de datos personales obedecerá exclusivamente a las atribuciones legales o reglamentarias de cada ente público y deberán obtenerse a través de medios previstos en dichas disposiciones. De allí que

los sistemas de datos personales no pueden tener finalidades contrarias a las leyes o a la moral pública y en ningún caso pueden ser utilizados para finalidades distintas o incompatibles con aquella que motivaron su obtención. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos; b) *Consentimiento,* referido a la manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de sus datos personales; c) *Calidad de los Datos,* que supone que deban ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Los datos recabados deberán ser los que respondan con veracidad a la situación actual del interesado; d) *Confidencialidad,* que persigue garantizar que exclusivamente la persona interesada puede acceder a los datos personales o, en su caso, el responsable o el usuario del sistema de datos personales para su tratamiento, así como el deber de secrecía del responsable del sistema de datos personales, así como de los usuarios.

Se aclara que los instrumentos jurídicos que correspondan a la contratación de servicios del responsable del sistema de datos personales, así como de los usuarios, deberán prever la obligación de garantizar la seguridad y confidencialidad de los sistemas de datos personales, así como la prohibición de utilizarlos con propósitos distintos para los cuales se llevó a cabo la contratación, así como las penas convencionales por su incumplimiento. Lo anterior, sin perjuicio de las responsabilidades previstas en otras disposiciones aplicables.

Los datos personales son irrenunciables, intransferibles e indelegables, por lo que no podrán transmitirse salvo disposición legal o cuando medie el consentimiento del titular y dicha obligación subsistirá aún después de finalizada la relación entre el ente público con el titular de los datos personales, así como después de finalizada la relación laboral entre el ente público y el responsable del sistema de datos personales o los usuarios.

El responsable del sistema de datos personales o los usuarios podrán ser relevados del deber de confidencialidad por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la seguridad nacional o la salud pública.

Se suma el principio de e) *Seguridad, q*ue consiste en garantizar que únicamente el responsable del sistema de datos personales o en su caso los usuarios autorizados puedan llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan; f) *Disponibilidad,* en cuanto que los datos deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del interesado; y g) *Temporalidad,* en el aspecto que los datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubiesen sido recolectados. Queda exceptuado el tratamiento que con posterioridad se les dé con objetivos estadísticos o científicos, siempre que cuenten con el procedimiento de disociación. Únicamente podrán ser conservados de manera integra, permanente y sujetos a tratamiento los datos personales con fines históricos.

La ley establece que para la integración, tratamiento y tutela de los sistemas de datos personales se debe realizar el procedimiento siguiente:

I. Cada ente público deberá publicar en la *Gaceta Oficial del Distrito Federal* la creación, modificación o supresión de su sistema de datos personales;

II. En caso de creación o modificación de sistemas de datos personales, se deberá indicar por lo menos:

a) La finalidad del sistema de datos personales y los usos previstos para el mismo;

b) Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos;

c) El procedimiento de recolección de los datos de carácter personal;

d) La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo;

e) De la cesión de las que pueden ser objeto los datos;

f) Las instancias responsables del tratamiento del sistema de datos personales;

g) La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición; y

h) El nivel de protección exigible.

III. En las disposiciones que se dicten para la supresión de los sistemas de datos personales, se establecerá el destino de los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción.

IV. De la destrucción de los datos personales podrán ser excluidos aquellos que, con finalidades estadísticas o históricas, sean previamente sometidos al procedimiento de disociación.

El sistema de inscripción permite conocer las bases de datos y especialmente sus finalidades.

Los datos especiales se protegen en el artículo 10 que dice:

Ninguna persona esta obligada a proporcionar datos personales considerados como sensibles, tal y como son: el origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual.

Queda prohibida la creación de sistemas de datos personales que tengan la finalidad exclusiva de almacenar los datos personales señalados en el párrafo anterior y sólo pueden ser tratados cuando medien razones de interés general, así lo disponga una ley, lo consienta expresamente el interesado o, con fines estadísticos o históricos, siempre y cuando se hubiera realizado previamente el procedimiento de disociación.

Tratándose de estudios científicos o de salud pública el procedimiento de disociación no será necesario.

El Instituto de Acceso a la Información Pública del Distrito Federal es el órgano encargado de dirigir y vigilar el cumplimiento de la presente ley, así como de las normas que de ella deriven; será la autoridad encargada de garantizar la protección y el correcto tratamiento de datos personales.

Tiene las atribuciones siguientes:

I. Establecer, en el ámbito de su competencia, políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales que

estén en posesión de los entes públicos, así como expedir aquellas normas que resulten necesarias para el cumplimiento de esta ley.

II. Diseñar y aprobar los formatos de solicitudes de acceso, rectificación, cancelación y oposición de datos personales.

III. Establecer sistemas electrónicos para la recepción y trámite de solicitudes de acceso, rectificación, cancelación y oposición de datos personales.

IV. Llevar a cabo el registro de los sistemas de datos personales en posesión de los entes públicos.

V. Elaborar y mantener actualizado el registro del nivel de seguridad aplicable a los sistemas de datos personales, en posesión de los entes públicos, en términos de esta ley.

VI. Emitir opiniones sobre temas relacionados, así como formular observaciones y recomendaciones a los entes públicos, derivadas del incumplimiento de los principios que rigen esta ley.

VII. Hacer del conocimiento del órgano de control interno del ente público que corresponda, las resoluciones que emita relacionadas con la probable violación a las disposiciones legales.

VIII. Orientar y asesorar a las personas que lo requieran acerca del contenido y alcance de la presente ley.

IX. Elaborar y publicar estudios e investigaciones para difundir el conocimiento de los datos personales.

X. Solicitar y evaluar los informes presentados por los entes públicos respecto del ejercicio de los derechos previstos en esta ley. Dicha evaluación se incluirá en el informe que de conformidad con el artículo 74 de la Ley de Transparencia y Acceso a la información pública presenta el Instituto a la Asamblea Legislativa del Distrito Federal y deberá incluir por lo menos:

a. El número de solicitudes de acceso, rectificación, cancelación y oposición de datos personales presentadas ante cada Ente Público, así como su resultado.

b. El tiempo de respuesta a la solicitud.

c. El estado que guardan las denuncias presentadas ante los órganos internos de control y las dificultades observadas en el cumplimiento de esta ley.

d. El uso de los recursos públicos en la materia.

e. Las acciones desarrolladas.

f. Sus indicadores de gestión; y

g. El impacto de su actuación.

XI. Organizar seminarios, cursos, talleres y demás actividades que promuevan el conocimiento de la presente ley y los derechos de las personas sobre sus datos personales.

XII. Establecer programas de capacitación en materia de protección de datos personales y promover acciones que faciliten a los entes públicos y a su personal participar de estas actividades, a fin de garantizar el adecuado cumplimiento de los principios que rigen la presente ley.

XIII. Promover entre las instituciones educativas, públicas y privadas, la inclusión dentro de sus actividades académicas curriculares y extracurriculares, los temas que ponderen la importancia del derecho a la protección de datos personales.

XIV. Promover la elaboración de guías que expliquen los procedimientos y trámites materia de esta ley.

XV. Investigar, substanciar y resolver el recurso de revisión en los términos previstos en esta ley y en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

XVI. Evaluar la actuación de los Entes Públicos, mediante la práctica de visitas de inspección periódicas de oficio, a efecto de verificar la observancia de los principios contenidos en esta ley, las cuales en ningún caso podrán referirse a información de acceso restringido de conformidad con la legislación aplicable.

XVII. Procurar la conciliación de los intereses de los interesados con los de los entes públicos, cuando éstos entren en conflicto con motivo de la aplicación de la presente ley; y

XVIII. Las demás que establezca esta ley, y demás ordenamientos aplicables.

381. La ley Federal de Protección de Datos Personales

381.1. El 5 de Julio del año 2010 se publica en el *Diario Oficial* el decreto por el que se expide la *Ley Federal de Protección de Datos Personales en posesión de particulares,* que reforma los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

A diferencia de los modelos que tienen los Estados federativos, la norma que tiene alcance nacional y se considera de orden público, solamente alcanza a los archivos de particulares, siempre que estén destinados al tratamiento de datos personales.

El nivel de protección se instala en la privacidad y en el derecho a la autodeterminación informativa en los términos como se explican en esta obra.

381.2. Los archivos privados se refieren a los que posean sujetos individuales, sean estas personas físicas o morales; más no incluye las bases de datos de entidades públicas que contengan informaciones privadas.

Expresamente se excluye a los burós de créditos cuando deba aplicarse la ley de regulación de sociedades de información crediticia; así como las personas que almacenan datos personales para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

En el primer caso, la excepción se fundamenta en la especialidad de la legislación aplicable cuya última reforma data del 25 de mayo de 2010 cuando se cambia la redacción de los artículos 3, 4, 6, cuarto párrafo; y se adicionan los artículos 4 Bis; 4 Bis 1; 4 Bis 2; 8, segundo párrafo; 13 Bis; 15 Bis; 19, segundo párrafo; 19 Bis; 43 Bis; 49, fracciones V, VI, VII y VIII; y 49 Bis, de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros.

En cuanto a los archivos de particulares para uso personal, la aplicación práctica de la ley de protección de datos personales difiere del modelo adoptado en otros lugares. En España, se inscriben ficheros de titularidad pública y privada, mientras que en México, los archivos privados de uso particular, no tienen que registrarse y menos aun, quedar alcanzados por los principios previstos.

No obstante, si ese archivo diera informes a terceros excedería el uso personal, y quedaría en el marco de la previsión normativa.

Archivo de uso personal, básicamente, es el banco de información que tiene para uso profesional o doméstico una determinada persona física o jurídica. Esos datos que almacena, pueden haberse obtenido directamente del cliente (titular de los datos) o del afectado, o lograrlos mediante procedimientos indirectos, o de fuentes accesibles al público; pero en todos los casos, con la obligación de mantenerlos en reserva y confidencialidad debido al carácter secreto que tiene su propio registro. Esta calidad que no emerge de la ley, surge de la propia aplicación que tiene la base de datos personal y exclusiva, toda vez que la información almacenada no se puede ceder ni ser transferir.

Además, un registro de esta naturaleza no está alcanzado por la ley, circunstancia que evita aplicarle los principios de proporcionalidad (tener sólo los datos necesarios para la actividad o el uso específico de carácter exclusivo), y de calidad de los datos en general.

Mientras que si decide darle a esa base informativa otro destino, y en particular la cesión a terceros, estará alcanzado por la ley como los demás archivos particulares, necesitando expreso consentimiento de las personas que hubiera guardado en el banco.

381.3. *Principios:* Los responsables en el tratamiento de datos personales, deberán observar los principios de *licitud*, *consentimiento*, *información*, *calidad*, *finalidad*, *lealtad, proporcionalidad* y *responsabilidad*, previstos.

Como se ha visto en los capítulos anteriores, los principios de protección de datos personales se pueden resumir en solo uno: "*Calidad de los datos*", pero en México, éste se entiende como integrante del conjunto y reducido a su particular alcance.

De ellos tiene especial importancia el *consentimiento,* pues todo tratamiento de datos personales depende de la autorización expresa del titular.

El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

> El consentimiento que preste voluntariamente el titular de los datos, debe ser libre, expreso e informado. Los resultados de cualquier análisis genético se deben formular dentro de los límites de los objetivos de la consulta, el diagnóstico o el tratamiento para el que se obtuvo el consentimiento. Cuando se trate de procesar datos médicos de una persona legalmente incapacitada que es incapaz de una decisión libre, y cuando la ley nacional no le permita actuar en su propia representación, es preciso obtener el consentimiento de la persona legalmente habilitada para actuar en interés de éste, o de la autoridad o persona u órgano designados por la ley con este fin. Si una persona legalmente incapacitada ha sido informada de la intención de recoger o procesar sus datos

médicos, sus deseos deben tenerse en cuenta, a menos que la ley nacional disponga otra cosa.[284]

El artículo 10 dispone que no será necesario el consentimiento para el tratamiento de los datos personales cuando: a) *esté previsto en una ley;* b) *los datos figuren en fuentes de acceso público;* c) *los datos personales se sometan a un procedimiento previo de disociación;* d) *tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;* e) *exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;* f) *sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o* g) *se dicte resolución de autoridad competente*.

Las excepciones se toman del modo como se asegura la reserva y confidencialidad de la información personal que suministra la persona concernida. Cuando los datos se consiguen de fuentes de acceso público es obvia la exclusión toda vez que resulta casi imposible controlar esta forma de almacenamiento; en cambio cuando los datos se "disocian" la excepción agrega indirectamente una obligación al titular del archivo, porqué le obligan a establecer encriptamientos a la información de forma que no se puedan relacionar con la simple compulsa del registro.

A diferencia de reglamentos, en Argentina, cuando se trata de información relacionada con la circulación de datos de salud en situaciones de necesidad o urgencia (salud pública, emergencia o estudios epidemiológicos) requiere que la persona no pueda identificarse; pero es un supuesto distinto al que considera en los casos de atención programada de enfermos físicos o mentales donde se prioriza el deber de secreto profesional; en el restante, se atienden cuestiones extraordinarias donde peligra el interés general.

381.4. *El aviso de privacidad*. Es éste un mecanismo propio de la legislación mexicana que la pone en la vanguardia de la protección procesal que persigue, especialmente, custodiar que los datos se almacenen con expreso consentimiento del titular.

El artículo 15 establece: "El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad".

La ley obliga a difundir y dar a conocer las actividades que realizan los archivos de datos personales. En este sentido, el aviso está pensado como un requisito de procedibilidad para proceder el procesamiento informativo con datos personales, siendo en consecuencia la comunicación al titular, una información necesaria e ineludible, basado en el principio de transparencia en la creación y funcionamiento de las bases de información personal.

---

[284] GOZAÍNI, *Derecho Procesal Constitucional – Habeas Data. Ley y Reglamentación,* cit., pp. 153/154.

Asimismo, el deber de información individual se cumple con el requerimiento de colaboración al titular de los datos, debiéndose comunicar inequívocamente los motivos para los que se piden datos personales, sin ocultar la finalidad y destino que a ellos se aplicarán.

Lo común en la recolección de datos es dar información al tiempo de pedir los datos personales, de modo tal que la forma como ella se ofrezca, va a depender de la manera como se practique el requerimiento. Por eso, el aviso de privacidad es posterior y no se instala en el momento de la recolección, sino después.

No olvidemos que en el tratamiento de datos personales, hay etapas que inician con el almacenamiento y continúa con las siguientes hasta la cesión local e internacional. En este sentido, si un fichero no informó oportunamente deberá hacerlo antes de la cesión, como mínimo, pues de otro modo violaría las disposiciones legales.

> ART. 18.—Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el cambio en el aviso de privacidad.
>
> No resulta aplicable lo establecido en el párrafo anterior, cuando el tratamiento sea con fines históricos, estadísticos o científicos.
>
> Cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados, en consideración al número de titulares, o a la antigüedad de los datos, previa autorización del Instituto, el responsable podrá instrumentar medidas compensatorias en términos del Reglamento de esta ley.

La información a prestar no debe ser asociada al consentimiento como resultado. Con esto se quiere expresar que los archivos, registros, base o banco de datos que funcionen, y aquéllos que vayan a crearse con finalidades específicas, podrán suministrar la comunicación informada a las personas contenidas mediante cualquiera de los mecanismos fehacientes que la ley autoriza: por escrito, medios electrónicos, telefónicos, de imagen, u otros medios idóneos al fin que deben alcanzar.

El consentimiento es el medio a conseguir, pero no legitima la ausencia de información previa. Por ello la ley dispone que el consentimiento pueda revocarse en cualquier tiempo, aun cuando no tenga efectos retroactivos (art. 8º párrafo final).

El aviso de privacidad deberá contener, al menos, la siguiente información (art. 16):

a) La identidad y domicilio del responsable que los recaba.

b) Las finalidades del tratamiento de datos.

c) Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos.

d) Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta ley.

e) En su caso, las transferencias de datos que se efectúen, y

f) el procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad.

En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

381.5. El procedimiento está pensado en sede administrativa. Comienza con el ejercicio del derecho de acceso que puede ser individual (pretensión simple) o estar completado con requerimientos de rectificación, cancelación u oposición.

La legitimación, como antes observamos, es del titular de los datos, quien puede conferir representación legal; pero muerto el titular se pierde el derecho de acceso y control.

No hay plazos para interponer la petición pues depende del tiempo que se considere o conozca la afectación por el uso de datos que le pertenecen y sobre los cuáles no haya prestado consentimiento.

381.6. La solicitud de acceso, rectificación, cancelación u oposición deberá contener y acompañar los requisitos previstos en el art. 29 que son: *a)* nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud; *b)* los documentos que acrediten la identidad o, en su caso, la representación legal del titular; *c)* la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y *d)* cualquier otro elemento o documento que facilite la localización de los datos personales.

En las *Instrucciones* dictadas para España se indica que el ejercicio de los derechos deberá llevarse a cabo mediante solicitud dirigida al responsable del fichero, que contendrá:

- Nombre, apellidos del interesado y fotocopia del DNI del interesado y, en los casos que excepcionalmente se admita, de la persona que lo represente, así como el documento acreditativo de tal representación.
- La fotocopia del DNI podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido en derecho.
- Petición en que se concreta la solicitud.
- Domicilio a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula, en su caso.

El interesado deberá utilizar cualquier medio que permita acreditar el envío y la recepción de la solicitud.

El responsable del fichero deberá contestar la solicitud que se le dirija, con independencia de que figuren o no datos personales del afectado en sus ficheros, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción.

En el caso de que la solicitud no reúna los requisitos especificados, el responsable del fichero deberá solicitar la subsanación de los mismos.

El responsable del fichero deberá adoptar las medidas oportunas para garantizar que todas las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

381.7. Recibida la petición, el responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes que los titulares presenten.

En el caso de solicitudes de rectificación de datos personales, el titular deberá indicar, además de lo ya señalado, las modificaciones a realizarse y aportar la documentación que sustente su petición.

El responsable comunicará al titular, en un plazo máximo de veinte (20) días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince (15) días siguientes a la fecha en que se comunica la respuesta. Tratándose de solicitudes de acceso a datos personales, procederá la entrega previa acreditación de la identidad del solicitante o representante legal, según corresponda.

Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso (art. 32).

381.8. La obligación de acceso a la información se dará por cumplida cuando se pongan a disposición del titular los datos personales; o bien, mediante la expedición de copias simples, documentos electrónicos o cualquier otro medio que determine el responsable en el aviso de privacidad.

En el caso de que el titular solicite el acceso a los datos a una persona que presume es el responsable y ésta resulta no serlo, bastará con que así se le indique al titular por cualquiera de los medios a que se refiere el párrafo anterior, para tener por cumplida la solicitud.

La respuesta al requerimiento de acceso que se menciona se refiere a la información que debe proporcionar el titular del archivo o responsable del mismo, cuando sea requerido en los términos de ley; en este supuesto, la contestación queda sujeta a iguales plazos de perentoriedad, y en la modalidad que se colija como la mejor.

Si el planteo se formula ante un archivo público, o privado destinado a dar informes, las vías para encausar la contestación son las que el interesado prefiera, es decir, copias simples, documentos electrónicos o cualquier otro medio que determine el responsable en el aviso de privacidad.

No obstante, el informe se responde *preferentemente* por el medio seleccionado, pero no *exclusivamente*, toda vez que depende de la configuración e implantación material del archivo.

La información se ha de proporcionar en un lenguaje simple, exento de codificaciones; es decir, que no puede haber respuestas que, al amparo de la confidencialidad que preservan, cumplan el requerimiento obligando al interesado a reglas de acceso técnico (*password*, claves, etc.) o aplicando sistemas crípticos ininteligibles por el afectado. Como antes se dijo, el contenido de la información a proporcionar ha de ser amplio y comprender la totalidad de datos que se tengan sobre el interesado, aun cuando el requerimiento solo comprenda un aspecto de los datos personales.

381.9. El responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos previstos por el art. 39: *a)* Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello; *b)* cuando en su base de datos, no se encuentren los datos personales del solicitante; *c)* cuando se lesionen los derechos de un tercero; *d)* cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el

acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y *e)* cuando la rectificación, cancelación u oposición haya sido previamente realizada.

La negativa a que se refiere este artículo podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular. En todos los casos anteriores, el responsable deberá informar el motivo de su decisión y comunicarla al titular, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes.

El derecho de acceso se confiere para que toda persona pueda tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos particulares de uso personal; la información que se proporciona, es la que consta en el archivo y se vincule en forma directa con el requirente, y por tanto, se establece que en ningún caso el informe podrá relevar datos pertenecientes a terceros, aun cuando se vinculen con el interesado. La revelación que se impide es sobre otras personas —individuales o ideales— que se encuentren en la base de datos, más no a los casos de información relacionada con terceros que, en su calidad de cesionarios, reportan información (por ejemplo, sobre situaciones de cumplimiento en las obligaciones) al archivo.

381.10. La entrega de los datos personales será gratuita, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos. Dicho derecho se ejercerá por el titular en forma gratuita, previa acreditación de su identidad ante el responsable. No obstante, si la misma persona reitera su solicitud en un periodo menor a doce meses, los costos no serán mayores a tres días de Salario Mínimo General Vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas.

El titular podrá presentar una solicitud de protección de datos por la respuesta recibida o falta de respuesta del responsable.

382. El procedimiento especial de *habeas data*

382.1. El *habeas data* mexicano no se presenta como un proceso constitucional, sino como administración de una herramienta fundamental para la protección de datos personales que se registran en archivos particulares, cuyo procedimiento se encamina ante el titular o responsable de la base de datos y, eventualmente continúa sustanciado ante el *Instituto Federal de Acceso a la Información y Protección de Datos*, a que hace referencia la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

382.2. La acción judicial vigente en otras latitudes, que se conoce como *habeas data* genérico, en México queda planteado como un reclamo administrativo de acceso a los archivos y deducidos los reclamos que contra el mismo se tuviere.

No obstante, la afirmación no se puede llevar al extremo de negar la acción procesal basándose en la necesidad de transitar por vías previas o paralelas, porque es preciso diferenciar a la garantía constitucional, propiamente dicha, del reclamo administrativo previo que constituye la etapa prejudicial.

En efecto, la tutela sobre los datos personales persigue afianzar el control sobre los bancos de datos desde una doble perspectiva: *a)* la del acceso libre y sin restricciones de la persona interesada y, *b)* del órgano especialmente creado para esos fines de vigilancia y fiscalización.

En primer término se ha previsto que el derecho de acceso se deduzca directamente al archivo que almacenó la información personal, para que una vez conocido se resuelva las acciones a seguir.

En segundo lugar, el órgano de control (INAF) tiene la función de velar por el cumplimiento de la ley específica e informar a las personas afectadas en sus derechos para asumir la representación de ellas o adoptar decisiones particulares con poderes suficientes derivados del poder que acreditan.

> En Argentina la ley diferencia el derecho de acceso, otorgando al titular de los datos, previa acreditación de su identidad, la posibilidad de obtener información directa de los archivos públicos o privados destinados a proveer informes; respecto al *habeas data* que asume como demanda judicial cuando se quiera tomar conocimiento de los datos personales almacenados o se pretenda la rectificación, supresión, confidencialidad o actualización. En caso alguno se establece la subsidiariedad y, por ello, no hay reclamo administrativo obligatorio expreso, aunque ello se desprende del art. 41 párrafo final de la ley.

382.3. En consecuencia, el procedimiento se cumple en primera instancia ante el archivo, registro, base o banco de datos; y en caso de negativa al acceso o al derecho de rectificación, actualización, supresión u ocultamiento (confidencialidad), la causa prosigue ante el Instituto que actúa como órgano de aplicación de la ley.

¿Significa este mecanismo que no hay actuaciones judiciales? La respuesta no puede ser, sino, alternativa de acuerdo con la eficacia de los resultados.

Desde un panorama comparado, el proceso constitucional de *habeas data* es la etapa judicial ineludible, al menos en alguna de estas situaciones*: a)* cuando el derecho de acceso o las acciones consecuentes se niegan en la vía prejudicial o, *b)* cuando es necesario obrar con urgencia acordando al *habeas data* un sentido eminentemente cautelar.

Cuando los bancos de datos no suministran información o directamente la niegan, el tránsito por la autoridad de aplicación parece ineludible, pero ¿podría el afectado intentar una demanda judicial?

Si se aplica la ley con rigor, la etapa no es prejudicial, sino el mecanismo propiamente articulado para la tutela de los datos personales, que en caso de provocar agravios en el interesado cuenta, contra las resoluciones del Instituto, con la posibilidad de promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

En cambio, si la norma se interpreta con amplitud, el *habeas data* puede tener una finalidad cautelar consistente en prevenir el mal uso de los datos y conseguir otras proyecciones defensivas que el derecho a la intimidad promete (*v. gr.:* honor, reputación, identidad, etc.).

382.4. *Del Procedimiento de Protección de Derechos.* Establece el art. 45 que:

> […] el procedimiento se iniciará a instancia del titular de los datos o de su representante legal, expresando con claridad el contenido de su reclamación y de los preceptos de esta ley que se consideran vulnerados. La solicitud de protección de datos deberá presentarse ante el Instituto dentro de los quince (15) días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable.
>
> En el caso de que el titular de los datos no reciba respuesta por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo de respuesta previsto para el responsable. En este caso, bastará que el titular de los datos acompañe a su solicitud de protección de datos el documento que pruebe la fecha en que presentó la solicitud de acceso, rectificación, cancelación u oposición.
>
> La solicitud de protección de datos también procederá en los mismos términos cuando el responsable no entregue al titular los datos personales solicitados; o lo haga en un formato incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida.
>
> Recibida la solicitud de protección de datos ante el Instituto, se dará traslado de la misma al responsable, para que, en el plazo de quince (15) días, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que a su derecho convenga.
>
> El Instituto admitirá las pruebas que estime pertinentes y procederá a su desahogo. Asimismo, podrá solicitar del responsable las demás pruebas que estime necesarias. Concluido el desahogo de las pruebas, el Instituto notificará al responsable el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco (5) días siguientes a su notificación.
>
> Para el debido desahogo del procedimiento, el Instituto resolverá sobre la solicitud de protección de datos formulada, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, como pueden serlo aquéllos que deriven de la o las audiencias que se celebren con las partes.
>
> El Reglamento de la Ley establecerá la forma, términos y plazos conforme a los que se desarrollará el procedimiento de protección de derechos.

El artículo 55 esclarece que:

> […] ante la falta de respuesta a una solicitud en ejercicio de los derechos de acceso, rectificación, cancelación u oposición por parte del responsable, el Instituto dará vista al citado responsable para que, en un plazo no mayor a diez (10) días, acredite haber respondido en tiempo y forma la solicitud, o bien dé respuesta a la misma. En caso de que la respuesta atienda a lo solicitado, la solicitud de protección de datos se considerará improcedente y el Instituto deberá sobreseerlo.
>
> En el segundo caso, el Instituto emitirá su resolución con base en el contenido de la solicitud original y la respuesta del responsable que alude el párrafo anterior.

> Si la resolución del Instituto a que se refiere el párrafo anterior determina la procedencia de la solicitud, el responsable procederá a su cumplimiento, sin costo alguno para el titular, debiendo cubrir el responsable todos los costos generados por la reproducción correspondiente.

382.5. La solicitud de protección de datos se presenta sin formalidades, aunque es común que las autoridades de control tengan disponibles formatos preimpresos que resumen el objeto de la petición.

Con el pedido de protección de datos deberá acompañarse la solicitud y la respuesta que se recurre o, en su caso, los datos que permitan su identificación. En el caso de falta de respuesta sólo será necesario presentar la solicitud. Cuando la pretensión se interpone a través de medios que no sean electrónicos, deberá acompañarse de las copias de traslado suficientes.

382.6. El plazo máximo para dictar la resolución en el procedimiento de protección de derechos será de cincuenta (50) días, contados a partir de la fecha de presentación de la solicitud de protección de datos. Cuando haya causa justificada, el Pleno del Instituto podrá ampliar por una vez y hasta por un período igual este plazo (art. 47).

En caso que la resolución de protección de derechos resulte favorable al titular de los datos, se requerirá al responsable para que, en el plazo de diez (10) días siguientes a la notificación o cuando así se justifique, uno mayor que fije la propia resolución, haga efectivo el ejercicio de los derechos objeto de protección, debiendo dar cuenta por escrito de dicho cumplimiento al Instituto dentro de los siguientes diez (10) días (art. 48).

De inmediato, el art. 49 dice que:

> […] en caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere el artículo 46, y el Instituto no cuente con elementos para subsanarlo, se prevendrá al titular de los datos dentro de los veinte (20) días hábiles siguientes a la presentación de la solicitud de protección de datos, por una sola ocasión, para que subsane las omisiones dentro de un plazo de cinco (5) días. Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de protección de datos. La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto para resolver la solicitud de protección de datos.

382.7. Las resoluciones del Instituto podrán: *a)* sobreseer o desechar la solicitud de protección de datos por improcedente, o *b)* confirmar, revocar o modificar la respuesta del responsable.

Se desecha cuando el Instituto es incompetente (por ejemplo, por tratarse de denuncias contra archivos de información crediticia); o cuando haya conocido anteriormente de la solicitud de protección de datos contra el mismo acto y resuelto en definitiva respecto del mismo recurrente.

También si la petición está tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular que pueda tener por efecto

modificar o revocar el acto respectivo; o cuando se trate de una solicitud de protección de datos ofensiva o irracional, o bien, resulte extemporánea.

Por su lado el artículo 53 explica que la solicitud de protección de datos será sobreseída cuando: *a)* el titular fallezca; *b)* el titular se desista de manera expresa; o *c)* admitida la solicitud de protección de datos, sobrevenga una causal de improcedencia, y por cualquier motivo quede sin materia la misma.

382.8. El Instituto podrá en cualquier momento del procedimiento buscar una conciliación entre el titular de los datos y el responsable.

De llegarse a un acuerdo de conciliación entre ambos, éste se hará constar por escrito y tendrá efectos vinculantes. La solicitud de protección de datos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.

Para efectos de la conciliación a que se alude en el presente ordenamiento, se estará al procedimiento que se establezca en el Reglamento de esta ley (art. 54).

382.9. Cabe agregar que todas las resoluciones del Instituto serán susceptibles de difundirse públicamente en versiones públicas, eliminando aquellas referencias al titular de los datos que lo identifiquen o lo hagan identificable.

1514 blanca

Capítulo XIII

Derecho Procesal Constitucional local

Sección 1ª La legislación procesal constitucional en Argentina

383. El Código Procesal Constitucional de la provincia de Tucumán

383.1. Tras un largo periplo iniciado por el proyecto de Sergio Díaz Ricci en el año 1992, el día 7 de mayo de 1999 comenzó a regir el "Código Procesal Constitucional de la provincia de Tucumán" que fue el primer cuerpo orgánico y procedimental de Argentina, destinado a regular los procesos y la jurisdicción constitucional.

El sistema procesal se implementa sobre los lineamientos más modernos de su época, donde prevalece el conjunto de garantías procesales como un sistema armónico y unificado, que sostiene en el artículo 2 la columna de sus definiciones:

> Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro medio efectivo ante los jueces o Tribunales competentes que la ampare contra actos que violen o amenacen sus derechos fundamentales reconocidos por la Constitución Provincial y Nacional, la ley o los tratados, aún cuando tal lesión sea cometida por personas que actúen en ejercicio de sus funciones públicas.

383.2. Al proceso se lo interpreta como "única garantía" y se planifica su eficacia a través de los diversos procedimientos que dan en llamarse procesos constitucionales.

Donde luce con más rigor científico es en el capítulo de disposiciones generales aplicables a todos los procesos, estableciendo el principio de preferente acceso a la justicia a cualquier persona particularmente interesada, por sí o por apoderado; acordando al Ministerio Público el poder de interponer el *habeas corpus* y el amparo.

Inclusive se estableció que las acciones previstas se podían interponer aún después de las horas ordinarias de trabajo o en días inhábiles de los tribunales por ante el juez, secretario o ante la mesa permanente.

A tales fines, en cada jurisdicción debe darse a conocer en avisadores ubicados en sitios visibles donde el público habitualmente concurre o pueda acudir, el juez de turno y el lugar de la sede del tribunal de cada fuero de turno donde debe reclamarse la protección jurisdiccional. Para ello debe colocarse carteles en lugares ostensibles y fácilmente accesibles al público, en todos los edificios judiciales y policiales, y en dependencias de la Administración Pública.

Acorde con la facilitación se establece que durante la sustanciación del proceso de *habeas corpus* o de amparo y su ejecución, todos los días y horas son hábiles. Los plazos establecidos son perentorios e improrrogables, y cualquier retardo en su cumplimiento es sancionado disciplinariamente sin perjuicio de la acción por responsabilidad del funcionario. No se interrumpen ni se suspenden por ningún incidente ni actuación que no esté expresamente preceptuado por la ley. Los términos para las actuaciones y resoluciones judiciales se cuentan a partir del recibo de la gestión que los motive, y para las actividades de las partes desde la notificación de la resolución que las cause.

383.3. Una vez requerida la intervención judicial, el tribunal actúa de oficio y con la mayor celeridad sin que pueda invocarse la inercia de las partes para retardar el procedimiento. En el caso de un *habeas corpus* o de un amparo, en este orden, se hace sin pérdida de tiempo, posponiendo cualquier asunto de distinta naturaleza que tuviera el tribunal. Las comunicaciones entre jueces se hacen por el medio más rápido posible.

De igual modo, en todo proceso constitucional se debe proveer de inmediato las medidas necesarias para subsanar los defectos formales, en particular cuando se trata de un *habeas corpus* o de un amparo. En los demás, si la presentación es oscura de manera que no puede establecerse claramente el hecho que la motiva, o no llena los requisitos indicados, el tribunal dentro de las cuarenta y ocho (48) horas de recibida, si lo considera necesario, puede intimar al presentante para que en el término perentorio que le fije, que no puede exceder de las setenta y dos (72) horas, aclare los términos de su demanda o corrija defectos, los cuales deben señalársele concretamente en la misma resolución. Si el peticionante no lo hace, la presentación es rechazada de plano.

Cuando el juez al conocer el asunto advierta que no se trata de un *habeas corpus* sino de un amparo o viceversa, así lo declara y prosigue la tramitación de conformidad a lo establecido por esta ley. Además, si lo estima necesario, puede conceder al interesado un término de hasta tres (3) días para que convierta la acción. Si éste no lo hiciere resolverá el asunto conforme a derecho.

383.4. Un profundo estudio de Sergio Díaz Ricci[285] informa que en esta provincia del norte argentino, al reformar en 1990 su Constitución provincial, incorporó, un Tribunal Constitucional como órgano extrapoder a cuyo cargo estaría un control de constitucionalidad abstracto y *erga omnes* de las leyes (conjuntamente con los jueces del poder judicial para el caso concreto y efecto *inter* partes) y la resolución de los conflictos entre poderes. Así la reforma de 1990 de la Constitución de la provincia de Tucumán introdujo un órgano prácticamente desconocido en el panorama constitucional argentino: un Tribunal Constitucional provincial.[286] Fue ubicado en la última

---

[285] DÍAZ RICCI, Sergio, "El Tribunal Constitucional "*non nato*" de Tucumán", en *Proceso y Constitución*, AAVV (Director: Osvaldo A. Gozaíni), Ediar, Buenos Aires, 2009, pp. 111 y ss.

[286] "CAPÍTULO SEGUNDO: *Tribunal Constitucional*. ART. 133.—La obediencia de la Constitución y el equilibrio de los poderes que ella establece, quedarán especialmente garantizados por el Tribunal Constitucional,

parte del texto constitucional, en la Sección IX, junto con el capítulo dedicado a la Reforma Constitucional, se agrega un último Capítulo, de sólo dos artículos (arts. 133 y 134), estableciendo un Tribunal Constitucional entre los poderes del Estado provinciales. Esto en 1990 constituyó una total novedad en el derecho constitucional argentino. Empero, este Tribunal Constitucional nunca llegó a constituirse y una reciente reforma de la Constitución tucumana que tuvo lugar el 6 de junio de 2006, lo eliminó [...].

Si bien, en principio, —dice Díaz Ricci— en abstracto no habría objeción para que dentro de un Estado Federal pueda existir un Tribunal Constitucional provincial como ocurre en Alemania que casi todos los Länder tienen un *Verfassungsgerichtshöfe o Staatsgerichtshöfe* (con excepción de Schleswig-Holstein y Berlín), donde además del Tribunal Constitucional Federal (*Bundesverfassungsgerichtshoff)* existen en los län-

---

compuesto de cinco miembros. Para ser magistrado del Tribunal, se requiere ciudadanía, domicilio en la Provincia, título universitario de abogado, cuarenta años de edad, y veinte de ejercicio en la profesión o en la judicatura, dentro de la Provincia. Para su designación, un órgano compuesto por los jueces de la Corte Suprema, y los de la Cámaras de Apelaciones, seleccionará, en votación secreta, de entre la lista de profesionales en condiciones de ser magistrados del Tribunal, un número no menor de tres ni mayor de diez, de entre los cuales el Poder Ejecutivo designará uno que prestará juramento ante el propio Tribunal. Cuando los cargos a llenar fueren más de uno, se procederá sucesivamente, con listas así confeccionadas, de modo que la segunda, tercera, o más listas, sólo sean confeccionadas, una vez que el Poder Ejecutivo haya elegido dentro de la primera, o segunda o tercera, en su caso. Los miembros del Tribunal serán designados por diez años. Serán removibles por enjuiciamiento, ante el órgano compuesto por los jueces de la Corte Suprema y los jueces de Cámara.

ART. 134.—Son atribuciones del Tribunal Constitucional:

1º. Declarar la inconstitucionalidad de las leyes, decretos, ordenanzas, con el alcance general previsto en el artículo 22 última parte.

2º. Entender en la acción que deduzca el Poder Ejecutivo contra el Poder Legislativo, o un Departamento Ejecutivo contra el Concejo Deliberante, por demora en pronunciarse sobre proyectos de leyes u ordenanzas que aquellos hubieren presentado. El Tribunal, apreciando las circunstancias, fijará un plazo para que se expidan, vencido el cual sin que ello se hubiera producido, podrá autorizar al accionante para la directa promulgación, total o parcial, de la norma de que se tratare.

3º. Conocer, por vía de recurso, del rechazo de los diplomas de los electos como miembros de la Legislatura y Concejos Deliberantes, y de las sanciones que estos órganos impusieren a personas de fuera de su seno.

4º. Entender en las causas del art. 5.

5º. Decidir los conflictos de jurisdicción que se plantearen entre la Legislatura y el Ejecutivo de la Provincia, o entre uno de dichos poderes y un juez o tribunal de la Provincia, o entre los órganos de un Municipio, o entre la Provincia y un Municipio, o entre municipios.

ART. 141.—(Disp. Transitoria): Dentro del año de haberse sancionado esta reforma, la Legislatura deberá haber dictado la ley de organización y procedimiento del Tribunal Constitucional dictando todas las demás normas que fueren necesarias para su instalación. El Poder Ejecutivo, al remitir el presupuesto, deberá incluir las partidas necesarias para proveer a su desenvolvimiento. El órgano encargado de formar la lista que será presentada al Poder Ejecutivo deberá estar formado por magistrados con la inamovilidad prevista por las disposiciones permanentes de esta Constitución reformada. En consecuencia, su formación quedará diferida hasta que haya por los menos diez magistrados en tales condiciones. Hasta tanto se instaure el Tribunal Constitucional quedarán en suspenso las nuevas vías de los incisos 1 y 2 del artículo que enuncia las potestades del Tribunal Constitucional, correspondiendo las de los incisos 3, 4 y 5 a la Corte Suprema."

der Tribunales Constitucionales estaduales. Sin embargo, existe una diferencia con Argentina porque en Alemania, en ambos niveles, esto es, federal y estadual, se sigue el mismo modelo de control de constitucionalidad "europeo" o kelseniano, es decir, un control concentrado y con efecto *erga omnes,* donde a los jueces del poder judicial les está impedido pronunciarse sobre la constitucionalidad de las normas.

Por ello, la cuestión más bien se desplaza a ver si en un sistema federal pueden combinarse ambos sistemas de control de constitucionalidad, lo que depende del modelo definido por cada ordenamiento constitucional.

La República Argentina adoptó con su Constitución de 1853 el modelo de control *judicial* de constitucionalidad, es decir, el denominado sistema "norteamericano" o, mal llamado, "difuso".[287] Esta modalidad se aplica tanto dentro del Estado Federal como de los Estados federados, la justicia federal en relación a la Constitución nacional y los tribunales de las 24 jurisdicciones locales en relación a la Constitución local e, inclusive, la federal.[288] En esto, la Argentina sigue el modelo implantado en Norteamérica desde el caso Marbury vs.Madison. En dos estados federales (Alemania y Estados Unidos de Norteamérica) coexiste el control de constitucionalidad a nivel federal y a nivel de los Estados miembros, pero en ambos ámbitos se mantiene la homogeneidad de un mismo sistema de control de constitucionalidad.

En cambio, la Constitución tucumana de 1990, no sólo introduce un elemento del sistema de control europeo a nivel provincial, sino que lo hace de manera parcial ya que deja subsistente el sistema de control judicial. De este modo, consagra a nivel provincial un sistema de control mixto, a cargo de los jueces en causas concretas, por un lado, y a cargo de un Tribunal Constitucional en casos abstractos, por el otro.

En efecto, mantuvo el control de constitucionalidad por un juez de cualquier fuero (art. 22, sistema difuminado o norteamericano) y, simultáneamente, de manera expresa incorporó un sistema concentrado o europeo a cargo de un Tribunal Constitucional. Pero aquí puede señalarse un primer problema pues si bien se instituye un sistema mixto,[289] cada ámbito opera de modo independiente, como compartimientos estancos. De allí que haya sido calificado como "paralelo" absoluto pues está diseñado de una forma que establece un paralelismo total entre ambas jurisdicciones, porque lo resuelto por una de éstas no tiene influencia sobre la otra. Y esto fue establecido expresamente por el art. 22 que dispone:

---

[287] Siempre hemos criticado la calificación de "difuso" por la connotación de impreciso que conlleva. En realidad habría que denominarlo "difuminado" porque se encuentra distribuido en cualquier juez de cualquier fuero de todas las instancias y jurisdicción, o sea, que puede cualquier magistrado del Poder Judicial tiene a su cargo el control de constitucionalidad en las causas que se sometan a su decisión.

[288] *Vid.* DÍAZ RICCI, Sergio, "Algunos problemas de la jurisdicción constitucional argentina. Un Código procesal constitucional", en *Anuario de Justicia Constitucional*, Nº 9, 2005, Madrid, CEPC, 2005.

[289] Algunos países latinoamericanos (*v. gr.:* Perú, Ecuador) han establecido un sistema mixto, pero debemos advertir que no se trata de Estados federales, y esta modalidad está establecida por sus Constituciones Nacionales y en relación a un poder judicial único, distribuido en todo el territorio nacional. *Vid.* GARCÍA BELAÚNDE, Domingo, "*La jurisdicción constitucional y el modelo dual o paralelo*", en La Ley, 1998-E, 1175/1182.

> La declaración de inconstitucionalidad pronunciada por los jueces tendrá efectos específicos para la causa en que entendieren. Quien tenga suficiente interés jurídico podrá demandar ante el Tribunal Constitucional, la declaración de inconstitucionalidad con efectos generales de derogación de la norma impugnada. La impugnación será hecha pública, y el trámite se entenderá dando intervención a cualquier persona que sostenga la constitucionalidad, y al Poder Ejecutivo. Las costas que sean a cargo de cada interviniente, no podrán exceder la retribución mensual de un miembro del Tribunal. *Si el Tribunal no hiciere lugar a la declaración de inconstitucionalidad, la cuestión no podrá ser reeditada, quedando a salvo de los interesados la impugnación ante los jueces, con efectos específicos*.

Así quedó consagrada, por una expresa disposición constitucional, un auténtico sistema mixto "paralelo" puesto que nada impide que ante un fallo adverso del TC pueda intentarse una acción ante un juez y viceversa.

[...]

En el caso Tucumano, esta dualidad, consagrada y aceptada constitucionalmente, de emplear sucesivamente dos vías para plantear la cuestión de constitucionalidad (Tribunal Constitucional o juez, y viceversa) puede conducir a fallos contradictorios, y esto lesiona el principio de unidad jurisdiccional con todos los inconvenientes de seguridad jurídica que ello acarrea. Este asunto nos conduce al siguiente punto porque pone en entredicho al sistema republicano.[290]

384. El recurso extraordinario federal

384.1. En Argentina el sistema procesal federal divide en cada provincia el mecanismo procesal de sus procedimientos. A ello se suma el control de constitucionalidad difuso que le permite a cada juez y en cada jurisdicción, interpretar la Constitución sin límites ni orientaciones, desde que la jurisprudencia de la Corte Suprema de Justicia de la Nación no es obligatoria.

Sin embargo, en todos los procesos provinciales y federales, cuando la Norma Fundamental se encuentra afectada directa o indirectamente, permite al agraviado deducir el recurso extraordinario federal, que se ha considerado un proceso constitucional pese a su condición de medio de gravamen.

384.2. En efecto, la necesidad de reservar para los Tribunales Superiores de los Estados una función revisora del derecho aplicado, antes que de los hechos singulares que estuvieran en conflicto, llevan a la creación de recursos de carácter extraordinarios que tienen la misión de controlar la justicia del caso concreto mediante la aplicación del derecho superior que proviene de las Cartas Constitucionales. De allí que sea común reservar a estos tribunales la función de ser intérpretes finales de la Constitución, cuando esa tarea no se delega en Tribunales Constitucionales que dejan en las Cortes ordinarias, el oficio de aplicar el principio de legalidad. Diferencia ésta que no es baladí, porque obliga a encontrar los límites de cada supremo tribunal.

---

[290] DÍAZ RICCI, *El Tribunal Constitucional "non nato" de Tucumán,* cit., p. 121.

> Este esquema proviene de la *Judiciary Act* norteamericana, creada el 24 de noviembre de 1789. Que puesta en práctica significa establecer una serie de requisitos que obran como filtros de acceso a la Corte Suprema de Justicia de la Nación. Entre ellos el más importante en Argentina, fue la reglamentación creada por la Ley 48, que solo aceptó que dicho tribunal cimero interviniera cuando en cada caso hubieran cuestiones federales que pusieran en crisis, con una resolución contraria, el derecho constitucional emergente de la Carta Suprema de la Nación.
>
> En Estados Unidos, las *federal question* conservaron un sentido político desde el que se dejaba en claro que el supremo tribunal federal no podría conocer sino en casos regidos por el reducido grupo de disposiciones federales que se consideraban indispensables para el funcionamiento de la Unión; los principales interesados en esta limitación eran los Estados, deseosos de preservar sus potestades e impedir la expansión del poder federal, ante el que cedían de mala gana.[291]

384.3. El 25 de agosto de 1863 se sanciona la ley 48 (promulgada el 14 de septiembre de ese año), que se define como "adicional y correctiva" de la ley 27, cuyos artículos 7, 21 y 23 quedaron reformados dando lugar al esquema del actual recurso extraordinario. Se vuelcan así las ideas de la *Judiciary Act* de 1789, tanto en cuanto refiere a las materias que habilitan la actuación de la Corte, como para los "remedios procesales" del *common law* (como los *writs of prohibition* y *of mandamus*) que, por la amplitud de las atribuciones que le otorgaba, llevaran a la Corte norteamericana a declarar la "inconstitucionalidad" de esa norma legislativa.[292]

La incorporación significó tener un mecanismo procesal (procedimientos) regidos por el modelo escrito, formal y solemne de la ley de enjuiciamiento civil española que se había tomado como modelo; y recursos constitucionales del esquema americano, donde se destacaban los denominados, "*recursos extraordinarios de nulidad e injusticia notoria*" que continuaron la legislación de Indias.

Comenzó entonces a funcionar el recurso extraordinario como un sistema aplicado al control de constitucionalidad, pero no tardó en ampliar su dimensión al ocupar el espacio que antes cubrían los arts. 7 y 22 de la ley 27 con el recurso de nulidad, también reglado en los arts. 233 a 240 de la ley 50.

Sin embargo, tan amplio espectro de atribuciones conferidas a la Corte, de dudoso encuadre en la Constitución que no las prevé, no fue de modo alguno "objetada" por nuestro máximo tribunal que, por el contrario, se consideraba precisado a admitir su jurisdicción en los recursos "por arbitrariedad manifiesta". Exactamente a la inversa, de la actitud asumida por la Suprema Corte norteamericana de limitar su jurisdicción.[293]

Con la ley 23.774 del año 1990 se producen modificaciones sustanciales al trámite del recurso extraordinario. La norma aumenta el número de jueces de la Corte

---

[291] PRITCHETT, C. Herman, *La Constitución americana*, Tea, Buenos Aires, 1965, pp. 95 y ss. *Cfr.* LUGONES, Narciso, *Antecedentes históricos, crisis y replanteo de la cuestión federal*, La Ley, 1985-C, 1236 -Derecho Constitucional - Doctrinas Esenciales, Tomo IV, p. 705.

[292] EGÜES, Alberto J., *El certiorari argentino,* La Ley, 1993-C, 661.

[293] EGÜES, *El certiorari argentino,* cit., La Ley, 1993-C, 661.

(de cinco a nueve)[294] y promueve un mecanismo de selección de causas basado en la relevancia o interés institucional en atender la impugnación, que de no darse posibilitaba al tribunal a desechar el recurso con la sola mención del art. 280 del Código Procesal, lo que importaba entender que el recurso no era trascendente.

Cabe agregar que la ley 26.183 volvió al número de cinco (5) integrantes al que se llegará progresivamente a la espera de retiros, jubilaciones u otras causas por las cuales el número actual llegue a la composición esperada.

384.4. Finalmente, en los pasajes históricos, aparece la acordada 4 del año 2007 que, más allá de los cuestionamientos constitucionales que sufre por considerar que la Corte no puede por vía reglamentaria alterar normas que son propias del Congreso de la Nación, significó actuar con auténtica vocación docente, estableciendo un catálogo indicativo de formalidades propias para el recurso extraordinario federal.

La precisión se dispone no solo para la impugnación prevista en el art. 14 de la ley 48, sino además, para la queja o recurso directo. Con forma de anexo se enumeran los requisitos, y en el segundo punto del acuerdo disponen requerir la integración de un formulario que sintetice el objeto de la presentación y el cumplimiento concreto de las solemnidades propias del recurso. No vamos a reseñar ahora el contenido de la acordada, pero es menester adelantar que el primer punto de las "reglas para la interposición del recurso extraordinario federal" reglamenta que "deberá interponerse mediante un escrito de extensión no mayor a cuarenta (40) páginas de veintiséis (26) renglones, y con letra de tamaño claramente legible (no menor de 12)", mientras que en el recurso de queja, se reduce a diez (10) páginas.

> La acordada, en nuestro parecer, no busca aumentar el ritual, ni dar más solemnidades a un recurso que, por sí mismo, requiere de una técnica puntual. En cambio, persigue afanosamente convertir a la pieza en un riguroso escrito donde el recurrente señale con precisión cuál es la cuestión federal que le permite habilitar la intervención de la Corte.

---

[294] La Ley 26.183 del 18 de diciembre de 2006 deroga en el artículo primero, la norma de la Ley Nº 23.774, que había modificado el artículo 21 del Decreto Ley Nº 1285/58, texto según Ley Nº 16.895 (composición de miembros de la Corte). El artículo 2º estableció: Incorpórase como artículo 21 del Decreto Ley Nº 1285/58, texto según Ley Nº 16.895 el siguiente: "ART. 21.—La Corte Suprema de Justicia de la Nación estará compuesta por CINCO (5) jueces. Ante ella actuarán el Procurador General de la Nación y los Procuradores Fiscales ante la Corte Suprema de Justicia de la Nación y los Defensores Oficiales ante la Corte Suprema de Justicia de la Nación en los términos de la Ley Nº 24.946 y demás legislación complementaria".

El artículo 3º como disposición transitoria dijo: La reducción de los miembros de la Corte Suprema de Justicia de la Nación dispuesta por el artículo anterior, operará del siguiente modo: Desde la entrada en vigencia de la presente ley se reducirá transitoriamente a siete (7) el número de jueces que la integran. A partir de dicha reducción, las decisiones de la Corte Suprema de Justicia de la Nación se adoptarán por el voto mayoritario de cuatro (4) de sus miembros. A *posteriori*, en oportunidad de producirse una vacante definitiva se reducirá transitoriamente a seis (6) el número de jueces de la Corte Suprema de Justicia de la Nación. En dicho período las decisiones de la Corte Suprema de Justicia de la Nación se adoptarán por el voto mayoritario de cuatro (4) de sus miembros. Producida una nueva vacante definitiva, se reducirá a cinco (5) el número de jueces que la componen. Las decisiones se adoptarán por el voto de la mayoría absoluta de sus miembros.

Obsérvese que el mismo formulario interroga sobre la decisión que pretende obtener del tribunal.

Al mismo tiempo, la acordada supone cambiar una costumbre arraigada en la redacción del recurso directo, cuál es reiterar los argumentos del extraordinario sumado a la impugnación del auto que lo deniega. Si observamos que, ahora, se reduce a diez (10) páginas el escrito de interposición de la queja, es evidente que no se quiere la repetición innecesaria de fundamentos que ya están en el acto rechazado por el Superior Tribunal de la Causa.

Esta acordada se integra con otra del mismo año, la número 2 que varió significativamente el monto del depósito en el recurso de queja por apelación extraordinaria denegada. Con ella, la Corte envió un mensaje restrictivo.

La Acordada 4 del 16 de marzo de 2007 tiene varios registros a tener en cuenta. No se trata, únicamente, de formalizar con el acuerdo de ministros el catálogo de requisitos necesarios para interponer el recurso extraordinario federal, sino de advertir los mensajes implícitos que tiene la disposición.[295]

384.5. El recurso en estudio es de apelación aunque su procedencia sea extraordinaria. Recuérdese que proviene de la necesidad de revisar aquellas sentencias de notoria injusticia, que en palabras de Couture supone consagrar una nueva súplica ante el Superior, como aquellas que se realizaban en el recurso de mil y quinientas ante el Rey de España, que era el importe de la suma que debía depositarse para afianzar el resultado.[296]

En la práctica supone agregar una nueva instancia, de allí que se pretenda restringir la extensión del proceso acotando los presupuestos de admisión. Es de algún modo la tendencia que comienza el código italiano de 1940 cuando aumenta los poderes del juez y disminuye el número de recursos, o sea, el triunfo de una justicia pronta y firme sobre la necesidad de una justicia buena pero lenta.[297]

384.6. En Argentina el recurso extraordinario tiene varias posibilidades. La jurisdicción apelada obligatoria que habilita la actuación de la Corte Suprema se encuentra en las siguientes vías:

a) recurso extraordinario de apelación contra las sentencias de superiores tribunales de provincia (art. 14, ley 48);

b) recurso ordinario de apelación contra las sentencias de las cámaras nacionales de apelación (art. 24, inc. 6°, decreto-ley 1285/58);

c) cuestiones de competencia entre órganos judiciales que no tengan superior jerárquico común (art. 24, inc. 7°, decreto-ley 1285/58);

d) conflictos entre jueces (art. 24, inc. 7°, decreto-ley 1285/58);

e) recurso por retardo de justicia contra cámaras nacionales de apelaciones (art. 24, inc. 5°, decreto-ley 1285/58).

---

[295] GOZAÍNI, Osvaldo A., *Tratado de Derecho Procesal Civil,* Tomo V, La Ley, Buenos Aires, 2009, p. 378.

[296] COUTURE, *Fundamentos de derecho procesal civil,* cit., p. 349.

[297] COUTURE, *Fundamentos de derecho procesal civil,* cit., p. 349.

Sin perjuicio de ellos, la Corte puede intervenir también (decisión discrecional, si tenemos en cuenta lo previsto en el art. 280 del Código Procesal), en el recurso extraordinario por arbitrariedad manifiesta (o "nulidad" del art. 22, ley 27); o por avocación superintendencial (art. 22, Reglamento para la justicia nacional; y mediante lecturas jurisprudenciales consolidadas, con la invocación de la "gravedad institucional" o la trascendencia relevante de la causa..

A todos estos supuestos de "apelación" en que la jurisdicción de la Corte argentina no viene impuesta como "obligatoria" por el legislador y en las que ya se han dictado una o varias decisiones judiciales anteriores, naturalmente aún es necesario adicionarle el conocimiento de las "causas originarias" que le atribuye el art. 116 de la Constitución Nacional y, finalmente, aquellas decisiones que adopta como órgano administrativo.[298]

384.7. Desde otra perspectiva, el recurso es extraordinario porque permite que el superior tribunal de justicia de la nación intervenga como remedio final de conflictos donde la interpretación de cláusulas constitucionales esté en disputa.

Por eso, afirma Gelli que:

> [...] El recurso extraordinario federal constituye el instrumento procesal mediante el cual se habilita, en última instancia, el control de constitucionalidad por parte de la Corte Suprema. En sus orígenes, ese recurso extraordinario federal constituyó el medio procesal establecido para mantener la supremacía del derecho federal sobre los ordenamientos locales, con la finalidad de asegurar la unidad jurídica de la Nación, en las materias delegadas [...]. Según se mire, el recurso extraordinario federal puede considerarse un instrumento técnico de admisibilidad del control de constitucionalidad o una herramienta política para extender o restringir el análisis de políticas públicas, en tanto ellas afecten la supremacía federal, causando agravios a los derechos reconocidos en la Constitución.
>
> Se diría que la caracterización de las cuestiones federales y la inclusión en ellas de la arbitrariedad; el saltar los óbices formales para admitir el recurso extraordinario, alegando gravedad institucional; la significación dada al concepto de sentencia definitiva en relación también con la gravedad institucional, para abrir o cerrar el recurso extraordinario federal; la exigencia estricta del planteo oportuno de la cuestión federal, en cada ocasión procesal en que se suscite o, por el contrario, la aceptación del control de constitucionalidad de oficio; la admisión del "*per saltum*", constituyen ejemplos de la jurisdicción discrecional de la Corte Suprema, consagrada por vía pretoriana, que facilitan al Tribunal las vías para mostrarse permeable a los intereses del gobierno o, en cambio, para nunca cuestionarlos y, de rondón, establecer la propia agenda.
>
> La ampliación de la competencia apelada de la Corte Suprema a que dio lugar la flexibilización de los requisitos del recurso extraordinario federal, fue una de las causas invocada para la incorporación legal del llamado "certiorari" argentino o de denegación del recurso, por falta de agravio federal suficiente o planteamientos insustanciales o carentes de trascendencia. Como se advierte, el "certiorari" negativo, constituye la contra cara de la gravedad institucional mediante cuya invocación la Corte Suprema abrió el recurso pese

[298] EGÜES, *El certiorari argentino,* cit., La Ley, 1993-C, 661.

a la existencia de óbices formales para su admisibilidad o a pesar de la inexistencia de estricta cuestión federal.

De su lado, el reconocimiento o no de la legitimación activa por parte de la Corte Suprema ha constituido otra de las llaves que han abierto o cerrado el recurso extraordinario federal. El tema devino en verdadera cuestión problemática a propósito de la amplitud de la legitimación acordada al afectado, al Defensor del Pueblo y al las asociaciones del sector social, registradas conforme a la ley, en materia de discriminación, de los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general. Las recurrentes emergencias públicas y el empleo del amparo como remedio a las vulneraciones de los derechos constitucionales han agregado, si cabe, una incertidumbre más a las cuestiones sustantivas ligadas con el recurso extraordinario federal.[299]

La condición de recurso supone revisión de sentencia; lo de extraordinario tiene matices distintos. En la clasificación tradicional los remedios ordinarios se resuelven ante el mismo juez, en cambio los recursos exigen la participación del superior jerárquico. Si la intervención es ordinaria, revisa los hechos y el derecho aplicado, mientras que si es extraordinaria, por vía de principio, la actuación se restringe a verificar la aplicación correcta del derecho.

Cuando la intervención suscitada es de la Corte Suprema, lo extraordinario es la gravedad del caso donde las cuestiones constitucionales se encuentran en controversia, por eso algunos prefieren llamarlo "recurso de inconstitucionalidad".[300]

Claro está que el conflicto constitucional provoca la necesidad de ocuparse de todas las cuestiones que puedan derivar en una violación al principio de la supremacía (art. 31, Constitución Nacional) de allí que las cuestiones de hecho que provocan una injusticia notoria no pueden quedar fuera de la revisión. De algún modo es el permiso que tiene considerar a la "arbitrariedad" como una causal implícita del art. 14 de la ley 48.

En la dimensión estricta de la técnica procesal, se llama recurso extraordinario porque tiende a evitar que una sentencia inconstitucional o injusta alcance el grado de cosa juzgada, porque de llegar al estado no habría recurso sino revisión.

384.8. Para Imaz y Rey, el recurso extraordinario es una apelación excepcional que tiene por objeto el mantenimiento de la supremacía constitucional;[301] criterio

---

[299] El desmesurado crecimiento de la competencia extraordinaria de la Corte Suprema que la arbitrariedad y la gravedad institucional produjeron, se quiso remediar con la limitación del "certiorari", ya mencionado. Sin embargo, la innegable cuota de poder que ese instituto implica no ha solucionado el problema ni aliviado el trabajo del Tribunal -porque de todos modos debe examinar si hay o no agravio federal suficiente- aunque merced a aquél y a su propia jurisprudencia la Corte ha adquirido un poder discrecional verdaderamente notable. La discrecionalidad de la Corte Suprema para aplicar el "certiorari" ha llevado, en algunas ocasiones, a calificar de depredador al art. 280 del Código Procesal Civil y Comercial (GELLI, María Angélica, *Dilemas del recurso extraordinario federal,* La Ley, 2004-A, 1302).

[300] GUASTAVINO, Elías P., *Recurso extraordinario de inconstitucionalidad,* Tomo I, La Rocca, Buenos Aires, 1992, pp. 79 y ss.

[301] IMAZ, Esteban, REY, Ricardo E., *El recurso extraordinario,* Nerva, Buenos Aires, 1962 (2ª edición actualizada por Lino E. Palacio y Ricardo E. Rey), p. 13.

que la doctrina más representativa repite y acepta.[302] Esta coincidencia la pone de manifiesto Morello al destacar la capital importancia que en el plano de la política jurídica constitucional tiene el recurso extraordinario, y sobremanera, cuando actúa para asegurar la eficacia del servicio de justicia. En este aspecto ha dicho que:

> […] el carácter es de una verdadera casación *in indicando*, y su objetivo es el de permitirle a la Corte Suprema de Justicia de la Nación ser el fiel intérprete final de la Ley Fundamental —con lo cual mantiene y asegura la supremacía de sus principios y uniformidad de su interpretación—, preservar las garantías, la efectividad del proceso justo y la tutela eficaz de los derechos esenciales. Afirmar en concreto la misión de hacer justicia.[303]

Quedan expuestas así las dos tendencias que tiene el objeto a perseguir. Una tesis que acentúa el control de las cuestiones constitucionales implicadas en los tres incisos del art. 14 de la ley 48, de forma que la intervención de la Corte es un reaseguro del control de constitucionalidad y de legalidad; y otra de mayor espectro que admite bosquejar desde el recurso extraordinario la eficacia del servicio jurisdiccional, es decir, proyectando desde la fiscalización del principio de supremacía, cuestiones que no son directamente constitucionales (como el error, el desvío legal, la incongruencia normativa, el defecto fáctico de congruencia, la apreciación equivocada de la prueba, la arbitrariedad, etc.) aunque anidan y tienen protección constitucional bajo la garantía común del debido proceso.

Vale decir, sea una u otra, en ambos casos hay apoyos para decidir cuestiones constitucionales que figuran a la Corte como un auténtico "Tribunal de Garantías", de lo que deriva que, al no haber un tribunal superior, es a ella misma a la que le corresponde conocer de cualquier recurso a que hubiera lugar, como sucedía en la práctica antigua con el de súplica; y como actualmente sucede con el de revisión.[304]

384.9. La dimensión del recurso extraordinario no se aumenta con esta perspectiva, solamente sitúa sus posibilidades y enmarca el objeto, que no es otro que provocar una doctrina constitucional y la interpretación justa de la ley. Pero, además,

---

[302] Carrió sostiene que la ley 48 del 14.9.863 creó un remedio destinado a asegurar la supremacía de la Constitución Nacional, y en general, de los actos federales conforme a ésta…El recurso tiende, en términos generales, a asegurar el contralor judicial de constitucionalidad de las leyes, normas y demás actos de los gobernantes y sus agentes. De esta manera la Corte reserva y asegura para sí la última palabra al respecto, en cuanto intérprete final de la Constitución (CARRIÓ, Genaro, *El recurso extraordinario por sentencia arbitraria,* Abeledo Perrot, Buenos Aires, 1978 (2ª edición actualizada con la colaboración de Alejandro Carrió), p. 13. Bidart Campos compartía la función recursiva, como también Barrancos y Vedia que, además, sostiene que es una vía excepcional, que tiene como principal función la de asegurar la supremacía de la Constitución Nacional (BARRANCOS Y VEDIA, Fernando N., *Recurso Extraordinario y gravedad institucional,* Abeledo Perrot, Buenos Aires, 1969, p. 23).

[303] MORELLO, Augusto Mario, *El recurso extraordinario,* Platense-Abeledo Perrot, Buenos Aires, 1999 (2ª edición con la colaboración de Ramiro Rosales Cuello), p. 3.

[304] Fallos, 24:199.

reconocido por la Corte la doctrina de la arbitrariedad de las sentencias, el tribunal genera una corriente que pone entre las finalidades del recurso la de encontrar soluciones razonables y equitativas, teniendo en cuenta que la misión más delicada de la justicia es la de saberse mantener dentro del ámbito de su jurisdicción, sin menoscabar las funciones que incumben a los otros poderes.[305]

El interrogante que cuadra consiste en responder si la "arbitrariedad" de las sentencias es o no un caso constitucional, recordando para ello que el recurso solo funciona con el estándar reglado de las cuestiones federales, donde la arbitrariedad es doctrina judicial que, como tal, podría abandonarse.

Sin embargo, pensamos que el objeto de la doctrina de la arbitrariedad no es corregir en tercera instancia fallos equivocados, sino cubrir los defectos graves de fundamentación o razonamiento, por la manifiesta carencia de motivos que tornen ilusorio el derecho de defensa y conduzcan a la frustración del derecho federal invocado. Son supuestos de extrema gravedad los que permiten invocar el desvío y procurar el arreglo a ese apartamiento palmario de la solución prevista en la ley.

La Corte no desdeña la posibilidad, pero marca el territorio anticipando que sus fallos no la autorizan a sustituir el criterio de los magistrados de la causa cuando el conflicto versa sobre situaciones distintas a las federales regladas.

Recuerda Morello que:

> […] desde que la Corte estableciera el precedente de Fallos, 184:137 sobre la arbitrariedad de las sentencias judiciales, se preocupó por fijar sus límites restrictivos, establecidos por el carácter específico con que esta legislada, su jurisdicción extraordinaria, es decir, como apelación excepcional para el control de supremacía federal previsto en el art. 31 de la Constitución Nacional, y como casación del derecho federal.[306] En tal orden de ideas, el tribunal no dejó de advertir, en cuanta oportunidad se le presentó, que no es su función sustituir su propio criterio al que, en materia no federal, está reservado a los jueces de la instancia ordinaria, y que, por eso mismo, en tanto las sentencias contengan fundamentos jurídicos mínimos que impidan su descalificación como acto judicial, la doctrina de la arbitrariedad no es invocable en torno a supuestos de error en la solución acordada, incluso en los casos en que tal error pudiera existir a juicio de la misma Corte,[307] pues el recurso extraordinario no se propone rectificar toda injusticia que pueda existir en un fallo apelado, ni importa extender la jurisdicción de la Corte más allá de sus prerrogativas constitucionales y legales, sino que significa la afirmación de su jurisprudencia constante de rever toda resolución definitiva de cualquier autoridad del país, en la cual se haya planteado cuestiones que afecten principios constitucionales y aquélla haya sido contraria a la letra, espíritu o supremacía de la Constitución o leyes nacionales invocadas.[308]

---

[305] MORELLO, *El recurso extraordinario,* cit., p. 10.

[306] Fallos, 248:189; 256:372; 261:223, entre muchos otros.

[307] Fallos, 251:243; 254:505; 255:211; 261:223; 290:95 y 365, entre otros.

[308] Fallos, 158:78 y 186:497. *Cfr*. MORELLO, Augusto Mario, *La sentencia arbitraria; alternativas de la Corte Suprema ante esa manifestación negativa de la jurisdicción*, La Ley, 1987-B, 921 - Derecho Constitucional - Doctrinas Esenciales, Tomo IV, p. 717.

Pero, esta doctrina no es impermeable, porque la función del recurso extraordinario opera como proceso constitucional, en el sentido de advertir una función especial que obliga al activismo de los jueces, y en particular, de la Corte Suprema de Justicia de la Nación. Se trataría, por consiguiente, de un medio apto para asegurar el reconocimiento de derechos fundamentales, garantizados por la Constitución, contra pronunciamientos gravemente contrarios a derecho o repugnantes a las pautas valorativas básicas que se desprenden de aquélla. Si procediere contrariamente y no revisara la sentencia apelada, la Corte dejaría de actuar como tribunal cimero del control de constitucionalidad.

384.10. En otra banda de significativa importancia que en la experiencia del proceso lleva lejos la frontera de la apelación federal, abundan las decisiones que nucleadas en cuestiones de hecho, prueba, derecho común, derecho provincial o local, destacan que tales circunstancias no resultan óbice decisivo para abrir el recurso extraordinario cuando la sentencia recurrida satisface sólo en apariencia la exigencia constitucional de adecuada fundamentación.[309]

En suma, de lo que se ocupa el recurso extraordinario es de evitar que se menoscabe el valor justicia cuando se avasallan garantías constitucionales; y pese al supuesto obstáculo que tiene entrar a considerar hechos que manifiestan el absurdo o la arbitrariedad, ello no es causa de inhibición a la intervención reparadora del máximo tribunal, pues implícitamente se suscita una verdadera cuestión constitucional en aspectos circunstanciales pero cardinales para el adecuado desemboque del proceso y de la sentencia final.[310]

384.11. *Doctrina de la arbitrariedad*. El origen de la doctrina de la arbitrariedad se da como una suerte de superación del dogma impuesto por el restricto alcance de los tres incisos del art. 14 de la ley 48. A fines del año 1909, la jurisprudencia cimera comienza a ensanchar el terreno abonado por las cuestiones federales para entrar a remediar procesos donde la sentencia se muestra con error evidente al punto de ser arbitraria. No había pasado tanto tiempo desde la sanción de la ley cuando

---

[309] MORELLO, *La sentencia arbitraria; alternativas de la Corte Suprema ante esa manifestación negativa de la jurisdicción*, cit., La Ley, 1987-B, 921 - Derecho Constitucional - Doctrinas Esenciales, Tomo IV, p. 717.

[310] Advierte Morello que este pensamiento que reflejamos no significa deducir que la Corte posea una jurisdicción omnicomprensiva, que le permita avocar el conocimiento de cualquier causa en la que no se haya realizado la idea vigente de justicia. De adoptarse tal temperamento, se establecería que la Corte Suprema argentina es la depositaria original de todo el Poder Judicial de la Nación y de las provincias y que todos los demás órganos judiciales lo ejercen por una suerte de delegación. Convergentemente y en ese orden de ideas, también ha puntualizado que la jurisdicción de la Corte debe sujetarse a los límites que le fijan la Constitución y las leyes, sujeción en la cual la autoridad de sus fallos encuentran uno de sus más claros y sólidos fundamentos (MORELLO, *La sentencia arbitraria; alternativas de la Corte Suprema ante esa manifestación negativa de la jurisdicción*, cit., La Ley, 1987-B, 921 - Derecho Constitucional - Doctrinas Esenciales, Tomo IV, p. 717).

ya se advirtió la necesidad de remediar aquellos pronunciamientos que, viciados por error manifiesto, tornaban al fallo en arbitrario e insostenible.

El famoso caso "*Rey c. Rocha*"[311] permitió a la Corte fundar la admisión del recurso extraordinario fuera de los cánones reglados, cuando se alteraba con la decisión el derecho de propiedad. Nadie puede ser privado de su propiedad sino en virtud de sentencia fundada en ley, dijo por entonces, y consideró que una sentencia que iba contra ese dogma, quedaba desprovista de todo apoyo legal y fundada, tan solo, en la voluntad de los jueces. No era una interpretación errónea de la ley, sino una aplicación arbitraria tal como expone el *obiter dictum* del fallo.

Desde entonces, el tribunal comenzó a diferenciar entre sentencias arbitrarias y sentencias erróneas, permitiendo solo el primero y no el restante en la admisión del recurso extraordinario. El error en la apreciación de la ley o en la estimación de contingencias sufridas en el litigio, no reflejaron problemas de arbitrariedad, sino de faltas o deslices que tornaban al fallo en irrevisable por la senda del carril extraordinario. Muchas veces se dijo que la gravedad del traspié era una cuestión técnica que no hacía arbitraria una sentencia en el sentido propio y estricto de la expresión, porque la existencia de error era por sí sola demostrativa de que el pronunciamiento no se había desentendido de la ley y de la prueba sino que padecía una interpretación equivocada.[312]

Por mucho tiempo se mantuvo esta diferencia, y recién en 1939 cuando dicta sentencia en la causa "*Storani de Boidanich*"[313] refiere a la arbitrariedad del pronunciamiento que afecta el derecho de propiedad. Comienza entonces a bosquejar algunas líneas de interpretación para la doctrina, dando preferencia a dicho derecho individual. En este sentido el fallo sostuvo que, "la declaración constitucional de que nadie puede ser privado de su propiedad sino en virtud de sentencia fundada en ley, da lugar a recurso para ante la Corte Suprema en los casos extraordinarios de sentencias arbitrarias desprovistas de todo apoyo legal, fundadas tan sólo en la voluntad de los jueces". En el caso se consideró violatoria de los arts. 222 del Código de Procedimientos Civiles supletorio de la ley federal 50 y del art. 17 de la Constitución Nacional, la resolución que había modificado la sentencia definitiva pasada en autoridad de cosa juzgada, que estaba cumplida por el demandado, y en consecuencia, significó privar a dos de los actores del derecho a la indemnización reconocida en la misma e incorporado a su patrimonio.

Desde entonces, no hay fallos rutilantes que muestren un avance progresivo, pese a que la cita de cuestiones arbitrarias va aumentando. Es más, cuando se analiza la jurisprudencia no se puede eludir la impresión que genera el tipo de cuestiones donde se aplica, básicamente impregnada de motivaciones políticas antes que de razones de carácter jurídico constitucional.

---

311 Fallos, 112:384.

312 Fallos, 207:72.

313 Fallos, 184:137.

A partir del año 1955 la arbitrariedad expande sus fundamentos; si bien se apoya en el derecho de defensa consagrado en el art. 18 de la Constitución Nacional, y también en la naturaleza de la afectación sobre derecho constitucional de propiedad (arts. 14 y 17, Constitución Nacional), pronto amplifica las cuestiones federales a materias que vician la construcción formal de la sentencia. Se califica ahora al pronunciamiento como arbitrario y se deja de lado la tesis del error.

La preocupación del momento es evitar que desde las sentencias se produzcan graves consecuencias que impacten, no solo en el derecho individual, sino en la extensión que puede conseguir el efecto jurisprudencial.

Se aclara, no obstante, que el objeto de la doctrina de la arbitrariedad no es corregir en tercera instancia fallos equivocados, sino cubrir los defectos graves de fundamentación o razonamiento, por la manifiesta carencia de motivos que tornen ilusorio el derecho de defensa y conduzcan a la frustración del derecho federal invocado;[314] asimismo se resguarda el carácter excepcional, pues solo atiende supuestos de gravedad extrema en los que se verifique un apartamiento palmario de la solución prevista en la ley.

La evolución es progresiva, los tiempos político institucionales lo permiten, y de un plano estricto de control de constitucionalidad, el recurso extraordinario consigue desde la arbitrariedad, penetrar en la razonabilidad técnica y discursiva que edifica la sentencia.[315] Las cuestiones de hecho, prueba y derecho común, que fueron irrevisables por no ser cuestión federal, tuvieron excepciones amparadas en la imposibilidad de consagrar injusticias notorias.

---

[314] Fallos, 298:360.

[315] Sostiene Morello que "[…] Todo ello es así dado el carácter de aquella tacha, que no autoriza a sustituir el criterio de los magistrados de la causa por los de la Corte para resolver cuestiones no federales. En un resumen lapidario de los fundamentos de esa corriente, en la que nos parece destacado —esto muy respetuosamente—, se proyectan las luces de arrastre del clásico u ortodoxo recurso extraordinario, el plasmado en los tres incisos del art. 14 de la ley 48, se apiñan estas consideraciones: Desde que esta Corte estableciera el precedente de Fallos, 184:137 sobre la arbitrariedad de las sentencias judiciales, se preocupó por fijar sus límites restrictivos, establecidos por el carácter específico con que está legislada, su jurisdicción extraordinaria, es decir, como apelación excepcional para el control de supremacía federal previsto en el art. 31 de la Constitución Nacional, y como casación del derecho federal (Fallos, 248:189; 256:372, entre muchos otros). En tal orden de ideas, el tribunal no dejó de advertir, en cuanta oportunidad se le presentó, que no es su función sustituir su propio criterio al que, en materia no federal, está reservado a los jueces de la instancia ordinaria, y que, por eso mismo, en tanto las sentencias contengan fundamentos jurídicos mínimos que impidan su descalificación como acto judicial, la doctrina de la arbitrariedad no es invocable en torno a supuestos de error en la solución acordada, incluso en los casos en que tal error pudiera existir a juicio de la misma Corte (Fallos, 251:243; 254:505; 255:211; 261:223; 290:95 y 295:365, entre otros), pues el recurso extraordinario no se propone rectificar toda injusticia que pueda existir en un fallo apelado (Fallos, 172:149), ni importa extender la jurisdicción de esta Corte más allá de sus prerrogativas constitucionales y legales, sino que significa la afirmación de su jurisprudencia constante de rever toda resolución definitiva de cualquier autoridad del país, en la cual se haya planteado cuestiones que afecten principios constitucionales y aquélla haya sido contraria a la letra, espíritu o supremacía de la Constitución o leyes nacionales invocadas (Fallos, 158:78 y 186:497) (MORELLO, Augusto Mario, *La sentencia arbitraria; alternativas de la Corte Suprema ante esa manifestación negativa de la jurisdicción*, cit., La Ley, 1987-B, 921 - Derecho Constitucional - Doctrinas Esenciales, Tomo IV, p. 717).

La Corte descalifica sucesivamente fallos que, a su juicio, tenían solo fundamentación aparente, ya por carecer de verdadera motivación o estar carentes de sustento normativo; a veces por dejar a un lado las normas claramente aplicables al caso, ya por apartarse de los hechos probados en la causa, ya por presentar otros vicios emparentados con los que acabo de mencionar e igualmente graves.[316]

La casuística obligó a definiciones que precisaran cuando se estaba o no ante una sentencia arbitraria. Carrió las estructura y asienta en tres pilares: *a)* el derecho de propiedad en sentido amplio, es decir, aquél que trasciende los bienes y las cosas; *b)* las acciones que muestran el desvío evidente de la sentencia que, como tales, constituyen una franca transgresión al adecuado servicio de la administración de justicia, y *c)* el derecho de defensa en juicio, por su impacto en el debido proceso adjetivo.[317]

Fue también este autor quien elaboró una lista no cerrada de tipos de sentencias arbitrarias, a partir de una gran cantidad de pronunciamientos del alto tribunal. Ella se basa en la múltiple y heterogénea variedad de vicios ("causales de arbitrariedad") que, según la Corte, justificaban dejar sin efecto una decisión por ser arbitraria.

> Alineados con el apunte, se indican como motivos de arbitrariedad*: a) el objeto de la decisión*: es decir cuando no se resuelven cuestiones planteadas; o se deciden pretensiones inexistentes; *b) los fundamentos normativos de la sentencia*: como arrogarse el juez al fallar, el papel del legislador; o cuando prescinde del texto legal aplicable sin dar razón alguna; o si aplica una norma derogada o aún no vigente; o la sentencia tiene fundamentos de excesiva latitud); *c) los fundamentos de hecho de la decisión*: que surgen cuando se omite considerar prueba decisiva; o se invoca prueba inexistente; o se contradicen otras constancias de los autos; *d) cuando existe colisión interna del fallo, o defectos de congruencia,* como a la correspondencia entre los dos tipos de fundamentos y la conclusión; por ejemplo cuando se sustenta el fallo en afirmaciones dogmáticas o dar un fundamento sólo aparente; o se incurre en excesos rituales; o el pronunciamiento es autocontradictorio; *e) efectos de la decisión*: o cuando la sentencia vulnera los efectos de la cosa juzgada al dejar sin efecto decisiones anteriores firmes.[318]

384.12. *La gravedad institucional* como factor de apertura al recurso extraordinario es también una herramienta argumental que exige suficiente demostración cuando se la invoca, aunque puede traerla de oficio el Superior Tribunal cuando considera que ella está presente y flexibiliza la aplicación de todos los presupuestos de admisión del recurso extraordinario.

El origen de la institución data de 1903[319] cuando la Corte, en un asunto de contenido patrimonial donde podía estar discutido el alcance de sentencia definitiva (se trata de un juicio de apremio) permite la defensa del Estado ante una excepción interpuesta.

---

[316] CARRIÓ, Genaro, *Don Quijote en el Palacio de Justicia (La Corte Suprema y sus problemas*), La Ley, 1989-E, 1131.

[317] CARRIÓ, *El recurso extraordinario por sentencia arbitraria,* cit., p. 39.

[318] CARRIÓ, *Don Quijote en el Palacio de Justicia (La Corte Suprema y sus problemas*), La Ley, 1989-E, 1131. También, *El recurso extraordinario por sentencia arbitraria*, cit., pp. 41 y ss.

[319] Fallos, 98:309.

Es la Corte de Bermejo, y pese a que la integración del tribunal en este tiempo se caracterizó por el empleo de un método de interpretación indiscutiblemente literal e histórico, que condujo a un positivismo jurídico exagerado que privilegió los intereses del Estado sobre los derechos individuales; también hizo suya la aplicación dinámica de situaciones rituales que motivaron decisiones en las que se instrumentó la pauta de la "gravedad institucional".[320]

Históricamente, la apertura fue acordada cuando los intereses del Estado podían quedar afectados, de manera que la gravedad fue leída con sentido patrimonial; por ejemplo, pese al aspecto procesal de la cuestión, se toleraba el recurso cuando la solución podía afectar el régimen y regular funcionamiento del impuesto a los réditos;[321] o si estaba alterada la prestación de un servicio público;[322] o existían razones institucionales que obligaban a preservar la percepción de impuestos nacionales.[323] Después comienza a citar la eventual restricción de garantías básicas de la organización nacional,[324] en fin:

> […] "estos precedentes fueron configurando y preparando el terreno para el empleo de la pauta valorativa de la *gravedad* o *interés institucional,* excluyente de la sujeción estricta a ciertos requisitos de admisión del recurso extraordinario, como ser la exigencia de que la sentencia apelada sea *definitiva* o recaudos de índole procesal para su admisibilidad".[325]

No obstante, no está bien perfilada la idea cuando se confronta el desarrollo jurisprudencial y se advierte que no todos son conflictos del Estado los que generan la apertura por gravedad institucional. A veces, el interés público, la trascendencia de los hechos, la urgencia en resolver, entre otros motivos, han permitido abrir el recurso invocando el permiso mencionado.

La causa "*Antonio, Jorge*", permitió explanar algo más, al punto que desde aquí se elaboran proyecciones que expandieron el uso de la institución.

Las dudas que tiene la gravedad institucional aplicada como "causal independiente" o como "excusa formal", se ponen de manifiesto con la contradicción jurisprudencial existente.

La actual composición de la Corte sostiene que la gravedad institucional admite prescindir de ciertos requisitos formales, pero no a suplir la inexistencia de cuestión federal.[326] Sin embargo, fue dicho que este motivo lleva como finalidad superar el requisito sustancial de la inexistencia de cuestión federal.[327]

---

[320] SAHAB, Ricardo J., *El recurso extraordinario por gravedad institucional,* Ediar, 1978, p. 34.

[321] Fallos, 197:426.

[322] Fallos, 228:542.

[323] Fallos, 230:469.

[324] Fallos, 242:55.

[325] BARRANCOS Y VEDIA, *Recurso extraordinario y gravedad institucional,* cit., p. 54.

[326] CS, 2008/12/22, "*Alsogaray, María Julia*", DJ 11/02/2009, 288, con cita de Fallos, 331:2799; 318:2611, disidencia del doctor Fayt; 325:2534; 326:183, entre otros.

[327] MORELLO, *Recurso extraordinario,* cit., p. 575.

Probablemente la diferencia de criterios tenga causa en la distinción proveniente entre adoptar a la gravedad institucional como un motivo independiente para argumentar el acceso a la Corte mediante el recurso extraordinario (en cuyo caso, al cuarto inciso no escrito del art. 48 que implica la arbitrariedad de las sentencias, habría que agregar un quinto implícito para la gravedad institucional) respecto al criterio de flexibilización de causales que desarrolló la jurisprudencia, o la discrecionalidad pura que instaura la ley 23.774.

Recientemente el tribunal cimero pone de relieve la necesidad de fundamentar con independencia del resto de los requisitos (procesales y materiales) la cuestión de interés general que torne viable el supuesto de gravedad institucional.

En efecto, sostiene la sentencia que:

> [...] la alegada trascendencia económica y jurídica del litigio no alcanza para configurar un supuesto de gravedad institucional, si no aparece fehacientemente demostrado que lo decidido en la causa, en torno al rechazo de la capitalización de intereses devengados por el monto de la condena, pueda afectar principios del orden social vinculados con instituciones básicas del derecho que autoricen a prescindir de los recaudos formales y sustanciales de la apelación extraordinaria intentada.[328]

La atención fue puesta en la realidad económica y en la duración del pleito -casi 30 años-, donde un conflicto suscitado por la capitalización de intereses devengados por el monto de la condena, que por vía de principio son cuestiones fácticas y de índole procesal, ajenas a la instancia del art. 14 de la ley 48, permitieron interpretar que había cuestión federal ante el menoscabo de los derechos de propiedad y de defensa en juicio, y desatención de las consecuencias patrimoniales implicadas.

Por ello, concluyó que:

> [...] dada la inusitada duración del pleito, el rechazo de la capitalización de intereses del monto de la sentencia tiene suficiente relevancia institucional, a los fines del recurso extraordinario, pues, la falta de consideración de intereses adecuados, el premio a la conducta de quien no cumple con las reglas e incurre en mora, el impacto que ello tiene en la actividad económica y en el incremento de la litigiosidad innecesaria, justifica que la Corte Suprema intervenga, ya que, si se subsidian tales conductas —en el caso, el deudor se encuentra en mora desde 1976—, se consolida una regla que, indirectamente, afecta el derecho a un proceso que transcurra en un tiempo razonable.[329]

384.13. La tendencia actual del recurso extraordinario es restrictiva. No solamente expresada en la jurisprudencia que utiliza la Acordada 4/2007 como elemento desintegrador de los requisitos propios, comunes y procesales del remedio excepcional, sino aumentado en su rigor por la vía del art. 280 del Código Procesal Civil y Comercial de la Nación.

Se comprueba cuando está repetido que la invocación de la gravedad institucional solamente se tiene en cuenta para superar obstáculos de forma a la procedencia

---

[328] CS, 2009/03/17, "*Automotores Saavedra S.A. c. Fiat Concord S.A.*", Fallos, 332:466.

[329] CS, 2009/03/17, "*Automotores Saavedra S.A. c. Fiat Concord S.A.*", Fallos, 332:466.

del recurso, pero no para suplir la inexistencia de cuestión federal o de arbitrariedad. Por ejemplo, sirve para excusar la sentencia definitiva que no existe;[330] para aligerar cargas formales como la legitimación del recurrente, o para denegarla por el mismo motivo;[331] para proyectar la necesaria y oportuna recaudación de la renta fiscal;[332] o actuar sobre los intereses de la economía nacional.[333]

Pero lo que no es posible, es invocar la doctrina de la gravedad institucional sin fundamentarla adecuadamente y probar en su caso que ella es procedente. No es una causal asimilable a la arbitrariedad, aunque ésta pueda constituir el motivo central del agravio; tampoco suple la cuestión no justiciable si bien la revierte por la trascendencia que se exhorta.

En síntesis, no corresponde hacer lugar a la gravedad institucional, si el punto no es objeto de un serio y concreto razonamiento que demuestre de manera indudable la concurrencia de aquella circunstancia, o advierta a la Corte que su intervención es necesaria para remediar mucho más que los intereses de la parte.[334]

384.14. El *writ of certiorari* es un precepto que introdujo la ley 23.774, tomado del sistema judicial de Estados Unidos de América, por el cual el Tribunal Superior puede entrar a considerar el fondo de una causa superando obstáculos formales de admisión; la diferencia está en que en nuestro país, se le ha dado una práctica diferente, permitiendo a la Corte Suprema inhabilitar la instancia federal sin dar otro fundamento que la discrecionalidad para seleccionar las causas, con la sola invocación del precepto para rechazar el recurso extraordinario, sea ya por falta suficiente de agravios, por ser cuestiones insustanciales o carecer de trascendencia alguna.

Con el sistema no se resuelve el acierto o el error de la decisión recurrida, porque la providencia es una facultad discrecional que se funda en la selección de casos que tenga para la Corte interés o trascendencia suficiente. Es decir, más allá de los cuestionamientos constitucionales que importe esta disposición, la Corte puede rechazar el recurso sin razones que no sean alguna de los siguientes:

a) Simple invocación que la causa no se trata de alguna de las cuestiones que el art. 280 habilita (discrecionalidad técnica). Temperamento resistido por su contrariedad con el principio de que todas las sentencias han de ser fundadas.

---

[330] Es inadmisible el recurso extraordinario contra la sentencia que no importa un pronunciamiento contrario a los derechos de las apelantes, sino sobre la improcedencia de la acción instaurada —por ausencia de ilegalidad o arbitrariedad manifiesta— para poner en debate el respeto a esos derechos si tampoco existe gravedad institucional que justifique prescindir del requisito de sentencia definitiva previsto en el art. 14 de la ley 48 (CS, 2007/10/30, "*Comunidades Indígenas La Bendición y El Arenal c/Refinería del Norte S.A. (Refinor) y Conta S.R.L. s/amparo*", Fallos, 330:4606).

[331] El exceso incurrido por el juez, al reconocer una legitimación inexistente en la persona del peticionario, que se ha traducido en una inmotivada interferencia en la marcha de negocios públicos, de evidente importancia y repercusión político económica, configura un caso de gravedad institucional (CS, 1990/09/06, "*Dromi, José Roberto (Ministro de Obras y Servicios Públicos de la Nación) s/ avocación en autos: Fontenla, Moisés Eduardo c/ Estado Nacional*", Fallos, 313:863).

[332] Fallos, 281:379.

[333] Fallos, 279:291.

[334] Fallos, 303:221.

b) Cuestión federal insustancial; que supone la ausencia de alguno de los casos establecidos en el artículo 14 de la ley 48 y que por ello acarrea la denegatoria.

c) Cuestión insuficiente o carente de mínima fundamentación, en cuyo caso se invoca la ausencia de presupuestos o la falta de cumplimiento con los recaudos de la Acordada 4/2007.[335]

En suma, cuestión sin trascendencia, significa en algunos casos, interés o gravedad institucional inexistente; pero algunos consideran que esto es también comprensivo de asuntos, que sin incidir en el interés de la comunidad, presentan una proyección jurídica económica.[336]

384.15. La sanción de la ley 23.774 fue objeto de varias objeciones. La Corte Nacional, por ejemplo, en la Acordada 44/1989 se opuso al aumento del número de jueces integrantes del Superior Tribunal, aunque acompañó la selección discrecional de casos afirmando que ello no iba contra el sistema democrático, sino que afirmaba las potestades jurisdiccionales al mismo tiempo que reconocía una necesidad pragmática para reducir el número de expedientes.

Con relación al art. 280 fue planteada su inconstitucionalidad sobre la base de considerar que violaba los arts. 14, 16, 17, 18, 28 y 31 de la Ley Suprema. Esencialmente el problema estaba en la eventual desigualdad que provocaría la selección discrecional de causas ante la hipótesis de expedientes vinculados uno de los cuales no sea admitido frente a otro que reciba el placet de entrada. Está claro que lo inconstitucional no es la elección de cual entre ellos es más *trascendente*, sino de la difusa valoración entre los *intrascendentes* porque en igualdad de casos las soluciones deberían, por vía de principio, ser equivalentes.

El segundo conflicto con garantías sucede con el derecho a tener una decisión debidamente motivada, no siendo en principio así, el auto que "con la sola invocación de esta norma" —art. 280, Código Procesal—, puede expulsar del recurso extraordinario una causa eventualmente importante.

---

[335] Para Sagüés "[…] el nuevo art. 280 del Código Procesal alude, según vimos, a tres razones que autorizan nuestro *writ of certiorari*: a) *Falta de agravio federal suficiente*. Esta expresión ha sido criticada, y con motivo. ¿Cuál es la medida de lo "suficiente" o de lo "bastante"? ¿Cómo es posible imaginar que el derecho federal sea lesionado "poco" o "mucho"? ¿No es, acaso, un problema cualitativo, antes que cuantitativo, la infracción que una sentencia o un acto pueden hacer al derecho federal en juego? De todos modos, la nueva redacción del art. 280 del Código Procesal se remite a una reiterada terminología de la Corte Suprema de Justicia de la Nación…b) *Cuestiones insustanciales*. Bajo este rótulo la jurisprudencia de la Corte Suprema refiere, habitualmente, a recursos extraordinarios que objetan líneas jurisprudenciales firmes de la misma Corte, sin dar motivos valederos para apartarse de ellas. En tales hipótesis, puede haber "cuestión federal" de por medio, pero ella es baladí, o frívola, y no da lugar a la apelación federal extraordinaria. También se incluyen aquí supuestos de recursos extraordinarios que carecen de una fundamentación mínima; c) *Cuestiones sin trascendencia*. El concepto de "trascendencia", en el recurso extraordinario, se vincula con el de "interés" o "gravedad" institucional. Dicho de otra manera, un recurso extraordinario es "intrascendente", si no presenta un problema que tenga "interés" o "gravedad" institucional (SAGÜÉS, Néstor Pedro, *El "writ of certiorari" argentino (Las reformas de la ley 23.774, respecto al recurso extraordinario)*, La Ley, 1990-C, 717).

[336] PALACIO, Lino E., *El recurso extraordinario federal*, Abeledo Perrot, Buenos Aires, 1992, p. 204.

La apuntada "sana discreción" que nos consta fue prevista por Bidart Campos con una intención diferente a la que después se aplicó, jamás eludió la garantía que salvaguardia la fundamentación de toda sentencia; omisión que no queda salvada con la remisión a facultades discrecionales.

Para Sagüés:

> [...] la discrecionalidad sana parece referirse a un arbitrio legítimo, sensato, aproximadamente igualitario, y desde luego, no arbitrario, ni inequitativo, ni discriminatorio e irrazonable. En una palabra, la discrecionalidad sana es impuesta por la ley 23.774, y resultaría compatible con la Constitución. Pero la discrecionalidad no sana resultaría primero ilegal (por vulnerar el art. 280 del Código Procesal), y además inconstitucional (por atentar contra el debido proceso y la igualdad).[337]

Inclusive, la denegación sin otro argumento que la voluntad infundamentada, daría lugar a la aplicación del art. 46, inc. 2-b de la Convención Americana sobre Derechos Humanos, referida al acceso de las personas al sistema interamericano cuando el tránsito exigido por el derecho interno se obstruye indebidamente o se torna inútil y/o dilatorio.

La Corte, en una de las primeras observaciones que se efectuaron, salió del paso sosteniendo que la declaración de inconstitucionalidad del art. 280 del Código Procesal (modificado por la ley 23.774), debía plantearse en oportunidad de interponer el recurso extraordinario, ya que desde ese momento constituía una contingencia previsible que la Corte rechazara la vía intentada mediante el texto legal tachado de inconstitucional. No obstante esa inoportunidad, algunos dijeron que podían ser atendidos los agravios de conformidad con la consolidada tradición jurisprudencial tendiente a no impedir el esclarecimiento de relevantes temas constitucionales por mediar óbices procesales (voto de los Dres. Rodolfo C. Barra, Augusto César Belluscio y Antonio Boggiano).

Pero el permiso de análisis los condujo a sostener que el art. 280 del Código Procesal faculta a la Corte a ejercer su jurisdicción extraordinaria en casos de trascendencia, aún cuando existiera algún obstáculo formal para acceder a la misma; sin que la desestimación de un recurso extraordinario con la sola invocación de dicha norma importe confirmar ni afirmar la justicia o el acierto de la decisión recurrida.

En suma, el rechazo de un recurso extraordinario con la sola invocación del art. 280 del Código Procesal implica que la Corte ha decidido no pronunciarse sobre la presunta arbitrariedad invocada, por no haber hallado en la causa elementos que tornen manifiesta la frustración del derecho a la jurisdicción en debido proceso.[338]

384.16. La incorporación del *certiorari*, tras la experiencia habida desde su consagración legislativa, ha sido útil para rechazar recursos extraordinarios con la sola

---

[337] Sagüés, *El "writ of certiorari" argentino (Las reformas de la ley 23.774, respecto al recurso extraordinario)*, cit., La Ley, 1990-C, 717.

[338] CS, 1993/02/02, "*Rodríguez, Luis Emeterio c/ Rodríguez de Schreyer, Carmen Isabel y otro*", Fallos, 316:64.

invocación del art. 280 del Código Procesal; y al mismo tiempo, permitió tener un mecanismo de selección de causas cuando ellas se consideraron de trascendencia política o institucional. Precisamente, al invocar la trascendencia como motivo, se entabla un paralelo con la "gravedad institucional" que, como vimos, fomenta una causal más en el cuadro de cuestiones federales que permiten la intervención de la Corte. El interrogante que se formula es saber si actúan con independencia, o uno sustituye al otro, o bien, la trascendencia en un caso especial de gravedad institucional que obra en sus límites o con fronteras más amplias.

Para Gelli, la similitud entre el *certiorari* y la gravedad institucional deriva de que, en ambos, la Corte Suprema admite la revisión con fundamento en la trascendencia del caso. Y eso es todo, pues el primero fue establecido para restringir el control y el segundo para extenderlo.[339]

La jurisprudencia nacional fue definiendo la gravedad institucional con sentencias donde el concepto de *trascendencia* se releva más como adjetivo que como condición o presupuesto. De allí que se indiquen situaciones trascendentes (relevantes) de carácter constitucional, institucional, bienestar público, etc., que impactan en la buena marcha de las instituciones.

Pero la trascendencia también se aplica fuera de contextos, cuando se resuelve como presupuesto de admisión, sin tener en cuenta el compromiso con las instituciones básicas de la Nación,[340] las instituciones fundamentales del país[341] o las bases mismas del Estado,[342] donde la "gravedad institucional" toma cuerpo singular y la trascendencia actúa entre los recaudos procesales.

No obstante, en situaciones donde no hay cuestión federal la gravedad institucional sin mención de la trascendencia ha permitido entrar en el recurso extraordinario con el fin de preservar los principios básicos de la Constitución Nacional en casos que conmueven a la sociedad entera,[343] o cuando está afectada la buena marcha de las instituciones,[344] o cuando se trata de un conflicto que afecta a la conciencia de la comunidad.[345]

Puesto en práctica el *certiorari,* nos parece que la trascendencia excede la figura de la gravedad institucional. Con él se puede invocar el art. 280 y rechazar el recurso extraordinario con laconismo (no conveniente pero legal) como es el modelo norteamericano (*certiorari denied*); o denegarlo por falta de agravio federal suficiente, o cuando las cuestiones planteadas resultaren insustanciales; pero al mismo tiempo, el abogado que quiere anticiparse a una supuesta repulsa, debe motivar la cuestión de trascendencia.

---

339 GELLI, *El "writ of certiorari" en perspectiva*, cit., La Ley, 1994-B, 880.

340 Fallos, 289:36; 292:229; 307:973.

341 Fallos, 238:391.

342 Fallos, 306:250.

343 Fallos, 257:132.

344 Fallos, 300:417.

345 Fallos, 300:1110.

De allí que podamos distinguir las siguientes cuestiones federales: *a)* las directas y complejas que indica el art. 14 de la ley 48; *b)* las insustanciales pero de gravedad institucional; *c)* las que se fundan en la arbitrariedad de las sentencias, y *d)* las que ostentan trascendencia que interesan no sólo a las partes en el litigio sino también a la comunidad o a algún sector de ella.

384.17. La ausencia de orientación jurisprudencial, sumado a la discrecionalidad poco metódica de los fallos de la Corte, impide generar un esquema donde encuadrar situaciones donde la trascendencia pueda apoyarse siguiendo la actual tendencia de la Corte, cuando sostiene que:

> no obstante que las decisiones de la Corte se circunscriben a los procesos concretos que le son sometidos a su conocimiento, no cabe desentenderse de la fuerza moral que emana de su carácter supremo, sin verter argumentaciones que la contradigan, pues dada la autoridad institucional de los fallos del Alto Tribunal en su carácter de supremo intérprete de la Constitución Nacional y las leyes, de ello se deriva el consecuente deber de someterse a sus precedentes.[346]

Con esta pauta, se puede ofrecer una visión probable de cuestiones trascendentes. La primera llega de la mano de las que, indudablemente, son *cuestiones federales o constitucionales,* cuya relevancia está implícita en el deber de controlar la constitucionalidad de las leyes. Si se espera que la Corte federal sea la última intérprete de la Norma Fundamental no se ve posibilidad alguna para rehuir de esa misión con el argumento de la intrascendencia. En estos casos, el problema de eludir el recurso por ausencia de cuestión federal no es posible, por lo cual, como dice Guastavino "[…] de existir cuestión federal trascendente sería incorrecto que la Corte Suprema en ejercicio de la facultad selectiva discrecional conferida por la ley 23.774 rechazase el recurso extraordinario".[347]

En segundo lugar aparecen los *conflictos normativos derivados de leyes infraconstitucionales,* que siendo cuestiones federales tienen el mismo estándar que el recién expuesto. Aunque según Sagüés:

> [...] hay que distinguir entre interpretación de un precepto de derecho federal, y aplicación del mismo. La interpretación de una norma tiene comúnmente proyección (al menos eventual) a otros litigios. La aplicación (o efectivización de una regla a un caso concreto), puede que sí o puede que no, y de darse esta última situación, carecería de "trascendencia".[348]

El tercer orden de análisis se da con las *sentencias arbitrarias*, que según nuestra opinión, son pronunciamientos inconstitucionales porque violan el debido proceso en cualquiera de sus manifestaciones. Este es uno de los aspectos más conflictivos,

---

[346] CS, 2009/06/23, " *Romero, Carlos Ernesto c/Andrés Fabián Lema s/desalojo - recurso de casación e inconstitucionalidad*".

[347] GUASTAVINO, *Recurso extraordinario de inconstitucionalidad,* tomo I, cit., p. 488.

[348] SAGÜÉS, *El "writ of certiorari" argentino (Las reformas de la ley 23.774, respecto al recurso extraordinario*), cit., La Ley, 1990-C, 717 y ss.

porque la tendencia de la ley 23.774 fue, justamente, eludir con el *certiorari* los recursos fundados en la arbitrariedad, basados en lo *insustancial* o *intrascendente.*[349] Los tipos de arbitrariedad repercuten en la validez del fallo e inciden en los derechos de las partes y, a veces, se proyectan por la extensión y efectos de la cosa juzgada y el peso de la jurisprudencia.

Que sea una cuestión procesal (*v. gr.:* omisión de considerar prueba esencial) no disminuye el sacrificio al derecho de defensa en juicio, la inviolabilidad del derecho de propiedad o el derecho a la eficacia de la prestación del servicio jurisdiccional. Como consecuencia de ello, se comparte que:

> las reformas establecidas en la ley 23.774 sólo justifican extremar el rigor para considerar manifiestamente arbitrarias a las sentencias, pero en modo alguno —una vez acreditada esa palmaria causal descalificatoria de los pronunciamientos recurridos— pueden justificar el rechazo por intrascendente del recurso extraordinario donde se impugne la sentencia por tales vicios evidentes.[350]

El cuarto eslabón está puesto para las sentencias de *gravitación institucional,* que importan en sí mismas una cuestión federal trascendente, que debe demostrarse en la fundamentación del recurso. Es aquí donde la jurisprudencia del tribunal superior muestra su divagar, porque desde el caso "*Jorge Antonio*"[351] al presente, una misma línea de situaciones tiene interpretaciones distintas. Creemos así que no es solo la Corte quien debe orientar, sino el abogado, también, el que debe justificar razonadamente porqué entiende que el problema trasciende el interés de las partes.

El último escalón se instala con la *trascendencia, propiamente dicha*. Esta es la repercusión social, la evaluación de los efectos, la significancia del fallo, la urgencia del conflicto, etc. Para ellos el requisito de la cuestión federal es "intrascendente" aunque siempre exista una cuestión constitucional implícita desde que todos los derechos tienen un fundamento directo o mediato en la norma básica del Estado. Con esto quiere significarse que un asunto sin trascendencia normativa puede contar con trascendencia social, y entonces resultaría irrechazable el recurso extraordinario.[352]

---

[349] Para Sagüés hay que distinguir la arbitrariedad normativa de la fáctica. En materia de *arbitrariedad normativa*, los maxi errores de interpretación tendrán generalmente trascendencia, ya que una exégesis insalvablemente errónea, absurda, imprudente, inequitativa, etc., de una norma, importa un problema que puede exceder el mero interés de las partes y proyectarse a otras situaciones. Los maxi errores de aplicación, en cambio, podrán o no tener trascendencia, según las distintas situaciones. En cuanto la *arbitrariedad fáctica*, los maxi errores en la valoración de las pruebas (*v.gr.*, omisión de probanzas decisivas; sentencias basadas en pruebas inexistentes, o que no realizan una meritación razonable de las pruebas, etc.), conciernen habitualmente nada más que al caso específico donde se presenta el vicio, y no se proyectan (dada su singularidad) a otros expedientes. No habría pues aquí —en principio— "trascendencia". En síntesis, la "trascendencia" se emparentaría, *prima facie*, con asuntos de interpretación normativa, antes que con problemas de aplicación o de arbitrariedad fáctica (SAGÜÉS, *El "writ of certiorari" argentino (Las reformas de la ley 23.774, respecto al recurso extraordinario*), cit., La Ley, 1990-C, pp. 717 y ss.).

[350] GUASTAVINO, *Recurso extraordinario de inconstitucionalidad,* tomo I, cit., p. 491.

[351] Fallos, 248:195.

[352] SAGÜÉS, *El "writ of certiorari" argentino (Las reformas de la ley 23.774, respecto al recurso extraordinario*), cit., La Ley, 1990-C, pp. 717 y ss.

384.18. *El per saltum.* Otra de las manifestaciones diferentes del recurso extraordinario es la apelación "per saltum". Aquí el molde del remedio excepcional del art. 14 de la ley 48 solamente se aplica para demostrar la trascendencia relevante de la cuestión, y la urgencia que necesita su tratamiento para conseguir una sentencia definitiva. Como ésta únicamente se alcanza después de transitar por las instancias, el recurso pretende "saltarlas" y auspiciar que intervenga la Corte Suprema pese a la ausencia del requisito de sentencia definitiva, y eventualmente, de cualquiera de los demás presupuestos.

El salto de instancia o *by pass* como también se refiere a esta modalidad, puede constituir una herramienta distinta del recurso extraordinario si se considera que el motivo central que permite actuar a la Corte *ante tempus* obedece a la urgente necesidad de resolver definitivamente un caso de gravedad y trascendencia institucional.

Como se advierte, tanto la relevancia como la urgencia pueden dar lugar a la intervención del Alto Tribunal superando las actuaciones que le corresponden a los órganos competentes de la justicia. Sin embargo, un criterio tan amplio choca con garantías procesales como el orden público de la competencia, la intervención del juez natural, e inclusive, con el derecho a la doble instancia.

Cabe recordar que uno de los temas cruciales que debate esta figura es su constitucionalidad, la que suele presentar diferencias según se trate de causas federales o radicadas en un tribunal de provincia. En la primera hipótesis —dice Sagüés—:

> [...] la Constitución afirma que la Corte Suprema actúa por vía de apelación según las reglas y excepciones que determina el Congreso. Por tanto, nada impide que en algunas situaciones se pueda apelar de lo decidido por un juzgado de primera instancia a la Corte Suprema, en lugar de transitar el camino juzgado-cámara de apelaciones-Corte. Compete al legislador ordinario propiciar o no esa posibilidad, según pautas de oportunidad y conveniencia que hacen a su esfera privativa de decisión. Si el proceso se diligencia en sede provincial, el tema es más espinoso. La Constitución encomienda a las provincias atender en su ámbito jurisdiccional los asuntos concernientes al derecho común (códigos civil, comercial, penal, de minería, del trabajo y seguridad social), y por supuesto, los relativos al derecho local. Además ellas tienen el derecho y el deber de organizar su administración de justicia, con la consiguiente facultad de adoptar una estructura judicial determinada, con las instancias que ellas entiendan ser las mejores.
>
> ¿Es posible que por vía de ley o de jurisprudencia federal se autorice la absorción de una causa provincial de primera instancia por la judicatura nacional, en este caso por la Corte Suprema sin agotar las instancias locales? Nos parece que no, a pesar de la solución que alguna vez implementó la ley 27 (apelación de fallos de juzgados de primera instancia provinciales, hacia el juez federal de sección). El derecho constitucional provincial de juzgar, involucra la competencia para establecer las categorías jurisdiccionales de ese juzgamiento, sin interferencias ni sustracciones del poder federal, por más que éste sea el Poder Judicial de la Nación.[353]

El art. 117 de la Constitución asigna la intervención de la Corte Federal en instancia originaria y exclusiva, o por vía de apelación. La primera forma esta fuera del

---

[353] SAGÜÉS, Néstor Pedro, *Constitucionalidad de la apelación "per saltum"*, La Ley, 1989-B, 318.

circuito del salto de instancia desde que ella ya existe radicada en el Superior tribunal; en cambio, en el segundo caso, en cambio, la decisión de actuar no necesita revisar la causa ni resolver expedientes, son únicamente decisiones de política judicial las que impulsan a requerir el expediente para resolverlo de inmediato, de manera que no se ve asiento en derecho fundamental alguno.[354]

De allí que la doctrina prohíje a la apelación *per saltum* en el carril del recurso extraordinario federal, sin darle significado al simple interés de la Corte (a través de la actuación dispuesta de oficio o a petición de parte) de actuar anticipadamente a los tiempos que corresponden, en cuyo caso, la base siempre está en la gravedad institucional.

384.19. En cuanto a las reglas técnicas, el recurso extraordinario no escapa a las de cualquier otro medio de gravamen, solo agrega requisitos especiales y establece condiciones para la admisión que se imponen como presupuestos particulares del remedio.

Desde Imaz y Rey[355] se divide entre:

a) *Requisitos comunes*: es decir, aquellos que se acostumbra a pedir en todo recurso (*v. gr.:* que la sentencia provenga de un tribunal con jurisdicción ordinaria, militar o provenga de un organismo administrativo y/o legislativo; que el fallo sea emitido en una causa, y que sea ésta posible de revisar por el Alto Tribunal; que la parte tenga gravamen, vale decir, que pueda expresar los agravios constitucionales que con la decisión se afecta; que el perjuicio sea actual y que al tiempo de resolver la impugnación subsistan las causas que originan la queja).

b) *Requisitos propios*: que significa aquellos que solamente requiere el recurso extraordinario (*v. gr.:* cuestión federal; relación directa; resolución contraria al derecho invocado; sentencia definitiva y que ella provenga del Superior Tribunal de la causa).

c) *Requisitos formales*: esto son los que juegan en la etapa de admisión del recurso (*v. gr.:* introducción, reserva y mantenimiento de la cuestión federal; legitimación del recurrente; cumplimiento del lugar, tiempo y forma de la presentación del recurso).

Para Carrió, los requisitos comunes responden a similares recaudos, con mínimas diferencias: *a)* que haya intervenido un tribunal de justicia; *b)* que dicha inter-

---

[354] Bidart Campos, en cambio, argumenta sobre el art. 117 de la Constitución Nacional sosteniendo que cuando la norma habla de "apelación", quiere decir que allí conoce en una, instancia que "no es originaria", de forma tal que la jurisdicción "no originaria" deja sitio para que la ley la regule tanto mediante recurso (que es lo normal), como por "avocación" (que es lo excepcional), interpretación esta última que a su juicio no ofrece reproche constitucional siempre que —y esto es fundamental— exista una resolución de fondo sobre el asunto en instancia inferior y en caso de real apremio o interés institucional, pues de otra forma, por vía de ley se estaría ampliando la competencia originaria de la Corte federal; en cambio, existiendo pronunciamiento inferior, se estaría ampliando competencia "no originaria" (BIDART CAMPOS, Germán J., "*El "certiorari" y la "avocación" en la Competencia de la Corte Suprema (Innovaciones en un proyecto de reforma*", ED, 115-805).

[355] IMAZ, REY, *El recurso extraordinario,* cit., pp. 17 y ss.

vención haya tenido lugar en un juicio; *c)* que en él se haya resuelto una cuestión justiciable; *d)* que la resolución cause gravamen y *e)* que los requisitos subsistan en el momento que la Corte deba dictar sentencia.[356]

a) *Tribunal de Justicia:* El remedio federal sólo procede respecto de sentencias o resoluciones definitivas dispuestas por órganos jurisdiccionales. El concepto involucra a: *i)* todos los tribunales integrantes del Poder Judicial de la Nación y de las provincias; *ii)* los que ejerzan por ley facultades jurisdiccionales, como son los organismos administrativos que admiten la revisión de sus decisiones ante los tribunales de justicia, y *iii)* los tribunales superiores militares (art. 6°, decreto/ley 4055), aunque respecto de éstas la actual ley 23.049 altera el presupuesto, toda vez que introduce en el art. 445 *bis* del Código de Justicia Militar el recurso ante las Cámaras Federales de apelación respecto de las decisiones de carácter definitivo del Consejo Supremo de las Fuerzas Armadas en tiempos de paz.[357]

Originariamente, la interpretación fue que sólo los tribunales ordinarios de justicia eran pasibles de revisión por el recurso extraordinario federal. Tanto la ley 48 como la 4055 adoptaron el sistema judicialista a ultranza, dejando la revisión plena para los actos administrativos que fueron considerados no jurisdiccionales.

Recuerda bien Tawil que:

> […] en este aspecto las razones —totalmente extrañas a nuestra realidad histórico-política— que motivaron la aparición del principal sistema de justicia administrativa: el francés. Admirado durante décadas en nuestro país, el origen del sistema de justicia administrativa galo se encontró íntimamente relacionado con ciertas circunstancias históricas propias que derivaron en una interpretación del principio de separación de poderes inaceptable en la mente de nuestros padres fundadores. Efectivamente, producto del temor que había suscitado en los revolucionarios el desmedido poder ejercido por las cortes —en manos de la nobleza— durante el Antiguo Régimen, el sistema francés tantas veces elogiado —más por la destacada labor del Consejo de Estado y los restantes tribunales administrativos que por las verdaderas razones que justificaron su origen— resultó así consecuencia directa de aquella interpretación en virtud de la cual se suponía que juzgar a la Administración equivalía a administrar (*juger l'administration c'est encore administrer*).[358]

---

[356] CARRIÓ, Genaro R., "Nuevas fronteras del recurso extraordinario", en *Temas de casación y recurso extraordinario (en honor a Augusto Mario Morello)*, Platense, La Plata, 1982, pp. 212/213.

[357] Fallos, 307:1530; 308:1960. De acuerdo con este precepto, el recurso podrá deducirse: *a)* por la inobservancia o errónea aplicación de la ley; *b)* por la violación de las formas establecidas para sustanciar el proceso; *c)* cuando se limita el derecho de defensa, o se altere o debilite la posibilidad de ofrecer y producir prueba.

[358] TAWIL, Guido Santiago, *El recurso extraordinario y las decisiones emitidas por la Administración en ejercicio de funciones materialmente jurisdiccionales*, La Ley, 1990-E, 908 - Derecho Constitucional - Doctrinas Esenciales, Tomo IV, p. 725. Aquí agrega "[…] Imbuidos de la influencia norteamericana, nuestros padres fundadores optaron, al contrario, por seguir en la organización constitucional de la Nación Argentina una visión sustancialmente distinta. Con ese propósito, privilegiaron la interpretación imperante en Inglaterra, donde la existencia de un sistema de frenos y contrapesos no implicaba, en modo alguno, un aislamiento entre los distintos órganos del gobierno confinados al ejercicio de una función específica sino, por el contrario, la existencia de una coordinación sobre la base de la distribución entre el parla-

En síntesis, el recurso extraordinario procede contra decisiones jurisdiccionales provenientes de tribunales ordinarios o administrativos, comprendiendo en éstos últimos a quienes por resolver derechos de particulares, mantienen el remedio federal como resguardo de su garantías.[359]

b) *Causa o controversia:* La Constitución Nacional asigna jurisdicción a la Corte Suprema de Justicia en causas concretas, es decir, en conflictos suscitados ante el Poder Judicial donde el Alto Tribunal podrá intervenir en forma originaria o por apelación.

Si no existiera esa limitación, los jueces nacionales podrían, por propia iniciativa, revisar los actos de los otros departamentos de gobierno, o de los poderes provin-

---

mento, el monarca y las cortes de justicia de las tres funciones básicas, otorgándose a estas últimas la función de custodiar la legalidad del obrar administrativo. Claro ejemplo de ello resultó la redacción del art. 100 de nuestra Constitución, fundado en el art. III, secc. 2ª de su par norteamericana. Mucho más aún, el hecho de que nuestros constituyentes optaron —al seguir la senda abierta con la aprobación del Estatuto Provisional del 22 de noviembre de 1816 que prohibió al Poder Ejecutivo el ejercicio de cualquier tipo de jurisdicción y, fundamentalmente, las previsiones contenidas en la Constitución chilena de 1833 conocida a través del art. 93 del proyecto de Alberdi— por ratificar su voluntad de adoptar un sistema típicamente judicialista al expresar en el art. 95 de nuestra Ley Suprema que "en ningún caso el Presidente de la Nación puede ejercer funciones judiciales, arrogarse el conocimiento de causas pendientes o restablecer las fenecidas". Esta previsión —injusta e inexplicablemente soslayada— demuestra el especial énfasis puesto de manifiesto por ellos con el propósito de aventar toda duda respecto al sistema adoptado al incorporar un precepto inexistente en la constitución norteamericana de 1787, ejemplo hasta allí más claro de la vertiente judicialista".

[359] Las objeciones vertidas frente al limitado alcance de la revisión judicial posible en un recurso extraordinario y —principalmente— respecto al reconocimiento del ejercicio de funciones jurisdiccionales por parte de la Administración, llevaron a la Corte a intentar una solución eminentemente pragmática: superada por una práctica sólidamente arraigada en el ámbito administrativo, admitió la constitucionalidad del ejercicio de tales funciones en tanto existiera una revisión judicial suficiente, no garantizada, en principio, por la apelación extraordinaria. En esas condiciones, la controversia pasó de la ausencia o existencia de control por parte de los jueces ordinarios, al alcance que debía revestir éste. Esta problemática, particularmente visible en el caso de los llamados "recursos directos" es, sin duda, una de las principales que se plantean en el campo del derecho procesal administrativo. Sin embargo, en tanto presupone la existencia de una revisión judicial ordinaria —de novo o limitada— resulta ajena a la temática aquí abordada. La doctrina sentada por la Corte —invocada y utilizada con mayor frecuencia en las aulas universitarias que en la práctica judicial— debió haber derivado en dos consecuencias inmediatas. En primer lugar, en la rápida adecuación por parte del legislador de aquellas normas que limitaban el control judicial a fin de garantizar en todos los casos la existencia de una revisión suficiente de las decisiones administrativas en las instancias judiciales ordinarias. Segundo, en la toma de conciencia por parte de los litigantes que, en caso de persistir esa situación, los planteos de inconstitucionalidad de las limitaciones existentes debían efectuarse ante los jueces ordinarios. Ellas, sin embargo, no se produjeron en la forma y con la celeridad esperada. La reproducción de circunstancias fácticas como las antes mencionadas resultaron, en consecuencia, en extremo frecuentes, De modo similar, el loable afán de nuestra Corte de asegurar a los administrados el acceso a una instancia judicial plena la llevó a conocer nuevamente -con contadas excepciones- en recursos extraordinarios interpuesto directamente contra decisiones administrativas (TAWIL, *El recurso extraordinario y las decisiones emitidas por la Administración en ejercicio de funciones materialmente jurisdiccionales*, cit., La Ley, 1990-E, 908 - Derecho Constitucional - Doctrinas Esenciales, Tomo IV, pp. 725 y ss.).

ciales. Su autoridad sería, por consiguiente, superior a la unos y otros, e inconciliable con el principio de la división y equivalencia de los departamentos del gobierno nacional y con la autonomía de los gobiernos locales.[360]

La causa o asuntos, son expresiones que indican la necesidad de tener un debate entre partes en el que la cuestión a decidir trasciende el interés de ellas y, por tanto, admite que el Alto Tribunal pueda actuar sobre temas específicos (art. 116, CN) y como órgano exclusivo (jurisdicción originaria) o a consecuencia del recurso extraordinario (art. 117, CN).

El caso debe ser contencioso, es decir una asunto, *causa* o *controversia,* que significa la existencia de un litigio adversarial cuyos intereses enfrentados, a los fines del art. 14 de la ley 48, se resguardan con la decisión final de la Corte, siempre que no promedian alguna de las siguientes situaciones:

1°) *La cuestión debe ser justiciable,* que supone tener que resolver una causa válida, vigente, no imaginada ni imposible, en la que es menester que su dilucidación conduzca a decidir una situación de hecho real y concreta, y no se la haya planteado por vía de hipótesis, ni para establecer reglas para casos no sucedidos.[361]

Claro está que, cualquiera que fuese el procedimiento mediante el cual se propusiera a decisión de los jueces una cuestión justiciable, nadie puede sustraer a la esfera de acción del Poder Judicial la atribución inalienable y la obligación que tiene —emanada del art. 31 de la Constitución Nacional— de hacer respetar el Estatuto Fundamental.[362]

Por eso, mediante el concepto de cuestión justiciable se persigue evitar la invasión en la esfera de los otros poderes del Estado; permitiendo al recurrente, acudir a la justicia en defensa de sus derechos, y, a los magistrados judiciales, ejercer la facultad de revisar los actos de los otros poderes, limitada a los casos en que se requiere ineludiblemente su ejercicio para la decisión de los juicios regularmente seguidos ante ellos, en la medida que deben conocer y decidir todas las causas que versen sobre puntos regidos por la Constitución (art. 116).

2°) *No debe tratarse de una cuestión política.* Este es un problema que trasciende lo específico del recurso extraordinario, en la medida que se cuestiona la intervención de la justicia, desde el control de constitucionalidad, en las decisiones que se consideran privativas del gobierno y la administración.

> Una causa recurrente surge de alegar que se politiza la justicia. Carl Schmitt sostuvo que dar una expansión de semejante naturaleza a los jueces convertía a los tribunales en instancias políticas despojándoles su sentido jurisdiccional. A su entender ningún Tribunal especializado llega a conocer de verdaderos conflictos constitucionales, ni existe un proceso auténtico sea como criterio técnico o procesal en el que "[…] las partes en conflicto deben estar en una cierta relación a la Constitución de que resulte su papel de

---

360 Fallos, 190:142. *Cfr.* IMAZ, Esteban, REY, Ricardo E., *El recurso extraordinario,* Abeledo Perrot, Buenos Aires, 2000 (3ª ed.), p. 41.

361 IMAZ, REY, *El recurso extraordinario,* cit. 3ª ed., p. 51.

362 Fallos, 321:3620.

> partes en función de su legitimación activa y pasiva. Esta situación sólo podría darse cuando la Constitución fuese considerada como un contrato ... Pero la Constitución no es un contrato.[363]
>
> Agregó también un fundamento que luego se utilizó reiteradamente, destacando cómo se desnaturaliza la función judicial al convertirla, prácticamente, en un órgano legisferante, puesto que en definitiva de lo que se trata es de fijar el contenido de una ley. Las agudas observaciones de Schmitt no perdieron de vista el famoso "veto judicial" que a través de los tribunales constitucionales se lograba, llegando a cimentarse el no menos polémico gobierno de los jueces.

La composición de los tribunales representa una variante del problema, pues la adhesión —hipotética— a cierta línea de pensamiento (político) puede ocasionar condicionamientos o fidelidades; las que por esa maleable situación pueden arrojar decisiones vacilantes perjudicando la seguridad jurídica ante una jurisprudencia inconsistente.

Otra cuestión destacada fue la metodología que aplica este tipo jurisdiccional, pues se despoja del análisis de los hechos sobre los cuales toda sentencia funda sus decisiones, para tornar el estudio a un problema de naturaleza bien diferente como es el contenido de una norma jurídica, circunstancia que obra trascendente al mudar el sentido del pronunciamiento judicial.

Estas críticas abundan confrontando el paralelo de funciones jurisdiccionales ordinarias y constitucionales; pero no son únicas, ni el frente de ataque esta parcializado en estos aspectos.

En realidad, la idea de considerar cuestiones *no justiciables* está en retroceso. La idea que se mantiene es evitar que la Corte actúe donde no es necesario, sea porque se plantea el conflicto como una consulta, o se refiere a espacios donde el caso no tiene contenido constitucional, ni se trata de uno de los motivos que habilita el art. 14 de la ley 48. De allí que no interesa que la decisión sea política y, por tanto, que se presente como materia expurgada de la revisión judicial. Por ejemplo, se ha dicho que las decisiones en materia de los llamados juicios políticos o enjuiciamientos de magistrados en la esfera provincial, cuyo trámite se efectuó ante órganos ajenos a los poderes judiciales locales, configuran una cuestión justiciable en la que le compete intervenir a la Corte Suprema por vía de recurso extraordinario sólo cuando se acredita la violación del debido proceso legal.[364]

3°) *Se trate de cuestiones de derecho común o procesal sin quebrantamiento de derechos constitucionales.* Es decir, estamos ante las cuestiones no federales que tampoco ingresan por arbitrariedad, gravedad institucional o *per saltum*.

Las cuestiones de naturaleza fáctica y de derecho común y procesal resultan, por regla, propias de los jueces de la causa y ajenas a la instancia extraordinaria, salvo

---

[363] SCHMITT, *La defensa de la Constitución,* cit., p. 155.

[364] CS, 2006/02/07, "*Foro de Abogados de San Juan c/ juez del Juzgado de Paz del Departamento Judicial de San Martín*", Fallos, 329:12.

arbitrariedad manifiesta en la resolución en cuyo caso, mediando ese planteo entre otros, corresponde tratarlo en primer término, dado que, de verificarse tal circunstancia, no existiría sentencia propiamente dicha.

Los pronunciamientos judiciales que se objetan por la interpretación acordada a los hechos, o razonan los agravios con fundamentos de derecho sustancial no constitucional, son ajenos a la instancia superior, máxime si la sentencia se funda en argumentos no federales que, más allá de su acierto o error, resultan suficientes para sustentarla e impiden su descalificación como acto judicial.

c) *Gravamen:* Como en todo recurso, la presencia de gravamen o perjuicio es ineludible y necesario para cumplir con uno de los presupuestos comunes. La Corte repetidamente señala que la existencia de efectivo gravamen (no potencial, imaginado, ni contingente o probable) que afecte a quien deduce la apelación extraordinaria constituye uno de los recaudos jurisdiccionales cuya previa comprobación condiciona la admisibilidad del recurso,[365] estando a cargo del tribunal superior de la causa, la verificación de tal requisito.

El planteo debe referir con exactitud a la cuestión constitucional, indicando con claridad y fundamentos cuáles son los aspectos de la resolución atacada que generan la afectación a derechos fundamentales, y de qué manera impactan en el interesado.

Otra exigencia que debe estar presente en el gravamen es que *no debe derivar de la conducta discrecional de quien recurre,* principio similar al que rige en las nulidades procesales (art. 171, Código Procesal) y como una proyección de la doctrina de los propios actos.

Los agravios derivados de la propia conducta omisiva del recurrente no resultan susceptibles de suscitar la intervención de la Corte. Concretamente, si la ausencia de consideración del legajo personal y la historia clínica del apelante se debió a su inactividad en incorporarlos al expediente, no cabe atender a sus agravios, derivados de su propia conducta discrecional.[366]

Asimismo, el gravamen presentado debe ser *grave* o *trascendente* como para motivar la actuación del recurso, no debe tener encontrar reparación por otras vías[367] y obviamente, todo agravio deducido en los términos del art. 14 de la ley 48 debe ser *federal*.[368]

d) *Gravamen actual y subsistente:* El gravamen debe ser *actual* y perdurar hasta que se resuelva el recurso, de otro modo, la cuestión deviene abstracta y pierde sentido la rogatoria ante el tribunal superior. En tales supuestos, se torna inoficiosa la intervención, porque las sentencias de la Corte Suprema deben ceñirse a las circunstancias cuando se dictan, aunque sean sobrevinientes al recurso extraordinario,

---

[365] Fallos, 256:327; 267:499; 303:1852; 315:2125, entre otros.

[366] Fallos, 311:358; 308:1478 y 540, entre otros.

[367] Fallos, 306:637.

[368] MORELLO, *El recurso extraordinario,* cit., p. 233.

pues la subsistencia de los requisitos jurisdiccionales es comprobable de oficio y su desaparición importa la del poder de juzgar.[369]

No obstante, hay situaciones que al quedar consumadas y perder así la reparabilidad del perjuicio que se ofrece, permiten a la Corte continuar el interés por la trascendencia del caso, que por su propia naturaleza, conserva la necesidad de definir desde la jurisprudencia superior, una posición que oriente para el futuro.

384.20. La especialidad del recurso extraordinario obliga a dar cumplimiento con otros recaudos que exigen alegación y fundamentación, es decir que no basta con invocar su existencia, porque al mismo tiempo se debe demostrar cada uno de ellos.

Es el campo de: *a)* las cuestiones federales, y a partir de ellas, es preciso demostrar que: *b)* tienen una relación directa con el asunto donde el recurso se interpone; *c)* que se ha resuelto en forma contraria a la Constitución Nacional o su doctrina; *d)* que la sentencia es definitiva y *e)* que proviene del Superior Tribunal de la Causa.

Cada requisito supone fundamentación autónoma, y globalmente el recurso tiene que ser autosuficiente para encontrar en esa motivación la suficiencia de razones que eviten tener que confrontar el expediente. Cuando ello no ocurre, el extraordinario no satisface el cumplimiento de los requisitos propios y, por tanto, se debe desechar por inoficioso.

a) *Las cuestiones federales:* Las cuestiones constitucionales se presentan en dos grandes campos:

a) Las llamadas *cuestiones constitucionales "simples"*; y las

b) *cuestiones constitucionales "complejas"*.

Las primeras se vinculan siempre con la interpretación directa de normas o actos de naturaleza federal que ponen en crisis a disposiciones de la Constitución Nacional. Las segundas, en cambio, se ocupan de los denominados "conflictos de constitucionalidad", es decir, al enfrentamiento entre normas o actos de carácter infraconstitucional con la Carta Fundamental.

En las *cuestiones simples* es deber del interesado demostrar el agravio constitucional, porqué el derecho común o local está fuera de la posibilidad interpretativa que puede realizar el juez de la causa. En su lugar, la tarea de inteligencia y encuadre en el principio de la supremacía recae sobre la propia Constitución federal, las leyes federales, los tratados, los decretos reglamentarios de leyes federales, los reglamentos autónomos del poder ejecutivo, y los actos federales de órganos del gobierno nacional.

El planteo de las *cuestiones complejas*, a su turno, muestran dos senderos. Uno transita la colisión entre una norma infraconstitucional (*v. gr.:* ley local o federal; actos de autoridad local o federal, etc.) con la Constitución. Estas se llaman cuestiones constitucionales "*complejas directas*". El otro se refiere al enfrentamiento entre normas o actos de autoridades federales, con otras de similar carácter o condición (*v.*

[369] Fallos 328:3996.

gr.: entre un decreto reglamentario y una ley; entre una ley federal y un decreto provincial; entre actos federales y provinciales, etc.). A estas se las conoce como cuestiones constitucionales "*complejas indirectas*".

En las *cuestiones federales complejas directas* la actuación de la Corte tiende a resolver la impugnación de una norma o de un acto que se estima incompatible con la Constitución, con prescindencia de otra norma o acto. De este modo la interpretación inmediata que realiza en el sistema anterior, ahora tiene otra etapa: primero, fija el alcance o significado de la norma y después verifica su constitucionalidad. Si las leyes impugnadas son, en cambio, normas o actos de derecho común o local, el Tribunal cimero comienza por atenerse a la interpretación acordada a aquéllos por el órgano judicial inferior -que cuenta para ello con facultades propias y exclusivas conforme a lo dispuesto en los artículos 75 inc. 12 y 122 y siguientes de la Constitución, correspondiendo únicamente resolver si tal interpretación —que no puede ser practicada sin riesgo de trasgredir los límites trazados a la competencia federal—, es o no compatible con los preceptos constitucionales que se estiman vulnerados.

> En estos casos —explican Imaz y Rey— la Corte Suprema tiene que partir de la base de que la norma, o el acto, dice lo que el tribunal de la causa declara que dice. El recurso extraordinario no autoriza a revisar esa interpretación, sino a decidir si interpretados en la forma que lo han sido, son o no constitucionales. Porque también para los supuestos de cuestiones federales complejas rigen las limitaciones impuestas a la justicia federal por la Constitución Nacional.[370]

Finalmente, en el caso de *cuestiones federales complejas indirectas,* la inconstitucionalidad de una norma o acto se funda en su incompatibilidad con otra norma o acto que, de acuerdo con la Norma Básica, reviste carácter preeminente. Es claramente una afrenta al principio de la supremacía constitucional (art. 31), y obliga a la Corte a actuar con el mismo doble sentido ya apuntado: primero, establecer el alcance de la norma y después resolver su ajuste con la Constitución.

Si, por el contrario, las normas en conflicto no revisten carácter federal, la actividad del tribunal debe atenerse a la interpretación que de ellas haya formulado el órgano judicial inferior, careciendo por lo tanto de facultades para rever la declaración de compatibilidad o de incompatibilidad que respecto de esas normas o actos contenga la resolución recurrida (arts. 75 inc. 12, 121, 122, 126 y siguientes de la Constitución Nacional.

Como se observa, todas las cuestiones federales asientan en conflictos de interpretación constitucional o legal, o bien sobre actos emanados de autoridades de la Nación, y siempre que la decisión adoptada sea contraria a lo que ellas disponen, como se verá en el requisito específico.

En consecuencia, son temas de derecho, de allí que las causales de arbitrariedad que, por vía de principio, se refieren a situaciones de hecho, como la misma grave-

---

[370] IMAZ, REY, *El recurso extraordinario,* cit., 3ª ed., pp. 136 y ss.

dad institucional, o la trascendencia del caso (art. 280, Código Procesal), cuando se articulan como fundamento central del recurso, tienen la necesidad ineludible de demostrar el enclave con la Constitución, sea mediante la invocación al debido proceso (art. 18, 43, 75.22, CN), o demostrando el conflicto normativo.

b) *Relación directa:* La procedencia formal del recurso extraordinario depende de las cuestiones federales, y dentro de ellas es necesario acreditar que la misma guarda una relación directa e inmediata con lo resuelto en la causa.

Este es un requisito del art. 15 de la ley 48, al decir que, "cuando se entable el recurso de apelación que autoriza el artículo anterior deberá deducirse la queja con arreglo a lo prescripto en él, de tal modo que su fundamento aparezca de los autos y tenga una relación directa e inmediata a las cuestiones de validez de los artículos de la Constitución, leyes, tratados o comisiones en disputa".

La relación directa e inmediata debe demostrarse, no basta la simple invocación. Hay veces que la remisión del recurrente a los preceptos constitucionales que considera violentados considera bastantes, sin serlo, porque es propio de la técnica de fundamentación indicar cuáles son las afectaciones sufridas, de qué manera perjudica al interesado, y si ellas fueran de derecho común, tendrá que razonar suficientemente la articulación con las cuestiones federales.

c) *Resolución contraria:* La cuestión federal invocada tiene que haber sido resuelta en forma contraria al basamento constitucional que consagra la Norma Fundamental, o una ley, decreto o disposición de una autoridad nacional. Lo de "contraria" significa que la sentencia atacada prefiere dar validez a un acto que contraría el principio de supremacía.

La decisión que se adopta en contra de una cláusula constitucional tiene diferencias de resultados cuando se está frente a una *cuestión federal simple*. En estos casos, basta con demostrar la violación al precepto para tener fundado este extremo del recurso. Peor cuando se trata de *cuestiones complejas* la compatibilidad de normas o actos locales con la Constitución tiene aristas diferentes porque, cabe recordar, que las autonomías provinciales permiten consagrar cartas constitucionales propias, que obviamente, no pueden contrariar el principio de la Norma Fundamental de la Nación, pero que encuentra posibilidades expansivas que al confrontarse, no encuentran un alojamiento preciso para deducir ciertamente la violación a dicha supremacía.

Es decir, cuando el art. 14 inciso 3º de la ley 48 dice que procede el recurso extraordinario cuando se pone en juego la inteligencia de alguna cláusula de la Constitución, o de un Tratado o ley del Congreso, o bien, de una comisión ejercida en nombre de la autoridad nacional, está indicando que la decisión es adversa o opuesta al uso corriente o a la aplicación general que se tiene acordada, llevando entonces el pronunciamiento a vulnerar la validez del título, derecho, privilegio o exención que se funda en la cláusula constitucional que es materia de litigio.

d) *Sentencia definitiva:* Sólo se pueden apelar ante la Corte federal las sentencias definitivas pronunciadas por los superiores tribunales de provincia, y por las cámaras federales y de la "justicia nacional".

Tanto el Código Procesal (art. 289) como la jurisprudencia afirman que sentencia definitiva es la que pone fin al pleito e impide su continuación. Pero este solo requisito no torna viable el recurso, porqué además, el pronunciamiento debe generar con esa definitividad un gravamen de imposible o insuficiente reparación ulterior.[371]

La problemática de la exigencia ritual asienta en la equiparación de muchas decisiones que, dejando abierta la revisión en otro proceso o resolviendo antes del pronunciamiento final, importan definiciones que se vuelven irreversibles provocando claras afecciones en los intereses de quien lo padece.

e) *Superior Tribunal de la causa:* Este requisito del recurso extraordinario se vincula con la determinación del órgano judicial del que emana la sentencia que la Corte Suprema entenderá mediante el recurso extraordinario. Está previsto al comienzo del art. 14 de la ley 48 y, pese a que la norma es clara cuando se refiere a los "tribunales superiores de provincia", la definición no ha encontrado, por mucho tiempo, interpretación concordante.

El recaudo contenido en el art. 14 de la ley 48 según el cual es menester que la sentencia atacada haya sido dictada por el tribunal superior de la causa ha sido descripto por Imaz y Rey como el órgano jurisdiccional que debe decidir en última instancia, dentro de la respectiva organización procesal, la cuestión federal se disputa. O sea sin recurso alguno para ante otro tribunal, fuera de la Corte Suprema de la Nación.[372]

384.21. Los *requisitos formales del recurso extraordinario* difieren de aquellos que se establecen para los demás recursos. Algunos de ellos dependen del principio de eventualidad, es decir, de la precaución que haya tenido el interesado en anunciar que el conflicto suscitado podría llevarlo ante los estrados de la Corte federal si la decisión sobre las cuestiones federales fuera contraria a las pretensiones que se fundan en normas constitucionales. Otras dependen del carácter y personalidad de quien formula la impugnación, y, finalmente, la formalización de exigencias incorporadas en la Acordada 4/2007 que significa un cambio profundo en la presentación del recurso extraordinario y la queja por su denegación.

a) *Introducción, reserva y mantenimiento de la cuestión federal:* La admisión del recurso extraordinario exige verificar que la Corte puede resolver la causa donde se plantea porque en ella existen cuestiones federales oportunamente planteadas. La introducción (art. 14, ley 48) tiene por objeto permitir que el tema de agravio haya sido sometido a las instancias ordinarias y debatido en ellas, evitando así lo que constituye una reflexión tardía de las partes. Habitualmente, la cuestión federal se anuncia (reserva) sosteniendo que el problema en ciernes pone en tela de juicio alguna de las previsiones contempladas en los incisos del mencionado art. 14.

---

[371] Fallos, 242:460; 245:204; 248:402; 307:784, etc.

[372] IMAZ, REY, *El recurso extraordinario,* Nerva (2ª ed.), cit. p. 217; Fallos, 66:257; 99:228; 149:427; 158:197 y 200.

Tanto la introducción como el mantenimiento de la cuestión federal no requiere de fórmulas sacramentales, pero es preciso observar que muchas veces el conflicto no centra el debate en asuntos constitucionales (aunque el fundamento sea mediato sobre ellos) sino de derecho común. En tal caso, este problema que no se da con las cuestiones federales simples, aparece con las complejas, donde el requisito de introducción debe agregar las normas fundamentales que se verían afectadas en la hipótesis de una decisión contraria.

b) *Legitimación:* La legitimación difiere del interés que antes tratamos. En este caso se trata de resolver quienes son los portadores de la cuestión federal que pueden ser parte en el recurso extraordinario. Obviamente, quienes son "justas partes" del litigio tienen legitimación procesal, sin diferenciar el tipo de proceso desde que lo esencial, en tal caso, es la definición de sentencia definitiva. Tampoco interesa la calidad del litisconsorcio que la parte integre, sin perjuicio de los efectos que se produzcan. Inclusive, los terceros adhesivos (art. 90 inciso 1°, Código Procesal) y aun los que suelen quedar presentados como "partes transitorias o incidentales" como los abogados y peritos en orden a los honorarios regulados en las actuaciones.

Según Palacio:

> [...] no ofrece dificultad alguna el caso del litisconsorte originario o del tercero que habiendo sido debidamente citados para intervenir en el proceso lo hacen recién para interponer el recurso extraordinario federal contra la sentencia definitiva o alguna resolución que les ocasiona gravamen irreparable. El juez o tribunal de la causa debe, en tal hipótesis, conferir traslado a las partes interesadas y, contestado éste o vencido el plazo para hacerlo, pronunciarse sobre la admisibilidad de la impugnación (art. 257 párr. 2°, Código Procesal). Es en cambio distinto el supuesto del interviniente voluntario (simple o litisconsorcial) que comparece con la misma finalidad precedentemente referida. En razón de que aquél puede presentarse cualquiera sea la etapa o instancia en que el proceso se encuentre (art. 90, Código Procesal), la interposición del recurso extraordinario configura sin duda un acto de intervención provisto de aptitud para convertirlo en parte, pero como tal conversión no es automática en tanto se halla supeditada a la prueba que produzca el interviniente acerca de la calidad invocada y a la resolución que corresponde dictar en el supuesto de mediar oposición de cualquiera de las partes originarias (art. 92, Código Procesal), simultáneamente con aquella interposición el interviniente voluntario tiene la carga de acreditar su interés o legitimación y el juez o tribunal el deber de conferir traslado a las mencionadas partes. Por lo tanto, el juez o tribunal debe diferir la concesión del traslado previsto en el artículo 257, segundo párrafo del Código Procesal hasta tanto venza el que corresponde otorgar a los litigantes originarios o, en su caso, exista decisión favorable a la admisibilidad de la intervención.[373]

c) *Lugar, tiempo y forma (Acordada CS 4/2007):* El recurso extraordinario se deduce por escrito que se presenta ante el Superior Tribunal de la causa, o quien haya pronunciado la sentencia definitiva. Se interpone fundado en el lugar donde está el asiento del tribunal aunque éste no conserve el expediente por haberlo remitido a otras instancias para que fueran ellas quienes practicasen las notificaciones de rigor.

---

[373] Palacio, *Recurso extraordinario federal,* cit., pp. 32 y ss.

Corresponde aclarar que cuando las resoluciones son inapelables por disposición legal (*v. gr.:* arts. 78 a 92 de la ley de procedimiento impositivo n° 11.863), el superior tribunal de la causa es el juez de primera instancia que ha dictado la sentencia definitiva o la resolución equiparable a tal. Por ello el recurso extraordinario se debe efectuar ante ese magistrado.[374]

Cuando la presentación se concreta por error y el tribunal que asienta el cargo de recepción lo remite al competente, la fecha de ingreso no se tiene en cuenta sino la de recepción por el último, en cuyo caso, solamente será admisible si llega dentro del plazo de diez (10) días contados desde que fue notificado el recurrente de la sentencia definitiva.[375]

> De todos modos, como en tantas cuestiones más donde la Corte es flexible para el cumplimiento de los requisitos formales (enseguida veremos si continúa esta línea después de la Acordada 4/2007) ha dicho que, si bien es requisito de los actos procesales, como el de deducir el recurso del art. 14 de la ley 48, que se realicen ante el órgano judicial correspondiente, de manera que el cargo puesto al escrito respectivo cobre la validez que de esa observancia dimana, ello no debe ser entendido como la enunciación de un principio inflexible, que ineluctablemente lleve a desconocer validez a toda actuación que de él se separe. Este criterio deriva de un concepto del proceso civil que impide su conducción en términos estrictamente formales, pues no se traduce en el cumplimiento de ritos caprichosos, sino en el desarrollo de procedimientos destinados a establecer la verdad jurídica objetiva que es su norte. La custodia de las formas a que deben ajustarse los procesos, depositada en los magistrados judiciales es cometido que deben éstos cumplir atendiendo en todo momento al fin último a que aquéllos se enderezan, que no es otro que contribuir a la más efectiva cuando eficaz realización del derecho […]. En consecuencia, "corresponde admitir la validez de la interposición del recurso extraordinario si el error de hecho en que se incurrió acerca del órgano en que fue presentado, se muestra excusable, máxime cuando cabe desechar la búsqueda, por el interesado, de algún objetivo censurable, atento el estado de la causa".[376]

El *plazo* para interponerlo es de diez (10) días contados a partir de la notificación de la resolución que se apela. Es un plazo general para todo tipo de procesos de manera que no interesa la celeridad o urgencia que tenga el expediente donde el recurso se deduce. Por supuesto tiene la ampliación prevista en el art. 158 del Código Procesal, aplicándose las reglas y términos de este ordenamiento; pero la notificación de la sentencia definitiva trabaja con el sistema procesal de la jurisdicción local competente. Sin que ello determine modificar el régimen federal, pues la resolución sobre el cómputo del término, a los efectos de decidir si el recurso extraordinario fue interpuesto en plazo, es propia del superior tribunal de la causa cuando se pronuncia sobre la admisibilidad.[377]

---

[374] Palacio de Caeiro, Silvia B., *Recurso extraordinario federal,* Alveroni, Córdoba, 1997, p. 267.

[375] Fallos, 306:616.

[376] Fallos, 306:738.

[377] Fallos, 108:353; 112:73; 123:113; 137:30; 180:16; 240:422; 242:15 y 521; 247:124; 250:85; 251:524; 254:113; 256:339; 290:381; 298:432; 307:2029, entre muchos más.

Dejamos para el final las *formas*. El art. 257 del Código Procesal exige la presentación por escrito respetando a consigna que ya estaba en el art. 209 de la ley 50. Como toda pieza debe estar firmada por el recurrente o sus mandatarios (art. 1012, Código Civil), el patrocinio letrado de abogado con matrícula federal, la constitución de domicilio en Capital Federal, y el acompañamiento de las copias en número suficiente para sustanciar el recurso.

La técnica es otra constante a resolver para alcanzar la posible interpretación de ajuste constitucional que se pretende. Esta es una de las herramientas más difíciles de lograr en los recursos extraordinarios.

La exigencia de fundamentación autónoma, muchas veces cargada de rigideces extremas, obliga a un laboreo intenso donde el abogado no puede eludir, prácticamente, ninguno de los pasos previstos -aunque no especificados- que permitan la atención de la Corte Suprema de Justicia de la Nación.

A la solemnidad inicial, característica de los presupuestos o requisitos de admisibilidad formal, deben sumarse los fundamentos intrínsecos de cada uno de los motivos que contienen la motivación del gravamen. Para ello existen pautas jurisprudenciales que orientan sobre un método posible. Así, es posible verificar que la mera enunciación de principios no es bastante, pues debe requerirse cuanto menos, la demostración cabal de acierto o del error del juzgador a quien se impugna su sentencia.

Es muy copiosa la casuística que observa el desarrollo de esta vía excepcional, aunque puede resultar posible esquematizar dos andariveles principales: el *recurso extraordinario clásico* y el que motiva la *arbitrariedad de la sentencia*.

En ambos casos, las reflexiones siguientes son comunes, aun cuando es preciso reconocer matices muchos más intensos en el segundo de los carriles.

Las variadas gamas de agravios admiten el reproche de una sentencia. Por ejemplo: *a)* la omisión de tratamiento de cuestiones planteadas, o de prueba decisiva para la resolución efectiva de la causa, o la ausencia absoluta de consideración de una defensa estimada como principal, etc.; *b)* la calificación errónea del derecho aplicable, o la interpretación equivocada o ilógica que pugna con los antecedentes de la causa, etc.; *c)* la consagración de un grave desequilibrio entre las prestaciones recíprocas que llegan a desfigurar el caso propuesto determinando su pérdida de sentido, entre otras causales de posible explanación.

La Corte, al analizar cada hipótesis planteada, cuadrará sus principios de atención. En primer lugar, verificará si los requisitos formales de admisión se encuentran cumplidos (de manera que revisa la admisión del órgano apelado); después, centrará el foco en la pertinencia argumental. En ambas situaciones, no es posible descartar la aparición del supuesto ingresado por el art. 280 del Código Procesal, por el cual se permite cierta discrecionalidad y aligeramiento en el estudio preliminar y sobre el fondo de los motivos que porta el recurso; como de la expulsión del remedio con el argumento de no estar cumplidos los recaudos de la Acordada 4/2007.

384.22. *Trámite del recurso extraordinario*. El recurso extraordinario deberá ser interpuesto por escrito, fundado con arreglo a lo establecido en el art. 15 de la ley

48, ante el juez, tribunal u organismo administrativo que dictó la resolución que lo motiva, dentro del plazo de diez (10) días contados a partir de la notificación (art. 257, Código Procesal).

De la presentación en que se deduzca el recurso se dará traslado por otros diez (10) días a las partes interesadas, notificándolas personalmente o por cédula. Contestado el traslado, o vencido el plazo para hacerlo, el tribunal de la causa decidirá sobre la admisibilidad del recurso. Si lo concediere, previa notificación personal o por cédula, de su decisión, deberá remitir las actuaciones a la Corte Suprema dentro de cinco (5) días contados desde la última notificación. Si el tribunal superior de la causa tuviera su asiento fuera de la Capital Federal, la remisión se efectuará por correo, a costa del recurrente. La parte que no hubiera constituido domicilio en la Capital Federal quedará notificada de las providencias de la Corte Suprema por ministerio de la ley (art. 257, Código Procesal).

El procedimiento para la concesión del recurso difiere según se atienda la admisibilidad (formal) o la procedencia (mérito sobre el fondo). El recurso extraordinario federal se rige en cuanto a tiempos y formas por las disposiciones ordenatorias del código, que obliga a los jueces locales —en tanto órganos resolutivos de la admisión inicial— a ejecutar los plazos allí dispuestos.

De todos modos se ha dicho que, si bien el plazo para la interposición de un recurso extraordinario es de diez (10) días contados a partir de la notificación de la resolución que lo motiva, la decisión del tribunal de aclarar la resolución de fondo, debe entenderse como parte integrante de la misma, por lo que, el término legal debe computarse a partir de la notificación de esta última.[378] El plazo es individual y corre para cada una de las partes.

Apuntaríamos como situación excepcional el posible acuerdo entre las partes para suspender los plazos procesales; el que, de no mediar, deriva en la utilización lisa y llana de los tiempos perentorios y fatales consagrados.

Todo el trámite se sustancia ante el órgano local que fue (es) Superior Tribunal de la Causa. Las cuestiones eventuales que se suscitaran se notifican en el domicilio donde tramita la causa, porque el domicilio legal que se debe constituir en Capital Federal al presentar el recurso, tiene aplicación una vez que el expediente radica en la jurisdicción federal.

En contadas ocasiones, cuando:

> las cuestiones federales exhiban inequívocas y extraordinarias circunstancias de gravedad, y demuestren con total evidencia que la necesidad de su definitividad y solución expedita es requisito para la efectiva y adecuada tutela del interés general, las importantes razones que fundan la exigencia de tribunal superior deben armonizarse con los requerimientos formales, para que el marco normativo que procura la eficiencia del Tribunal no conspire contra la eficacia de su servicio de justicia al que, en rigor, debe tributar todo ordenamiento procesal.[379]

---

[378] CNPenal Económico, Sala A, 1999/08/05, "*Iglesias, Marcelo y otra*", La Ley, 2000-A, 217.

[379] Referimos al conocido caso "Dromi", caratulado "*Fontela, Moisés Eduardo c/ Estado Nacional*", sentenciado el 6 de setiembre de 1990.

El supuesto de la apelación "per saltum" elude en el caso que precede la definitividad de la sentencia, como el principio de radicación o lugar donde debe deducirse el remedio extraordinario, bajo el argumento de evitar consecuencias irreparables.

384.23. *Contestación del recurso extraordinario.* La notificación que se realiza a la parte contraria a la que deduce el recurso extraordinario tiene por finalidad permitir a cada litigante ejercer con plenitud el derecho de defensa.

> Si bien algunos opinan que "[…] el responde debe cumplir iguales exigencias que el escrito de interposición, en orden a la temporaneidad, completividad de la presentación, fundamentación correcta, etc.",[380] pensamos que no es completamente así, porque la sustanciación del recurso no obliga a contestarlo, ni implica una tácita aceptación ni admisión del mismo; de hacerlo, la réplica al extraordinario se sostiene en las eventuales deficiencias que pueda contener la pieza que se responde, o bien, por no haber cuestiones federales, o alguna otra carencia de tipo formal o sustancial. Pero la contestación en sí misma, no es un respaldo a la sentencia del tribunal superior, sino la respuesta al remedio que se plantea.

Excepcionalmente se puede prescindir del traslado del recurso, tal como sucede cuando la decisión impugnada es una resolución que desestima una medida cautelar o se trata de un recurso interpuesto fuera del plazo legal o en la hipótesis de que presentado el escrito sin firma de letrado o sin copias, el recurrente no supla la omisión dentro de los dos días siguientes al de la notificación, por ministerio de la ley, de la providencia que exige el cumplimiento de las cargas pertinentes.[381]

384.24. *Suspensión de la causa. Ejecución provisional de la sentencia.* El art. 258 del Código Procesal prescribe lo siguiente:

> Si la sentencia de la cámara o tribunal fuese confirmatoria de la dictada en primera instancia, concedido el recurso, el apelado podrá solicitar la ejecución de aquélla, dando fianza de responder de lo que percibiese si el fallo fuera revocado por la Corte Suprema.
>
> Dicha fianza será calificada por la cámara o tribunal que hubiese concedido el recurso y quedará cancelada si la Corte Suprema lo declarase improcedente o confirmase la sentencia recurrida. El fisco nacional está exento de la fianza a que se refiere esta disposición.

La norma parece indicar que, una vez que el recurso extraordinario se concede, se debe prestar fianza a satisfacción del superior tribunal de la causa, y con ello se podría iniciar la ejecución. Sin embargo la cuestión no es tan clara.

El art. 499 del Código Procesal permite ejecutar la sentencia cuando ésta se encuentra firme o ejecutoriada; mientras el art. 258 que analizamos, admite que se

---

[380] PALACIO DE CAEIRO, *Recurso extraordinario federal,* cit., p. 269.

[381] PALACIO, *Recurso extraordinario federal,* cit., p. 314. Con la opinión contraria de Morello que afirma que […] "este criterio es de interpretación estricta y que, de haber dudas, deberá sustanciarse" (*El recurso extraordinario,* cit., 3ª ed., p. 655).

fuerce el cumplimiento de la condena si la sentencia de Cámara fuera confirmatoria de la dictada en primera instancia [...].

Quiere decir que hay dos problemas a superar. El primero se vincula con la eventual suspensión de los efectos de la condena mientras esté tramitando el recurso extraordinario (se entiende que ante el tribunal de admisión formal); el segundo, debe resolver si la ejecución inmediata es factible prestando fianza suficiente sin importar la articulación del remedio excepcional.

> La Corte Suprema de Justicia de la Nación ha interpretado la situación en tres casos orientadores: el primero es "*César Arias*"[382] donde dijo que la sentencia no se podía ejecutar porque la sola interposición del recurso genera efectos suspensivos. Más tarde, en el expediente "*Jorge Escobar",* se sostuvo que al haber deducido los peticionarios el recurso extraordinario contra las sentencias de la Cámara Electoral, ésta no resulta susceptible de ejecución —art. 499, Código Procesal— y, por lo tanto, hasta que el tribunal no se pronuncie con respecto a la concesión o denegación del recurso federal no se puede ejecutar ningún pronunciamiento.[383]
>
> Finalmente en "*Gabriela Oswald"*[384] se decidió que no es la concesión sino la *interposición* del recurso extraordinario lo que produce efectos suspensivos, en tanto los jueces de la causa no se pronuncien sobre su admisión o rechazo.

La Corte, en suma, sostiene que mientras el recurso extraordinario no esté resuelto en la etapa de admisión no se puede ejecutar la sentencia. Pero cabe interrogarse si concedido el recurso ¿se mantiene la suspensión a tenor de lo dispuesto en el art. 258?

La pregunta no es baladí, pues algunos tribunales no esperan diez días desde la notificación para devolver el expediente a la instancia apelada, pudiendo en ésta, en consecuencia, iniciar la ejecución. Pero, si articulado el recurso extraordinario éste se concede, la sentencia deja de estar ejecutoriada y por ello las cosas deben regresar al estado anterior.

En nuestra opinión hay que hacer una diferencia entre cuestiones patrimoniales que se pueden ejecutar, y cuestiones de otra naturaleza que impiden por esas características la ejecución inmediata.

El primer sentido es tradicional y recepta la tendencia que establece que, la ejecución de la sentencia de cámara confirmatoria de la dictada en primera instancia, es factible prestada la fianza prevista en el art. 258 del Código Procesal. De este modo, concedido el recurso extraordinario, procede en aquellos casos donde se discuten cuestiones de exclusivo contenido patrimonial.

Pero si esa característica (económica) no es clara, dentro de la unidad conceptual en que se solicita el cumplimiento de la sentencia, sin que se aporten elementos que permitan discriminar la petición, resulta excluido dicho carácter, toda vez que com-

---

382 Fallos, 314:1675

383 CS, 1993/09/23, La Ley, 1994-B, 253 - DJ, 1994-1-947 - ED, 155-57.

384 Causa O.38.XXXI "*Oswald, María Gabriela s/ su solicitud en autos: 'Wilner, Eduardo Mario c/ Oswald, María Gabriela s/ exhorto'*" del 17 de abril de 1995, ED, 154-55.

prende aspectos como la publicación de la revista y disponibilidad de sus ejemplares cuya ejecución eventualmente tornaría abstracta la decisión adversa de la Corte sobre dicha situación insusceptible de adecuada reparación económica ulterior.[385]

En pocas palabras, aunque sea la cuestión de contenido patrimonial, la complejidad para determinarlo puede actuar en contra de quien requiere una rápida ejecución.

> Por ejemplo, se ha dicho que, al no existir aún una obligación debidamente determinada y consolidada, y por ser exclusivamente facultativa la posibilidad conferida al acreedor de ejecutarla en ese estado, la falta de conformidad de éste con el pago intentado por su deudor, impuso sujetar el esclarecimiento de la razón de uno u otro en esa controversia, a la dilucidación exacta del resultado de la litis. De tal suerte entonces, si en definitiva, el último recurso posible —extraordinario o en queja— daba como consecuencia la revocación de la sentencia de segunda instancia, la consignación intentada por el "solvens" y no aceptada por el "accipiens" debería ser rechazada y produciría efectos negativos a quien improcedentemente la había intentado. Por el contrario, confirmada definitivamente la sentencia como consecuencia de la denegación de los últimos remedios recursivos, la consignación sería válida, y produciría efectos desde su misma concreción, (art. 759, Código Civil).[386]
>
> Cabe agregar que esta lectura no contradice la facultad de la Corte para disponer de oficio, o a pedido de parte, la suspensión de la ejecución de sentencia si entiende que promedian razones de orden institucional.[387]

Otros autores como Morello opinan que, a pesar de esta suerte de guía jurisprudencial, se puede promover la ejecución de fallos que no revistan necesariamente carácter patrimonial.[388] En cambio Sagüés sostiene que, sin descartar esta alternativa, cuando el dinero no sea idóneo para subsanar el daño de una posible ejecución de la sentencia, la resolución objetada por un recurso extraordinario otorgado resultará por el momento inejecutable.[389]

Ahora bien, una vez que el recurso extraordinario se resuelve, la suspensión depende del resultado. Si fue concedido, todo el expediente va a la Corte y queda el proceso suspendido, a tenor del principio que establece el art. 498 del código, es decir, que solo se pueden ejecutar sentencias firmes y ejecutoriadas. Sin embargo,

---

385 CNFedContenciosoadministrativo, Sala I, 1982/11/30, "*Editorial Perfil, S. A. c. Gobierno nacional -PEN, Ministerio del Interior*", ED, 102-831.

386 CNCiv., Sala B, 1987/04/13, "*La Baskonia, S. A. c. Municipalidad de la Capital*", La Ley, 1987-C, 153.

387 Fallos, 245:425; 248:24. También se afirmó que [...] "corresponde decretar la suspensión del incidente de ejecución si los argumentos aducidos en el recurso extraordinario y mantenidos en la queja, podrían, *prima facie*, involucrar cuestiones susceptibles de examen en la instancia del art. 14 de la ley 48, en tanto el *a quo* admitió la ejecución de la sentencia, en los términos del art. 258 del Código Procesal, requiriendo a tal efecto solamente la caución juratoria de la parte apelada, en una causa en la que se encuentra en juego un monto excepcionalmente elevado" (CS, 2004/09/21, "*Caja de Previsión y Seguro Médico de la Provincia de Buenos Aires c/ Poder Ejecutivo Nacional y otros*", Fallos, 327:3801).

388 MORELLO, *Recurso Extraordinario*, 3ª edición, cit., p. 335

389 SAGÜÉS, *Derecho Procesal Constitucional – Recurso Extraordinario,* tomo 2, cit., p. 401.

si se trata de cuestión patrimonial, no se impide la extracción de fotocopias del expediente para requerir la ejecución conforme el art. 258, Código Procesal.

Finalmente, si se tiene que ir en queja por denegación del extraordinario, sólo se puede suspender el proceso si la Corte hace lugar a la queja (art. 285 párrafo final, CPC). Va de suyo que el actor puede pedir (art. 212 inciso 3º, 258, Código Procesal) medidas cautelares y que puede ejecutar la sentencia pese al recurso que se articule. La única limitación será que no podrá ejecutar hasta que se resuelva la admisión del recurso extraordinario.

Para ejecutar la sentencia se debe prestar fianza acorde para responder por lo que importase restituir las cosas a su estado anterior, en caso de prosperar el recurso extraordinario.[390] Como en toda caución, la calidad y cantidad de la misma debe ponderarse por el Juez; pero aquí la particularidad radica en que el trámite de ejecución se debe requerir ante el superior tribunal de la causa, pudiendo o no sustanciarse con el afectado.

Por eso se afirma que, corresponde desestimar la nulidad deducida contra la resolución que en función de lo solicitado por la actora determinó la fianza prevista en el art. 258 del Código Procesal, omitiendo correr traslado de esa petición, pues dicho traslado es una exigencia no prevista por la ley y la resolución inaudita parte es aceptada en doctrina, sin perjuicio del derecho de quien se crea afectado a pedir reposición.[391]

La fianza juratoria a veces se cuestiona, aunque la discrecionalidad judicial se tolera como pauta general. No obstante, otros sostienen que, concedido el recurso extraordinario, debe prestarse caución real por la totalidad de la suma pretendida para proveer a la solicitud de ejecución de sentencia —con sustento en lo dispuesto por el art. 258, Código Procesal—, siendo inadmisible la juratoria —art. 199— por atender a distinta finalidad.[392]

384.25. Si la apelación extraordinaria se deniega (se declara inadmisible) la sentencia recurrida, no obstante, conserva incertidumbre respecto a su definitividad. Es cierto que tomando la pauta del artículo 285 del Código Procesal, "*mientras la Corte no haga lugar a la queja no se suspenderá el curso del proceso*", lo que supone estar atentos a la posible deducción del recurso directo o de hecho.

La dificultad está en que la Corte ha dicho que puede hacer excepción a esta regla "cuando median en la causa razones de orden institucional o de interés público",[393] contingencias que por lo común rodean las premisas que consagra la teoría de la "gravedad institucional".

---

[390] MARTÍNEZ, Hernán J., *El nuevo recurso extraordinario federal,* La Ley 1982-A, 740.

[391] CNFed. Civ. y Com., Sala I, 2004/02/12, "*Atanor S.A. c. Ministerio de Economía*", La Ley, 2004/07/12, p. 7.

[392] Del voto en disidencia parcial del doctor Licht. CNFedContenciosoadministrativo, Sala I, 2001/08/23, "*Silva, Luis A. y otros c. M.D.*", La Ley, 2002-A, 816.

[393] Fallos, 253:445.

Sagüés relata que esta actitud sólo puede concretarse una vez declarada admisible la queja, pues en caso contrario, estaría operando una "interpretación mutativa por adición", lo que equivale a sumar, al supuesto legal de suspensión, otro más, que surgen del derecho judicial.[394] Compartimos esa lectura porqué permite a los jueces no refugiarse en los límites circunspectos de la norma jurídica tornando con mayor y mejor realidad las situaciones cotidianas que el litigio pretende solucionar.

[394] SAGÜÉS, *Derecho Procesal Constitucional - Recurso extraordinario*, tomo 2, cit., p. 54.

Sección 2ª La legislación procesal constitucional en México

385. Antecedentes

385.1. El derecho procesal constitucional en México comenzó en los estados de la Federación después de la reforma de 1994. No referimos a la autonomía que adquiere el juicio de amparo, tampoco al juicio político, ni al poder de investigación de la Corte Suprema, sino a la expansión del control de constitucionalidad hacia las Cartas máximas locales que generan en los Tribunales superiores un deber de fiscalización que antes quedaba solamente radicado en la Constitución Política de México.

La modificación va de la mano con la reforma que convierte a la Corte Suprema de Justicia de la Nación en un tribunal jurisdiccional integrado y ordenado en competencias que puede espejarse con los Tribunales Constitucionales europeos.

En síntesis, la función consiste en privilegiar la supremacía de la constitución federal, pero otorgando a la Corte local un poder muy amplio de preservación por las normas propias, pensando en proteger las normas o leyes de rango constitucional, y toda la construcción infraconstitucional del Estado, contra leyes del mismo rango o actos de autoridades estatales que contrarían las disposiciones constitucionales reguladoras del régimen interno de las entidades federativas.

385.2. En América Latina no son muchos los países de estructura federal, y aun están quienes así organizados, en materia jurisdiccional trabajan con unificación legislativa y sin división territorial en sus códigos.

Por ello, los ejemplos de Argentina y México para evidenciar el rol del derecho procesal constitucional local son muy importantes.

> En América la jurisdicción constitucional local se desarrolla en países como Argentina, Venezuela y México, en este último, pese a que desde 1824 las entidades federativas previeron, en sus respectivas constituciones instrumentos para su protección, no fueron eficaces en virtud de la concentración del control constitucional a través del juicio federal de amparo. Sin embargo a partir del año 2000 se ha tendido a desarrollar ese aspecto, por ejemplo los tribunales superiores de justicia de los estados de México, Veracruz, Tlaxcala, Chihuahua y Coahuila cuentan con salas de lo constitucional que conocen de procesos y procedimientos como acciones de inconstitucionalidad y controversias constitucionales. Quizás este inicio haya tomado como punto de partida las figuras implementadas a nivel federal pero lo cierto es que son el punto de partida para un desarrollo de la protección de sus constituciones por sus propios poderes judiciales. Aunque hasta el momento haya sido incipiente la actividad en las entidades federativas en este rubro,

> debe reconocerse que es el comienzo de una dinámica persistente y tenaz por consolidar medios de control constitucional local.[395]

En México, existen procesos constitucionales que se desenvuelven en armonía, e instituciones que garantizan a operatividad, a saber: *a)* el juicio político; *b)* el procedimiento de investigación de la Suprema Corte de Justicia; *c)* las controversias constitucionales; *d)* el juicio de amparo; *e)* la acción abstracta de inconstitucionalidad; *f)* el juicio de protección de los derechos político electorales; *g)* el juicio de revisión constitucional electoral.

385.3. Veracruz, Coahuila, Tlaxcala, Chiapas y Quintana Roo, comenzaron el movimiento dando un lugar preferente al principio de supremacía de la Constitución, preocupados por resguardar la Constitución Política de México, pero, al mismo tiempo, asignando un rol destacado al deber jurisdiccional de aplicar en primer término las disposiciones de las Cartas máximas particulares.

Pero no fueron solo ellas, porque otros Estados se suman con reformas en su "justicia constitucional", dando cuenta total de veinte (20) reformas en treinta y dos (32) Estados federativos (son Campeche, Chiapas, Chihuahua, Coahuila, Colima, Durango, Estado de México, Guanajuato, Guerrero, Hidalgo, Morelos, Nuevo León, Oaxaca, Querétaro, Quintana Roo, Sinaloa, Tabasco, Tlaxcala, Veracruz y Zacatecas). En ellas se han implementado variados medios de control judicial de la constitucionalidad local, entre los que destacan el juicio de protección de derechos fundamentales (llamado frecuentemente "amparo local"), la controversia constitucional, la acción de inconstitucionalidad, la cuestión de inconstitucionalidad y la acción por omisión legislativa.[396]

> Ahora bien, el aparente fortalecimiento al federalismo que se ha efectuado paulatinamente a través del establecimiento de sistemas judiciales de control constitucional local mediante sus respectivos instrumentos procesales, ha traído aparejado una serie de cuestiones de diversa índole. Por ejemplo, se ha manifestado que no existe la adecuada coordinación entre los mecanismos de control de constitucionalidad local y los de índole federal; que las resoluciones constitucionales locales carecen de definitividad real debido a la procedencia, en casos excepcionales, del amparo directo federal; que son cuestionables la aptitud y preparación de los jueces del fuero común sobre el conocimiento y resolución de asuntos de naturaleza constitucional.[397]

386. El Estado de Veracruz

386.1. El control de constitucionalidad el Estado de Veracruz, se realiza sobre la Constitución y leyes federales, los tratados internacionales y su propia Constitución, siendo ésta la ley suprema (art. 80, Constitución local).

---

[395] ALDASORO, Héctor, *El derecho procesal constitucional mexicano,* conferencia en el Ilustre Colegio Nacional de México, passim

[396] BUSTILLOS, Julio, "La realidad de la justicia constitucional local mexicana en el siglo XXI", *Revista Cuestiones Constitucionales*, n° 21 (2009), pp. 67 y ss.

[397] BUSTILLOS, ob. cit., p. 68.

Explica César Astudillo Reyes que:

[…] El principio de autonomía debe ubicarse en el contexto de una particular forma de Estado. Dentro de un Estado de naturaleza federal su reconocimiento se traduce en la coexistencia una pluralidad de sistemas jurídicos autosuficientes, y en la estratificación de niveles de gobierno y órganos de decisión. La convivencia de más de un sistema normativo no implica, por otro lado, dejar de vincularse a un nivel de gobierno y a un ordenamiento superior que es precisamente el que los *delimita* y que se sobrepone en calidad de coadyuvante y garante de la unidad del Estado.

La capacidad de *autoorganización* de los entes federados se ubica como la primera consecuencia de la consagración del principio de autonomía local. La amplitud o estrechez de esa autoorganización depende, en buena medida, de la extensión con que se consideren las diferentes *vertientes* en las que se manifiesta la autonomía. Además de implicar el permiso para la expedición de una Constitución propia, el reconocimiento del principio de autonomía representa el ejercicio de una decisión real de individuación de los fines últimos de la entidad federada, de estructuración de los poderes estatales y de asignación del cumplimiento concreto de esos fines a cada uno de esos poderes […]

La guía de los poderes locales, establecida desde la Constitución local dentro del marco de posibilidades que la Constitución general permite, puede dirigirse mediante fines que no coinciden plenamente con los de ésta; reconocerlo implica, sin embargo, sostener una tesis que conduce, probablemente, a la consideración más amplia que sobre el concepto de autonomía pueda difundirse, en tanto se deduce que el *espacio de poder periférico* está habilitado para marcar una dirección política de cuño diferente a la que desde el *espacio de poder central* pretende imponerse, organizando consecuentemente los poderes locales en modo de alcanzar los fines y propósitos delineados por la Constitución local.

México se articula constitucionalmente como un Estado federal, según se estipula expresamente en el artículo 40 de la Constitución de 1917. En la misma norma se reconoce el principio de autonomía local o estatal al señalar que la república se compone de *estados libres y soberanos en todo lo que concierne a su régimen interior*. En el ordenamiento constitucional mexicano, el principio de autonomía local recoge las vertientes ya señaladas, comprendiéndolas dentro de una, aquella que se manifiesta de modo más relevante: la capacidad para establecer su propia Constitución y desprender de ella un ordenamiento jurídico autónomo. Por ello, el artículo 41 establece que el ejercicio de la soberanía se realiza a través de los poderes de la unión, "y por los de los Estados, en lo que toca a su regímenes interiores, en los términos respectivamente establecidos por la presente Constitución federal y las particulares de los estados".

A pesar de ello, la autonomía reconocida a los entes federados en México no tiene los alcances que permite el ensanchamiento de su contenido. Las limitaciones establecidas en la ley fundamental tienen asignada una función consistente en garantizar niveles mínimos de homogeneidad en el entramado institucional delineado por las Constituciones locales con el objeto de que entre ellas y aquella no exista una diferencia sustancial en lo relativo al modelo de organización política, hecho que sería desfavorable a la idea de "unión" o "unidad" que subyace a la idea federal.

Atendiendo a esta idea, las Constituciones locales están constreñidas a observar una serie de principios constitucionales comunes referidos a la forma republicana de gobierno, el gobierno representativo y democrático, y la autonomía municipal, según lo estipula el artículo 115 de la Constitución. El artículo 116 completa el minucioso conjunto de limi-

taciones al señalar que las entidades deben acoger el principio de división de poderes; consecuente con esa determinación, la misma norma impone las reglas básicas que deben adoptar para la elección e integración de la tradicional tríada de poderes, estableciendo además los principios y garantías a que debe sujetarse la organización electoral. Normas relativas al establecimiento de tribunales contencioso-administrativos, a las relaciones laborales entre el Estado y sus trabajadores o a los convenios de prestación de servicios públicos entre la Federación y el Estado encuentran cobijo en la misma disposición fundamental.[398]

386.2. En el año 2009 se reforma el capítulo de la organización judicial, que trae una fuerte implicancia para el funcionamiento de las garantías locales.

El art. 55 de la Constitución, que queda redactado del siguiente modo: "El Poder Judicial se deposita en un Tribunal Superior de Justicia, en un Tribunal Electoral, en un Tribunal de lo Contencioso Administrativo, en un Tribunal de Conciliación y Arbitraje y en los juzgados que señale la Ley Orgánica de la materia.

El artículo 56 establece en el Poder Judicial del Estado las atribuciones (obsérvese que no instala al precepto como un deber de la función, sino como una potestad) de garantizar la supremacía y control de esta Constitución mediante su interpretación y anular las leyes o decretos contrarios a ella; proteger y salvaguardar los derechos humanos que el pueblo de Veracruz se reserve, mediante el juicio de protección correspondiente; interpretar y aplicar las leyes del fuero común y las federales en jurisdicción concurrente; dictar las medidas procedentes para que la administración de justicia sea pronta, expedita y completa; entre otras.

386.3. Para el cumplimiento de las atribuciones señaladas el Tribunal Superior de Justicia contará con una Sala Constitucional, integrada por tres magistrados, que tendrá competencia para:

I. Conocer y resolver, en los términos de la ley respectiva, del juicio de protección de derechos humanos, por actos o normas de carácter general que conculquen derechos humanos que el pueblo de Veracruz se reserve, provenientes de:

a) El Congreso del Estado;

b) El Gobernador del Estado; y

c) Los titulares de las dependencias o entidades de la administración pública estatal, municipal y de los organismos autónomos de Estado.

II. Conocer y resolver, en instancia única, de las resoluciones del ministerio público sobre la reserva de la averiguación previa, el no ejercicio de la acción penal y las resoluciones de sobreseimiento que dicten los jueces con motivo de las peticiones de desistimiento que formule el ministerio público;

III. Sustanciar los procedimientos en materia de controversias constitucionales, acciones de inconstitucionalidad y las acciones por omisión legislativa, y formular los proyectos de resolución definitiva que se sometan al pleno del Tribunal Superior de Justicia;

---

[398] ASTUDILLO REYES, César I., "La Justicia Constitucional en México. Presupuestos, sistemas y problemas", *Boletín Mexicano de Derecho Comparado*, n° 115 (2006), pp. 23 y ss.

> IV. Dar respuesta fundada y motivada a las peticiones formuladas por los demás tribunales y jueces del Estado, cuando tengan duda sobre la constitucionalidad o aplicación de una ley local, en el proceso sobre el cual tengan conocimiento. Las peticiones tendrán efectos suspensivos y deberán ser desahogadas en un plazo no mayor de treinta días naturales, en los términos que disponga la ley.

Como se puede apreciar, la Sala Constitucional reduce su competencia de control ya que tratándose de controversias constitucionales, las acciones de inconstitucionalidad y las de omisión legislativa quedan fuera de su reducto y alcance.

> La competencia de la Sala Constitucional actuando estrictamente como órgano especializado y terminal de naturaleza constitucional, se reduce a las hipótesis del juicio para la protección de derechos humanos (amparo local) y a la consulta que realicen los demás jueces sobre la constitucionalidad de una norma local en un proceso concreto. En resumen, el control de constitucionalidad local queda dividida entre el Pleno del Tribunal y la Sala Constitucional dependiendo del tipo de proceso constitucional de que se trate. Esta bifurcación de competencias no resulta lógica si se ha creado una sala especializada para la interpretación y aplicación de la Constitución veracruzana, por lo que en el futuro sería deseable ampliar sus atribuciones para configurarse como una auténtica jurisdicción constitucional, o bien, desaparecerla, dejando tal atribución al Pleno del tribunal.[399]

386.4. El sistema que adopta Veracruz continúa la tendencia común en México de no permitir el control difuso de la constitucionalidad de las leyes, prefiriendo confiar en el Tribunal Superior para esos fines.

La modalidad, como dice Astudillo Reyes:

> […] se inserta dentro de aquellos sistemas que forman parte del *tertium genus* configurado por el "modelo de control incidental de constitucionalidad", cuyo elemento caracterizante viene otorgado por la adopción del instrumento que sirve de puente o enlace entre la jurisdicción ordinaria y la constitucional: hablamos de la cuestión de inconstitucionalidad.[400]

El control se concentra en la Sala en Pleno o en la Sala Constitucional, una para el control abstracto y la otra para las cuestiones concretas o conflictos entre partes, respectivamente. La sala constitucional participa, sin embargo, en la totalidad de ellos, ya que sustancia y formula los proyectos de resolución definitiva que se someten al pleno, conociendo y resolviendo en forma definitiva los demás.[401]

> En el ordenamiento veracruzano se contempla un sistema global de defensa constitucional que incorpora ocho institutos protectores. Entre los mecanismos estrictamente procesales de control se encuentran: 1) El juicio de protección de los derechos humanos; 2) El recurso de regularidad constitucional de los actos del ministerio público; 3) Las controversias

---

[399] FERRER MAC GREGOR, Eduardo, *La nueva sala constitucional en el Estado de Veracruz,* en "Justicia Constitucional Local", AAVV (FERRER MAC GREGOR, Eduardo, VEGA HERNÁNDEZ, Rodolfo, coords.), Fundap, Querétaro, 2003, p. 202.

[400] ASTUDILLO REYES, César I., ob. cit., p. 26.

[401] ASTUDILLO REYES, César I., ob. cit., p. 27.

constitucionales; 4) Las acciones de inconstitucionalidad; 5) Las acciones por omisión legislativa y, finalmente; 6) Las cuestiones de inconstitucionalidad. Todos ellos se encuentran regulados en el artículo 64 de la CV. Encontrándose en el sistema veracruzano instrumentos procesales de control que proceden contra la ley en sí misma, al margen de su aplicación, y también con motivo de ella (el denominado control concreto y abstracto), su ámbito de protección se reconduce a intereses objetivos y subjetivos y, por tanto, en su promoción participan órganos del Estado y particulares lesionados en sus derechos fundamentales.

Respecto de los instrumentos que protegen intereses subjetivos, la legitimación corresponde a quien o quienes reciban un agravio personal y directo, consecuencia de un acto de autoridad violatorio de sus derechos fundamentales. Así lo dispone el artículo 64, fracción I de la CV, y 6 de la Ley del Juicio de Protección de Derechos Humanos del Estado de Veracruz-Llave, reglamentaria de aquél. Lo mismo sucede con el recurso encaminado a la tutela de los derechos fundamentales de los veracruzanos ante una eventual actuación irregular del ministerio público local, recogido en el artículo 64, fracción II de la CV.

En lo relativo a los instrumentos de tutela objetiva del ordenamiento, los entes legitimados tienen el carácter de autoridades u órganos constitucionales del Estado. Según los artículos 64 y 65 de la CV, las controversias constitucionales pueden ser interpuestas por los municipios, los poderes Ejecutivo y Legislativo. En las acciones de inconstitucionalidad se dota de cualificación procesal al gobernador del Estado y a cuando menos la tercera parte de los miembros del congreso. Las acciones por omisión legislativa pueden ser activadas por el gobernador del Estado o por la tercera parte de los ayuntamientos. Finalmente, las cuestiones de inconstitucionalidad pueden ser elevadas por todos los jueces y magistrados del Estado.[402]

387. El Estado de Coahuila

387.1. El art. 158 de la Constitución local establece que la justicia constitucional se erige dentro del régimen interior del Estado, como un medio de control para mantener la eficacia y la actualización democrática de la Constitución, bajo el principio de supremacía constitucional, sin perjuicio de los instrumentos de carácter federal.

La función la desempeña el Tribunal Superior de Justicia del Estado para las cuestiones de inconstitucionalidad, pero los jueces locales pueden declarar la inaplicación de la ley en el caso concreto. De este modo se aproxima más al mecanismo federal que al de Veracruz.

387.2. La Justicia Constitucional Local tiene por objeto dirimir de manera definitiva e inatacable los conflictos constitucionales que surjan dentro del ámbito interior del Estado, conforme a este artículo, sin perjuicio de lo previsto en los artículos 41, 99, 103, 105 y 107 de la Constitución Política de los Estados Unidos Mexicanos.

Cuando la autoridad jurisdiccional considere en su resolución que una norma, es contraria a esta Constitución, con base en lo establecido por el artículo 133 de la Constitución Política de los Estados Unidos Mexicanos, deberá declarar de oficio su

[402] ASTUDILLO REYES, César I., ob. cit., pp. 29 y ss.

inaplicabilidad para el caso concreto. En este supuesto, el Tribunal Superior de Justicia podrá revisar la resolución en los términos que disponga la ley.

El Tribunal Superior de Justicia en su carácter de Tribunal Constitucional Local conocerá, en los términos que establezca la ley, de los medios de control siguientes:

I. De las controversias constitucionales locales, que con excepción de las que se refieran a la materia jurisdiccional electoral en los términos del artículo 136 de esta Constitución, se susciten entre:

1. El Poder Ejecutivo y el Legislativo;
2. El Poder Ejecutivo y uno o más Municipios del Estado;
3. El Poder Legislativo y uno o más Municipios del Estado;
4. El Poder Legislativo y una o más entidades paraestatales o paramunicipales del Estado;
5. Un Municipio y otro u otros del Estado;
6. Uno o más Municipios y una o más entidades paraestatales o paramunicipales del Estado;
7. Una o más entidades paraestatales y otra u otras paramunicipales del Estado.
8. Uno o más organismos autónomos y otro u otros órganos del gobierno estatal y/o municipal..

En el caso del inciso 1, la controversia sólo procederá en materia de régimen interno del Estado, sin perjuicio de lo previsto en el artículo 105 de la Constitución Política de los Estados Unidos Mexicanos.

En los casos de los incisos 2., 3. y 5., la controversia sólo procederá en los supuestos previstos en el artículo 115, fracción II, último párrafo, de la Constitución Política de los Estados Unidos Mexicanos.

387.3. Las controversias constitucionales locales se sujetarán a las siguientes bases:

1. Podrán promoverse por cualquiera de las partes, según la controversia de que se trate;
2. La controversia tendrá por objeto resolver sobre si el acto o los actos reclamados son conformes o contrarios a esta Constitución con base en el principio de supremacía constitucional establecido en el artículo 133 de la Constitución Política de los Estados Unidos Mexicanos, y por vía de consecuencia declarar su validez o invalidez.
3. Las resoluciones que pronuncie el Tribunal Superior de Justicia, tendrán efectos de cosa juzgada únicamente respecto de las partes que intervinieron en la controversia. Sólo en los casos en que se forme jurisprudencia local tendrá efectos generales.
4. La ley establecerá el procedimiento a que deberán sujetarse las partes para dirimir la controversia.

387.4. También entiende de las acciones de inconstitucionalidad local que tengan por objeto plantear la posible contradicción entre una norma o acuerdo de ca-

rácter general y esta Constitución, las que deberán resolverse con base en lo establecido en el artículo 133 de la Constitución Política de los Estados Unidos Mexicanos.

El ejercicio de las acciones de inconstitucionalidad se sujetará a las bases siguientes:

1. Sólo podrá promoverse por: *a)* El equivalente al treinta por ciento de los integrantes de los Ayuntamientos o Concejos Municipales en contra de los bandos de policía y de gobierno, los reglamentos, circulares y disposiciones administrativas de observancia general, aprobadas por los propios Ayuntamientos o Concejos Municipales; *b)* el Ejecutivo del Estado por sí o por conducto de quien le represente legalmente, o el equivalente al treinta por ciento de los integrantes del Poder Legislativo, en contra de los bandos de policía y de gobierno, reglamentos, circulares y disposiciones administrativas de observancia general que dicten los Ayuntamientos o Concejos Municipales; *c)* el Ejecutivo del Estado por sí o por conducto de quien le represente legalmente, o por el equivalente al treinta por ciento de los integrantes de los Ayuntamientos o Concejos Municipales en contra de las leyes, decretos o acuerdos que apruebe el Congreso del Estado; d) el organismo público autónomo, por conducto de quien le represente legalmente, en contra de las leyes, decretos o acuerdos que apruebe el Congreso del Estado con relación a la materia de su competencia.

Se ejercitarán dentro de los treinta (30) días naturales siguientes a la fecha de publicación de la norma o acuerdo general o de que se tenga conocimiento de las mismas.

Las resoluciones del Tribunal Superior de Justicia sólo podrán declarar la invalidez de las normas impugnadas, siempre que fueren aprobadas por la mayoría absoluta de sus miembros y tendrán efectos de cosa juzgada.

La ley reglamentaria establecerá el procedimiento para resolver la acción de inconstitucionalidad local.

La única vía para plantear la inconstitucionalidad de leyes, decretos o acuerdos legislativos en materia electoral, es la prevista en este artículo, sin perjuicio del control difuso que ejercerá el Tribunal Electoral del Poder Judicial en los términos de esta Constitución.

Cabe agregar que la Justicia Constitucional se regirá en todos los casos por la jurisprudencia local.

> Para el nombramiento de los jueces constitucionales no se requiere de un perfil especial; más bien se pone el acento en el perfil judicial de los aspirantes (artículo 138 y 145 de la CCo, 80 de la LOPJCo). Dentro de los mecanismos de nombramiento se incorpora la participación del Consejo de la Judicatura, órgano al que le corresponde elaborar la lista de candidatos a magistrados que se presenta al gobernador con el fin de que proceda al nombramiento, previa aprobación que haga el congreso en un lapso no mayor a cinco días (artículo 146 de la CCo, 81 de la LOPJCo). El periodo constitucional de los magistrados es de seis años (artículo 135 CCo). En la vertiente difusa, por autoridades jurisdiccio-

nales para efectos de desaplicación concreta de normas debe entenderse el conjunto de tribunales unitarios de distrito, juzgados de primera instancia y juzgados letrados en que se estratifica el ejercicio del Poder Judicial (artículo 135 de la CCo, 2 de la LOPJCo). El nombramiento de los juzgadores corresponde al Consejo de la Judicatura con base en los requisitos y procedimiento señalados para la carrera judicial (artículo 147 de la CCo, 62, 83, 84 y 85 de la LOPJCo). Los magistrados y jueces recibirán una remuneración adecuada e irrenunciable, la cual no podrá ser disminuida durante su encargo (artículo 153 de la CCo). En materia de responsabilidades, se encuentran sujetos a juicio político, a juicio de responsabilidad y a responsabilidad penal, para lo cual deberá ejercitarse la respectiva declaración de procedencia (artículos 163 a 167 de la CCo).[403]

387.5. La confusa pero armónica relación entre el control difuso y el concentrado, impacta en los procesos constitucionales en materia de legitimación, porque los requerimientos difieren según la cuestión de constitucionalidad sea abstracta o derive en casos de concreta resolución.

Dentro de las acciones de inconstitucionalidad tienen legitimación el equivalente al 30 por ciento de los integrantes de los ayuntamientos o concejos municipales, el Ejecutivo del Estado y el equivalente al 30 por ciento de los integrantes del Poder Legislativo (artículo 158, fracción II de la CCo). En las controversias, el Poder Ejecutivo y Legislativo, y los municipios del Estado (artículo 158, fracción I de la CCo). En el recurso de revisión, la legitimación para interponerlo corresponde a las partes del litigio desarrollado ante el tribunal *a-quo,* ámbito judicial donde se suscita el incidente de inconstitucionalidad de una norma.[404]

388. El Estado de Tlaxcala

388.1. En este Estado de México se instala en la Corte Superior la función de tribunal constitucional cuando las denuncias de inconstitucionalidad provenga de particulares contra la autoridad que haya vulnerado un derecho fundamental. Esta actuación en una suerte de amparo contra la inconstitucionalidad de las leyes no agota la dimensión constitucional que adquiere el Superior pues avanza también con poderes propios en los conflictos de competencia entre órganos o entidades.

388.2. La exclusividad para el control de constitucionalidad aísla a los jueces comunes deja al sistema del Estado con algún desconcierto respecto del modelo federal, si bien es cierto que la Corte Suprema de la Nación conserva igual identidad y perfil institucional.

La integración numerosa del cuerpo estatal (catorce [14] magistrados más tres [3] supernumerarios), no obstante, no es propiamente un modelo jurisdiccional plenamente concentrado como fue el esquema pensado por Hans Kelsen, pues las competencias que tiene le obliga a dividirse en salas que se distribuyen procesos administrativos y contenciosos.

---

[403] ASTUDILLO REYES, César I., ob. cit., pp. 33 y ss.

[404] ASTUDILLO REYES, César I., ob. cit., p. 34.

388.3. En la Constitución local el art. 81 dispone que:

El pleno del Tribunal Superior de Justicia, actuando como Tribunal de Control Constitucional del Estado, conocerá de los asuntos siguientes:

I. De los medios de defensa que hagan valer los particulares contra leyes o actos de autoridades que vulneren los derechos fundamentales consagrados en esta Constitución;

II. De los juicios de competencia constitucional, por actos o normas jurídicas de carácter general que violen esta Constitución y las leyes que de ella emanen, y que se susciten entre:

a) Los poderes Legislativo y Ejecutivo del Estado;

b) El Poder Legislativo y un Ayuntamiento o Concejo Municipal;

c) El Poder Ejecutivo y un Ayuntamiento o Concejo Municipal;

d) Dos o más ayuntamientos o concejos municipales, de municipios diferentes, siempre que no se trate de cuestiones relativas a sus límites territoriales; en tal caso, la decisión corresponderá al Congreso; y,

e) Dos o más munícipes de un mismo Ayuntamiento o Concejo Municipal, incluidos los presidentes de comunidad.

III. De las acciones de inconstitucionalidad que se promuevan contra normas jurídicas de carácter general, provenientes del Congreso del Estado y en las que se plantee violación abstracta a esta Constitución. El ejercicio de estas acciones corresponderá:

a) Al equivalente al veinticinco por ciento de los diputados que integran el Poder Legislativo del Estado;

b) A la Comisión Estatal de Derechos Humanos;

c) A la Universidad Autónoma de Tlaxcala;

d) Al Procurador General de Justicia del Estado en los asuntos relativos a su función; y,

e) A los partidos políticos debidamente registrados ante el Instituto Electoral del Estado, en asuntos de la materia electoral.

IV. De las acciones de inconstitucionalidad que se promuevan contra normas jurídicas de carácter general, provenientes de algún Ayuntamiento o Concejo Municipal y en las que se plantee violación abstracta a esta Constitución. El ejercicio de estas acciones corresponderá:

a) Al equivalente al veinticinco por ciento de los munícipes del mismo Ayuntamiento o Concejo Municipal, incluidos los presidentes de comunidad;

b) Al o los diputados, en cuyo distrito electoral se comprenda el Ayuntamiento o Concejo Municipal que haya expedido la norma impugnada;

c) Al Gobernador del Estado;

d) A la Comisión Estatal de Derechos Humanos;

e) A las Universidades Públicas estatales; y,

f) Al Procurador General de Justicia del Estado en los asuntos relativos a sus funciones.

V. El trámite y resolución de los juicios de competencia constitucional y acciones de inconstitucionalidad a que se refieren las tres fracciones anteriores, se sujetará a los términos siguientes:

a) El término para promover el juicio de competencia constitucional será de treinta días naturales, contados a partir de aquél en que la parte actora haya tenido conocimiento del acto o norma jurídica que pretenda impugnar;

b) El término para ejercitar las acciones de inconstitucionalidad será de noventa días naturales, contados a partir de aquél en que la norma jurídica que se desea impugnar, haya sido publicada en el *Periódico Oficial del Gobierno del Estado*;

c) La promoción para el juicio de competencia constitucional suspenderá la ejecución de los actos materiales que se impugnen, salvo que con ello se cause mayor perjuicio al interés público, a criterio del órgano de control constitucional.

Cuando se trate de impugnaciones a normas jurídicas, mediante juicios de competencia constitucional o acciones de inconstitucionalidad, no procederá la suspensión de la aplicación de la norma;

d) Las resoluciones que declaren procedentes los juicios de competencia constitucional, cuando versen sobre normas jurídicas y las acciones de inconstitucionalidad, deberán ser aprobadas, cuando menos por diez magistrados, si el fines declarar inválida la norma y con efectos generales; en caso contrario se desestimará la impugnación;

e) El quórum en las sesiones del Tribunal cuando deban votarse resoluciones que versen sobre normas jurídicas, se formará cuando menos con doce magistrados. De no obtenerse ese quórum, se suspenderá la sesión y se convocará para el día hábil siguiente; y si tampoco así se pudiese sesionar, se llamará a los suplentes que corresponda, hasta obtener dicho quórum, informando de ello al Congreso, para que, de no tener justificación, suspenda de sus funciones a los ausentes;

f) Los acuerdos de trámite que dicte el Presidente del Tribunal y el Magistrado ponente, podrán ser recurridos ante el pleno del Tribunal. Las resoluciones dictadas por el pleno del Tribunal, cualquiera que sea su sentido, son irrecurribles;

g) Todas las resoluciones definitivas del Tribunal, deberán publicarse en el Boletín del Poder Judicial y en el Periódico Oficial del Gobierno del Estado; un extracto de las mismas, se publicará en los periódicos de mayor circulación en el Estado;

h) Las resoluciones del pleno deberán ser obedecidas; de no hacerlo, la autoridad omisa será destituida por el mismo pleno; e,

i) La ley reglamentaria de este artículo determinará las demás características del funcionamiento y atribuciones del Tribunal de Control Constitucional.

VI. De las acciones contra la omisión legislativa imputables al Congreso, Gobernador y ayuntamientos o concejos municipales, por la falta de expedición de las normas jurídicas de carácter general, a que estén obligados en términos de las Constituciones Políticas, de los Estados Unidos Mexicanos, del Estado y de las leyes.

El ejercicio de esta acción corresponderá a las autoridades estatales y municipales, así como a las personas residentes en el Estado.

Al admitirse la demanda, se ordenará correr traslado a la responsable y al Director del *Periódico Oficial del Gobierno del Estado*, para que rindan sus informes. Se celebrará una audiencia de pruebas y alegatos e inmediatamente después se dictará la resolución correspondiente. De verificarse la omisión legislativa, se concederá a la responsable un término que no exceda de tres meses para expedir la norma jurídica solicitada. El incumplimiento a esta sentencia, será motivo de responsabilidad.

En lo conducente, serán aplicables a esta acción lo establecido en los incisos *d)*, *e)*, *f)*, *g)* e *i)*, de la fracción anterior.

388.4. El 30 de noviembre de 2001 (última reforma data del 5 de diciembre de 2008) se reglamenta el art. 81 constitucional con la "Ley del Control Constitucional del Estado de Tlaxcala". Con ella se regulan los procesos de: *a)* Juicio de protección

constitucional; *b)* juicio de competencia constitucional; *c)* acción de inconstitucionalidad, y *d)* acción contra la omisión legislativa.

En todos los casos, el Pleno del Tribunal Superior de Justicia del Estado actúa como Tribunal de Control Constitucional competente para conocer y resolver en dichas actuaciones.

En cada proceso, tienen carácter de actores: *a)* Las autoridades; *b)* los partidos políticos; *c)* el Procurador General de Justicia en cuanto al interés público que le deriva legalmente, y *d)* los particulares, a quienes la Constitución del Estado les reconozca tal carácter.

Cada uno deberá señalar como demandadas a las autoridades que emitan y promulguen la norma que se impugne, y, en su caso, a las que hubieren ordenado, ejecutado o traten de ejecutar el acto o resolución combatidos. Si se reclama una omisión, material o legislativa, se demandarán a las autoridades que, conforme a la ley, deban realizar directa e indirectamente dicho acto.

También deberán ser llamados como terceros interesados las autoridades y particulares que sin ser partes, pudieran resultar afectados por la sentencia que llegue a dictarse. Si los actores no cumplieren con ese señalamiento, el Presidente del Tribunal o el Magistrado instructor, de oficio deberán llamarlos al proceso (art. 20).

388.5. Las sentencias además de ajustarse a la formalidad y procedimientos que determina el Código de Procedimientos Civiles del Estado, cumplirán con los requisitos siguientes:

> I. Previamente se decidirán los incidentes y recursos que estén pendientes de resolución, y si no existiere obstáculo legal, se pasará al análisis del fondo del asunto planteado;
>
> II. Analizarán en su conjunto los planteamientos de las partes y suplirán, en todo caso, las deficiencias que se observaren en la demanda, reconvención, ampliación o en su contestación;
>
> III. Precisarán los alcances y efectos de la sentencia; así como las autoridades que deban cumplirlas, aunque no hayan sido llamadas al proceso, si de manera indirecta se requiere de su participación;
>
> IV. Si se declara la inconstitucionalidad de una norma, los efectos de esta declaratoria se harán extensivos a las demás normas que dependan de la invalidada, aunque aquéllas no se hayan impugnado;
>
> V. Fijarán el término o plazo para su debido cumplimiento, tomando en cuenta la facilidad o dificultad inherentes, el que no deberá ser mayor de setenta días, que se reducirá a cinco días si se trata de actos privativos de la libertad, y
>
> VI. En ningún caso condenarán al pago de gastos y costas.

388.6. Las sentencias que versen sobre actos materiales u omisiones, se aprobarán por simple mayoría de votos de los Magistrados. En caso de empate, quien presida la sesión correspondiente del Tribunal, tendrá voto de calidad.

Para que pueda declararse la inconstitucionalidad de una norma o la procedencia de una acción por omisión legislativa, se requerirá que la sentencia respectiva sea

aprobada cuando menos por diez (10) Magistrados; en caso contrario se desestimará la impugnación.

La sentencia que invalide una norma tendrá efectos generales, mas no retroactivos, con excepción de la materia penal.

388.7. En orden a objeto y pretensiones que recrean los procesos constitucionales cabe agregar que, el *juicio de protección constitucional* persigue nulificar las normas y actos de las autoridades que violen las disposiciones contenidas en la Constitución del Estado y en la demás legislación que de ella emane, en perjuicio de los particulares. La promoción de este medio de control será siempre optativa para el interesado.

Este juicio procede contra normas jurídicas de carácter general que emanen de los Poderes Legislativo y Ejecutivo del Estado, de los Ayuntamientos o Concejos Municipales, de la Universidad Autónoma de Tlaxcala, de los demás organismos públicos autónomos o descentralizados; y en general de cualquier autoridad estatal o municipal, sin importar la materia, y contra actos materiales u omisiones, de cualquiera de las autoridades y organismos mencionados en la Fracción anterior, siempre y cuando no exista algún otro medio de defensa legal mediante el cual el Tribunal Superior de Justicia del Estado o sus Salas, puedan revocar o modificar esos actos.

El juicio de *Competencia Constitucional* procede en los casos a que se refiere la Fracción II del Artículo 81 de la Constitución del Estado.

Las *acciones de inconstitucionalidad p*odrán ejercitarse en los supuestos previstos en el Artículo 81, Fracciones III y IV de la Constitución del Estado.

Las *acciones contra la omisión legislativa* solo proceden cuando una persona demuestre que tiene su residencia permanente en el territorio del Estado, conforme a las Leyes aplicables. Las personas morales, acreditarán que su domicilio social o el de alguna de sus sucursales, se encuentra establecido en el territorio del Estado, cuando menos con una antigüedad de un año, a la fecha de presentación de la demanda. En todos los casos, se pedirá al Director del *Periódico Oficial del Gobierno del Estado* que remita, dentro de cinco días, un informe en el que especifique si ha sido publicada la norma cuya omisión se plantea; y en caso afirmativo deberá anexar los ejemplares correspondientes en los que conste dicha norma y sus modificaciones.

Si la demandada manifestare que su omisión obedece, a su vez, a la omisión legislativa de otra autoridad, se llamará al proceso, como demandada, a esa autoridad; y en la sentencia definitiva que se dicte, se resolverá sobre ambas omisiones.

389. El Estado de Chiapas

389.1. El 6 de noviembre de 2002 se publicó en el *Periódico Oficial del Estado* la reforma constitucional que continúa la línea de transformación del control constitucional en los Estados de la Federación.

Se crearon tres mecanismos propios para: *a)* las controversias constitucionales; *b)* las acciones de inconstitucionalidad y *c)* las acciones por omisión legislativa.

Se agregó un procedimiento de consulta sobre cuestiones del orden constitucional y se radicó el eje de las actuaciones en el Tribunal Superior del Estado.

La Constitución Chiapaneca no contempla una parte dogmática específica en su estructura. Únicamente reitera las garantías de la carta magna federal. No reconoce más derechos, pero también por implicancia protege a la población indígena debido a la composición poblacional de la entidad. El artículo 4 dice: "Toda persona gozará de las garantías individuales y sociales que otorga la Constitución Política de los Estados Unidos Mexicanos y que la presente Constitución reitera; garantías que no podrán restringirse o suspenderse, sino en los casos y con las condiciones que la primera de dichas Constituciones establece".

389.2. El artículo 49 de la Constitución Política del Estado Libre y Soberano de Chiapas, al respecto, establece que:

> Se deposita el ejercicio del Poder Judicial del Estado en un Supremo Tribunal de Justicia; en un Tribunal Electoral, en un Tribunal del Servicio Civil; juzgados de primera instancia; juzgados de paz y conciliación; juzgados de paz y conciliación indígena y juzgados municipales [...]. La administración, vigilancia y disciplina del Poder Judicial del Estado, con excepción de la Sala Superior [nuevo órgano jurisdiccional]; estará a cargo del Consejo de la Judicatura; [creado en esta reforma], en los términos que al efecto señale esta Constitución y la Ley Orgánica del Poder Judicial.
>
> El Tribunal Electoral del Poder Judicial del Estado será la máxima autoridad jurisdiccional en la materia: tendrá competencia y organización para funcionar en pleno y salas, y sus sesiones serán públicas. Las resoluciones del tribunal serán emitidas con plenitud de jurisdicción y sus fallos serán definitivos. Estará integrado por cinco magistrados numerarios, uno de los cuales fungirá como, presidente y por los magistrados supernumerarios que harán las veces de jueces instructores.
>
> La administración, vigilancia y disciplina de los recursos presupuestales del Tribunal Electoral del Poder Judicial del Estado, corresponderá en los términos que señale la ley a una comisión del Consejo de la Judicatura; que se integrará por el presidente del Tribunal Electoral, quien la presidirá, un magistrado electoral numerario designado por insaculación; y tres miembros del Consejo de la Judicatura. El tribunal propondrá su presupuesto al presidente de la Sala Superior del Supremo Tribunal de Justicia, para su inclusión en el proyecto del presupuesto del Poder Judicial del Estado, asimismo el tribunal expedirá su Reglamento Interno y los acuerdos generales para su adecuado funcionamiento.
>
> Los jueces y magistrados del Poder Judicial contarán con independencia en el ejercicio de sus funciones. Esta constitución y la Ley Orgánica de la materia establecerán los mecanismos que garanticen dicha independencia, igualmente establecerán las condiciones de ingreso, formación, permanencia y remoción de todo funcionario judicial.
>
> El magistrado presidente del Supremo Tribunal de Justicia tendrá la representación del Poder Judicial del Estado. Presidirá el pleno de la Sala Superior y del Consejo de la Judicatura. Deberá informar por escrito a ambas instancias en el mes de diciembre de cada año, sobre el estado que guarda la impartición y administración de justicia y la situación administrativa del Poder Judicial; de igual manera informará por escrito al Congreso del Estado; y ejercerá las demás atribuciones que le confiera esta Constitución y las leyes que de ella emanen.

389.3. Justamente la Sala Superior asume competencia para conocer las controversias constitucionales; acciones de inconstitucionalidad; acciones por omisión le-

gislativa y consulta judicial; aumentando sus roles con otras funciones implícitas, como son:

I. Garantizar la supremacía y control de la Constitución mediante su interpretación;

II. Conocer de las controversias constitucionales, y acciones de inconstitucionalidad, acciones por omisión legislativa y de las cuestiones de inconstitucionalidad a que se refiere La Constitución Política del Estado en el artículo 56 fracción IV;

III. Conocer, como tribunal de sentencia, de las causas instruidas a los servidores públicos, conforme a la Constitución Política del Estado, así como de las acusaciones por delitos oficiales a que se refieren la Ley de Responsabilidades de los Servidores Públicos, el Código Penal y las demás disposiciones legales aplicables;

IV. Resolver sobre las renuncias de los magistrados y miembros del Consejo de la Judicatura, y en el caso de magistrado, de ser aceptada la misma, dar aviso inmediato al Gobernador del Estado para que proceda a otorgar el nuevo nombramiento, en términos de la Constitución Local;

V. Acordar licencias a los magistrados integrantes de la Sala Superior para separarse del cargo hasta por tres meses y nombrar a quienes los suplan; cuando exceda de este término, deberá dar aviso al Gobernador del Estado, quien procederá a nombrar a los nuevos magistrados en términos de la Constitución Política del Estado;

VI. Emitir acuerdos generales a fin de lograr una adecuada distribución entre los órganos del Poder Judicial respecto de los asuntos que les compete conocer, para la mejor y mayor prontitud de su despacho, así como ordenar el turno de las salas, en los asuntos de su competencia;

VII. Presentar ante el Congreso del Estado, las iniciativas de leyes o decretos relacionados con la organización y funcionamiento de la administración de justicia, con el apoyo del Consejo de la Judicatura;

VIII. Dirimir conflictos de competencia que se susciten entre las Salas regionales o entre los juzgados del Supremo Tribunal de Justicia;

IX. Resolver sobre las contradicciones de criterios generales sustentados por magistrados y entre las Salas del Tribunal, sin perjuicio de observarse la jurisprudencia de los Tribunales Federales. Lo anterior podrá hacerse a petición de parte o de los órganos en conflicto;

X. Emitir acuerdos generales para la correcta elección del juez consejero del Consejo de la Judicatura;

XI. Nombrar a los miembros del Consejo de la Judicatura que corresponda al Poder Judicial;

XII. Ordenar al Consejo de la Judicatura, la investigación sobre los casos de los que se tenga conocimiento o presuma se está transgrediendo la normatividad y, en su caso, el cambio de adscripción de jueces o magistrados de las salas regionales o unitarias, o bien la remoción del cargo por causa justificada;

XIII. Conocer de los asuntos en apelación, de oficio o a petición fundada de la correspondiente sala colegiada o unitaria regional, o del Procurador General de Justicia del Estado, que por su interés o trascendencia así lo ameriten;

XIV. Emitir los criterios jurisdiccionales que coadyuven al mejoramiento de la impartición de justicia; formular las recomendaciones respectivas al Consejo de la Judicatura en los asuntos de su competencia y brindarle el auxilio que solicite en el desempeño de sus funciones de vigilancia;

XV. Calificar las excusas o recusaciones por impedimentos de sus miembros, para conocer de los asuntos de la competencia de la Sala Superior y acordar en la sesión correspondiente, la sustitución que proceda;

XVI. Acordar el registro de los títulos de licenciados en derecho en la secretaría de acuerdos y del pleno de la Sala Superior;

XVII. Decretar la suspensión de labores en los casos en que oficialmente no esté determinada y se considere procedente;

XVIII. Ordenar la compilación y sistematización de doctrina, leyes, precedentes y tesis de jurisprudencia, a través del Consejo de la Judicatura, así como prever las acciones necesarias para su difusión;

XIX. Acordar la aprobación de circulares de contenido jurídico, para que la impartición y administración de justicia sea pronta e imparcial;

XX. Comisionar a sus miembros para las prácticas de visitas a las instituciones de reclusión y readaptación social, con objeto de proveer a una mejor impartición de justicia;

XXI. Dictar el Reglamento Interior del Poder Judicial con excepción del Tribunal Electoral y Tribunal del Servicio Civil;

XXII. Conocer de los asuntos cuya resolución no este expresamente atribuida a otro órgano judicial; y

XXIII. Los demás asuntos que señale la ley u otros ordenamientos aplicables.

El sistema chiapaneco no estatuye mecanismo alguno para la protección de los derechos que la Constitución confiere a sus ciudadanos. No existe, por ende, institución alguna para la defensa de intereses subjetivos, y por ello, los entes legitimados para solicitar la protección de la justicia constitucional son exclusivamente órganos del Estado.

Dentro de las controversias constitucionales cuentan con legitimación el Poder Ejecutivo y el Legislativo, a lado de los municipios. En las acciones de inconstitucionalidad cuentan con ella, el gobernador, el equivalente al 33 por ciento de los integrantes del congreso, el procurador general de justicia y el equivalente al 33 por ciento de los ayuntamientos. En las acciones por omisión legislativa se reconoce legitimación al gobernador, a la tercera parte de los miembros del congreso y a la tercera parte de los ayuntamientos. Dentro de las cuestiones de inconstitucionalidad se reconoce capacidad para elevarlas a todos los magistrados y jueces del Estado.[405]

389.4. Cuando se reglamenta con la Ley de Control Constitucional, es expresivo el mensaje de elevación acompañado, donde se expresa que el control constitucional se conceptúa como aquél proceso que se encuentra instituido en la propia Constitución y tiende a salvaguardar y proteger a la misma, anulando o invalidando toda ley o acto de autoridad que la contravenga y afecte sus disposiciones.

Para ese cometido puede adoptar uno de los varios sistemas de defensa jurídica de la Norma Fundamental, cada uno con sus características específicas, que los distingue y diferencia categóricamente de los demás.

Con esta base se crean las *controversias constitucionales*, la acción de inconstitucionalidad y la acción por omisión legislativa. La primera lleva por objeto ventilar aquellos conflictos que se producen entre dos o más niveles de gobierno estatales,

[405] ASTUDILLO REYES, César I., ob. cit., p. 27.

en que se tilden de inconstitucionales, actos o disposiciones generales emitidos por una entidad, poder u órgano, cuando la cuestión debatida se refiera a la distribución o invasión de competencias que a cada uno le corresponde.

La *acción de inconstitucionalidad* se reconoce como un instrumento o mecanismo de control constitucional por medio del cual el Supremo Tribunal de Justicia adquiere el carácter de Tribunal Constitucional del Estado, cuyas resoluciones adquieren carácter general, y atienden las cuestiones dogmáticas y orgánicas del Código Supremo.

Estas acciones tienen por objeto el puro interés genérico de preservar la supremacía constitucional estatal, y se otorga a una representación parlamentaria calificada; al Procurador General del Estado o al propio Poder Ejecutivo.

Finalmente la *acción por omisión legislativa* es un proceso que tiene por destino garantizar la constitucionalidad de los actos legislativos ya que a éste poder le corresponde la obligación de hacer las leyes, definir el marco jurídico de la acción de gobierno y acentuar el principio de legalidad al que se somete la administración pública, los entes y órganos del Estado, y toda la sociedad en general.

390. El Estado de Quintana Roo

390.1. El control constitucional del Estado tiene por objeto dirimir de manera definitiva e inatacable en el orden jurídico estatal, los conflictos que por la constitucionalidad de sus actos o disposiciones generales, surjan en el ámbito interior del Estado entre el Poder Ejecutivo y el Legislativo o entre uno de ellos y los municipios que conforman el Estado, o entre dos o más municipios, sin perjuicio de lo previsto en los Artículos 76 fracción VII, 103, 105, 107 y último párrafo de la fracción II del 115 de la Constitución Política de los Estados Unidos Mexicanos.

La actividad le corresponde al Tribunal Superior, quien asume competencia positiva para entender de las *controversias* que, por la *constitucionalidad* de sus actos o disposiciones generales (con excepción de las que se refieran a la materia electoral), surjan entre: *a)* el Poder Ejecutivo y el Poder Legislativo; *b)* el Poder Ejecutivo y uno de los municipios; *c)* el Poder Legislativo y uno de los municipios; y *d)* dos o más municipios del Estado. Para que la controversia constitucional proceda, el actor deberá acreditar el interés jurídico.

390.2. Entiende también de las *acciones de inconstitucionalidad* que tengan por objeto plantear la posible contradicción entre una norma de carácter general y la Constitución local, con excepción de las que se refieran a la materia electoral, siempre que se ejerzan dentro de los treinta (30) días naturales siguientes a la fecha de publicación de la norma, por: *a)* cuando menos la tercera parte de los miembros del Congreso del Estado; y *b)* el Procurador General de Justicia del Estado, en contra de Leyes de carácter estatal.

La admisión de una acción de inconstitucionalidad no dará lugar a la suspensión de la norma impugnada.

Las resoluciones del Pleno del Tribunal Superior de Justicia solo podrán declarar la invalidez de las normas impugnadas, siempre que fueren aprobadas por cuando

menos las dos terceras partes del Pleno, y no tendrán efectos retroactivos, salvo en materia penal.

390.3. Otro proceso constitucional autorizado es por *omisión legislativa*, cuando se considere que el Congreso del Estado no ha resuelto sobre la expedición de alguna ley o decreto y que dicha omisión afecte el debido cumplimiento de esta Constitución, que interponga: *a)* el Gobernador del Estado, o *b)* un Ayuntamiento del Estado.

La resolución que emita el Pleno del Tribunal Superior de Justicia que decrete el reconocimiento de la inconstitucionalidad por omisión legislativa, surtirá sus efectos a partir de su publicación en el *Periódico Oficial del Estado*. En dicha resolución se determinará un plazo para que se expida la ley o decreto de que se trate la omisión, a mas tardar en el período ordinario que curse o el inmediato siguiente del Congreso del Estado; pudiendo disminuir este plazo cuando el interés público lo amerite.

390.4. El modelo de Quintana Roo es similar al de Veracruz, en el sentido Kelseniano de confiar todo el control de constitucionalidad a un solo organismo de carácter supremo; así como también se iguala en la distribución del ejercicio de control en dos órganos: el pleno y una sala. La diferencia entre dichos sistemas consiste en que, mientras en Quintana Roo el juez ordinario no participa y no se interesa por el control de constitucionalidad, en Veracruz todos los jueces se interesan en el control mediante la "cuestión de inconstitucionalidad".[406]

> Dejando de lado las atribuciones ordinarias que no interesan para efectos de esta contribución, diremos que en Quintana Roo existen tres procesos constitucionales de naturaleza abstracta y de defensa objetiva del ordenamiento, y dos de naturaleza concreta de tutela de intereses subjetivos.
>
> La legitimación dentro de las controversias constitucionales corresponde a los poderes Ejecutivo y Legislativo, y a los municipios (artículo 105, fracción I de la CQR). En las acciones de inconstitucionalidad corresponde a cuando menos la tercera parte de los miembros del congreso del Estado y al procurador general de justicia del Estado (fracción II). En las acciones por omisión legislativa se confiere competencia para poner en marcha la impartición de justicia constitucional al gobernador del Estado y a los ayuntamientos (fracción III). Dentro de los instrumentos de tutela de intereses subjetivos, la legitimación corresponde a cualquier particular que se sienta afectado en sus derechos por un acto proveniente del Ministerio Público o de alguna autoridad administrativa respecto del derecho de petición.[407]

---

[406] ASTUDILLO REYES, César I., ob. cit., p. 28.

[407] ASTUDILLO REYES, César I., ob. cit., p. 29.

Apéndice documental

1578 blanca

1. Código Procesal Constitucional del Perú

Ley Nº 28.237 ⋮ Código Procesal Constitucional[1]

EL PRESIDENTE DE LA REPÚBLICA

Por cuanto:

El Congreso de la República

Ha dado la Ley siguiente:

ÍNDICE

TÍTULO PRELIMINAR

TÍTULO I. Disposiciones generales de los procesos de *habeas corpus*, amparo, *habeas data* y cumplimiento

TÍTULO II. Proceso de *habeas corpus*
- CAPÍTULO I. Derechos protegidos
- CAPÍTULO II. Procedimiento

TÍTULO III. Proceso de amparo
- CAPÍTULO I. Derechos protegidos
- CAPÍTULO II. Procedimiento

TÍTULO IV. Proceso de *habeas data*

TÍTULO V. Proceso de cumplimiento

TÍTULO VI. Disposiciones generales de los procesos de acción popular e inconstitucionalidad

TÍTULO VII. Proceso de acción popular

TÍTULO VIII. Proceso de inconstitucionalidad

TÍTULO IX. Proceso competencial

TÍTULO X. Jurisdicción internacional

TÍTULO XI. Disposiciones generales aplicables a los procedimientos ante el tribunal constitucional

TÍTULO XII. Disposiciones finales

TÍTULO XIII. Disposiciones transitorias y derogatorias

[1] Promulgado: 28-05-2004. Publicado: 31-05-2004. Vigencia: De conformidad con la Segunda Disposición Transitoria y Derogatoria, entrará en vigencia dentro de (6) seis meses contados a partir de la fecha de su publicación. (30-11-2004). Concordancias: R.ADM. N° 095-2004-P-TC (Reglamento Normativo del T.C.).

TÍTULO PRELIMINAR

ART. I.—*Alcances*

El presente Código regula los procesos constitucionales de *habeas corpus*, amparo, *habeas data*, cumplimiento, inconstitucionalidad, acción popular y los conflictos de competencia, previstos en los artículos 200 y 202 inciso 3) de la Constitución.

ART. II.—*Fines de los Procesos Constitucionales*

Son fines esenciales de los procesos constitucionales garantizar la primacía de la Constitución y la vigencia efectiva de los derechos constitucionales.

ART. III.—*Principios Procesales*

Los procesos constitucionales se desarrollan con arreglo a los principios de dirección judicial del proceso, gratuidad en la actuación del demandante, economía, inmediación y socialización procesales.

El Juez y el Tribunal Constitucional tienen el deber de impulsar de oficio los procesos, salvo en los casos expresamente señalados en el presente Código.

Asimismo, el Juez y el Tribunal Constitucional deben adecuar la exigencia de las formalidades previstas en este Código al logro de los fines de los procesos constitucionales.

Cuando en un proceso constitucional se presente una duda razonable respecto de si el proceso debe declararse concluido, el Juez y el Tribunal Constitucional declararán su continuación.

La gratuidad prevista en este artículo no obsta el cumplimiento de la resolución judicial firme que disponga la condena en costas y costos conforme a lo previsto por el presente Código.

ART. IV.—*Órganos Competentes*

Los procesos constitucionales son de conocimiento del Poder Judicial y del Tribunal Constitucional, de conformidad con lo dispuesto en la Constitución, en sus respectivas leyes orgánicas y en el presente Código.

ART. V.—*Interpretación de los Derechos Constitucionales*

El contenido y alcances de los derechos constitucionales protegidos por los procesos regulados en el presente Código deben interpretarse de conformidad con la Declaración Universal de Derechos Humanos, los tratados sobre derechos humanos, así como de las decisiones adoptadas por los tribunales internacionales sobre derechos humanos constituidos según tratados de los que el Perú es parte.

ART. Vl.—*Control Difuso e Interpretación Constitucional*

Cuando exista incompatibilidad entre una norma constitucional y otra de inferior jerarquía, el Juez debe preferir la primera, siempre que ello sea relevante para resolver la controversia y no sea posible obtener una interpretación conforme a la Constitución.

Los Jueces no pueden dejar de aplicar una norma cuya constitucionalidad haya sido confirmada en un proceso de inconstitucionalidad o en un proceso de acción popular.

Los Jueces interpretan y aplican las leyes o toda norma con rango de ley y los reglamentos según los preceptos y principios constitucionales, conforme a la interpretación de los mismos que resulte de las resoluciones dictadas por el Tribunal Constitucional.

ART. VII.—*Precedente*

Las sentencias del Tribunal Constitucional que adquieren la autoridad de cosa juzgada constituyen precedente vinculante cuando así lo exprese la sentencia, precisando el extremo

de su efecto normativo. Cuando el Tribunal Constitucional resuelva apartándose del precedente, debe expresar los fundamentos de hecho y de derecho que sustentan la sentencia y las razones por las cuales se aparta del precedente.

ART. VIII.—*Juez y Derecho*

El órgano jurisdiccional competente debe aplicar el derecho que corresponda al proceso, aunque no haya sido invocado por las partes o lo haya sido erróneamente.

ART. IX.—*Aplicación Supletoria e Integración*

En caso de vacío o defecto de la presente ley, serán de aplicación supletoria los Códigos Procesales afines a la materia discutida, siempre que no contradigan los fines de los procesos constitucionales y los ayuden a su mejor desarrollo. En defecto de las normas supletorias citadas, el Juez podrá recurrir a la jurisprudencia, a los principios generales del derecho procesal y a la doctrina.

TÍTULO I
Disposiciones generales de los procesos de habeas corpus, amparo, habeas data y cumplimiento

ART. 1.—*Finalidad de los Procesos*

Los procesos a los que se refiere el presente título tienen por finalidad proteger los derechos constitucionales, reponiendo las cosas al estado anterior a la violación o amenaza de violación de un derecho constitucional, o disponiendo el cumplimiento de un mandato legal o de un acto administrativo.

Si luego de presentada la demanda cesa la agresión o amenaza por decisión voluntaria del agresor, o si ella deviene en irreparable, el Juez, atendiendo al agravio producido, declarará fundada la demanda precisando los alcances de su decisión, disponiendo que el emplazado no vuelva a incurrir en las acciones u omisiones que motivaron la interposición de la demanda, y que si procediere de modo contrario se le aplicarán las medidas coercitivas previstas en el artículo 22 del presente Código, sin perjuicio de la responsabilidad penal que corresponda.

ART. 2.—*Procedencia*

Los procesos constitucionales de *habeas corpus*, amparo y *habeas data* proceden cuando se amenace o viole los derechos constitucionales por acción u omisión de actos de cumplimiento obligatorio, por parte de cualquier autoridad, funcionario o persona. Cuando se invoque la amenaza de violación, ésta debe ser cierta y de inminente realización. El proceso de cumplimiento procede para que se acate una norma legal o se ejecute un acto administrativo.

ART. 3.—Procedencia frente a actos basados en normas

Cuando se invoque la amenaza o violación de actos que tienen como sustento la aplicación de una norma incompatible con la Constitución, la sentencia que declare fundada la demanda dispondrá, además, la inaplicabilidad de la citada norma.

Artículo modificado por la Ley Nº 28946, publicada el 24 de diciembre del 2006, cuyo texto es el siguiente:

"ART. 3.—*Procedencia frente a actos basados en normas*

Cuando se invoque la amenaza o violación de actos que tienen como sustento la aplicación de una norma autoaplicativa incompatible con la Constitución, la sentencia que declare fundada la demanda dispondrá, además, la inaplicabilidad de la citada norma.

Son normas autoaplicativas, aquellas cuya aplicabilidad, una vez que han entrado en vigencia, resulta inmediata e incondicionada.

Las decisiones jurisdiccionales que se adopten en aplicación del control difuso de la constitucionalidad de las normas, serán elevadas en consulta a la Sala Constitucional y Social de la Corte Suprema de Justicia de la República, si no fueran impugnadas. Lo son igualmente las resoluciones judiciales en segunda instancia en las que se aplique este mismo precepto, aun cuando contra éstas no proceda medio impugnatorio alguno.

En todos estos casos, los Jueces se limitan a declarar la inaplicación de la norma por incompatibilidad inconstitucional, para el caso concreto, sin afectar su vigencia, realizando interpretación constitucional, conforme a la forma y modo que la Constitución establece.

Cuando se trata de normas de menor jerarquía, rige el mismo principio, no requiriéndose la elevación en consulta, sin perjuicio del proceso de acción popular. La consulta a que hace alusión el presente artículo se hace en interés de la ley".

ART. 4.—*Procedencia respecto de resoluciones judiciales*

El amparo procede respecto de resoluciones judiciales firmes dictadas con manifiesto agravio a la tutela procesal efectiva, que comprende el acceso a la justicia y el debido proceso. Es improcedente cuando el agraviado dejó consentir la resolución que dice afectarlo.

El *habeas corpus* procede cuando una resolución judicial firme vulnera en forma manifiesta la libertad individual y la tutela procesal efectiva.

Se entiende por tutela procesal efectiva aquella situación jurídica de una persona en la que se respetan, de modo enunciativo, sus derechos de libre acceso al órgano jurisdiccional, a probar, de defensa, al contradictorio e igualdad sustancial en el proceso, a no ser desviado de la jurisdicción predeterminada ni sometido a procedimientos distintos de los previstos por la ley, a la obtención de una resolución fundada en derecho, a acceder a los medios impugnatorios regulados, a la imposibilidad de revivir procesos fenecidos, a la actuación adecuada y temporalmente oportuna de las resoluciones judiciales y a la observancia del principio de legalidad procesal penal.

ART. 5.—*Causales de improcedencia*

No proceden los procesos constitucionales cuando:

1. Los hechos y el petitorio de la demanda no están referidos en forma directa al contenido constitucionalmente protegido del derecho invocado;

2. Existan vías procedimentales específicas, igualmente satisfactorias, para la protección del derecho constitucional amenazado o vulnerado, salvo cuando se trate del proceso de *habeas corpus*;

3. El agraviado haya recurrido previamente a otro proceso judicial para pedir tutela respecto de su derecho constitucional;

4. No se hayan agotado las vías previas, salvo en los casos previstos por este Código y en el proceso de *habeas corpus*;

5. A la presentación de la demanda ha cesado la amenaza o violación de un derecho constitucional o se ha convertido en irreparable;

6. Se cuestione una resolución firme recaída en otro proceso constitucional o haya litispendencia;

7. Se cuestionen las resoluciones definitivas del Consejo Nacional de la Magistratura en materia de destitución y ratificación de jueces y fiscales, siempre que dichas resoluciones hayan sido motivadas y dictadas con previa audiencia al interesado;

8. Se cuestionen las resoluciones del Jurado Nacional de Elecciones en materia electoral, salvo cuando no sean de naturaleza jurisdiccional o cuando siendo jurisdiccionales violen la tutela procesal efectiva.

Tampoco procede contra las resoluciones de la Oficina Nacional de Procesos Electorales y del Registro Nacional de Identificación y Estado Civil si pueden ser revisadas por el Jurado Nacional de Elecciones;*

*Numeral modificado por el artículo único de la Ley N° 28642 (publicada en el diario oficial El Peruano el 08 Diciembre 2005), siendo el nuevo texto el siguiente:

8. Se cuestionen las resoluciones del Jurado Nacional de Elecciones en materias electorales, de referéndum o de otro tipo de consultas populares, bajo responsabilidad.

Resoluciones en contrario, de cualquier autoridad, no surten efecto legal alguno.

La materia electoral comprende los temas previstos en las leyes electorales y aquellos que conoce el Jurado Nacional de Elecciones en instancia definitiva.*

*La STC N° 0007-2007-PI (publicada en el diario oficial El Peruano el 22 de junio de 2007) dejó sin efecto el citado artículo único de la Ley N° 28642, toda vez que declaró su inconstitucionalidad.

El segundo párrafo del artículo 83º del Código Procesal Constitucional establece que "Por la declaración de ilegalidad o inconstitucionalidad de una norma no recobran vigencia las disposiciones legales que ella hubiera derogado".

9. Se trate de conflictos entre entidades de derecho público interno. Los conflictos constitucionales surgidos entre dichas entidades, sean poderes del Estado, órganos de nivel o relevancia constitucional, gobiernos locales y regionales, serán resueltos por las vías procedimentales correspondientes;

10. Ha vencido el plazo para interponer la demanda, con excepción del proceso de *habeas corpus*.

ART. 6.—*Cosa Juzgada*

En los procesos constitucionales sólo adquiere la autoridad de cosa juzgada la decisión final que se pronuncie sobre el fondo.

ART. 7.—*Representación Procesal del Estado*

La defensa del Estado o de cualquier funcionario o servidor público está a cargo del Procurador Público o del representante legal respectivo, quien deberá ser emplazado con la demanda. Además, debe notificarse con ella a la propia entidad estatal o al funcionario o servidor demandado, quienes pueden intervenir en el proceso. Aun cuando no se apersonaran, se les debe notificar la resolución que ponga fin al grado. Su no participación no afecta la validez del proceso.

Las instituciones públicas con rango constitucional actuarán directamente, sin la intervención del Procurador Público. Del mismo modo, actuarán directamente las entidades que tengan personería jurídica propia.

El Procurador Público, antes de que el proceso sea resuelto en primer grado, está facultado para poner en conocimiento del titular de la entidad su opinión profesional motivada cuando considere que se afecta el derecho constitucional invocado.

Si el demandante conoce, antes de demandar o durante el proceso, que el funcionario contra quien dirige la demanda ya no ocupa tal cargo, puede solicitar al Juez que este no sea emplazado con la demanda.

*Derógase el segundo párrafo del artículo 7 del Código Procesal Constitucional, derogado por la Ley Nº 28946, publicada el 24 de diciembre del 2006, cuyo texto es el siguiente:

"Derógase el segundo párrafo del artículo 7 del Código Procesal Constitucional."

ART. 8.—*Responsabilidad del agresor*

Cuando exista causa probable de la comisión de un delito, el Juez, en la sentencia que declara fundada la demanda en los procesos tratados en el presente título, dispondrá la remisión de los actuados al Fiscal Penal que corresponda para los fines pertinentes. Esto ocurrirá, inclusive, cuando se declare la sustracción de la pretensión y sus efectos, o cuando la violación del derecho constitucional haya devenido en irreparable, si el Juez así lo considera.

Tratándose de autoridad o funcionario público, el Juez Penal podrá imponer como pena accesoria la destitución del cargo.

El haber procedido por orden superior no libera al ejecutor de la responsabilidad por el agravio incurrido ni de la pena a que haya lugar. Si el responsable inmediato de la violación fuera una de las personas comprendidas en el artículo 99 de la Constitución, se dará cuenta inmediata a la Comisión Permanente para los fines consiguientes.

Concordancias: R.ADM. N° 095-2004-P-TC, Reg. Normativo del T.C., Art. 50, Últ. párrafo

ART. 9.—*Ausencia de etapa probatoria*

En los procesos constitucionales no existe etapa probatoria. Sólo son procedentes los medios probatorios que no requieren actuación, lo que no impide la realización de las actuaciones probatorias que el Juez considere indispensables, sin afectar la duración del proceso. En este último caso no se requerirá notificación previa.

ART. 10.—*Excepciones y defensas previas*

Las excepciones y defensas previas se resuelven, previo traslado, en la sentencia. No proceden en el proceso de *habeas corpus*.

*Artículo modificado por la Ley Nº 28946, publicada el 24 de diciembre del 2006, cuyo texto es el siguiente:

"ART. 10.—*Excepciones y defensas previas*

Las excepciones y defensas previas se resuelven, previo traslado, en el auto de saneamiento procesal. No proceden en el proceso de *habeas corpus*."

ART. 11.—*Integración de decisiones*

Los jueces superiores integrarán las decisiones cuando adviertan alguna omisión en la sentencia, siempre que en ella aparezcan los fundamentos que permitan integrar tal omisión.

ART. 12.—*Turno*

El inicio de los procesos constitucionales se sujetará a lo establecido para el turno en cada distrito judicial, salvo en los procesos de *habeas corpus* en donde es competente cualquier juez penal de la localidad.

ART. 13.—*Tramitación preferente*

Los jueces tramitarán con preferencia los procesos constitucionales. La responsabilidad por la defectuosa o tardía tramitación de estos, será exigida y sancionada por los órganos competentes.

ART. 14.—*Notificaciones*

Todas las resoluciones serán notificadas oportunamente a las partes, con excepción de las actuaciones a que se refiere el artículo 9 del presente Código.

ART. 15.—*Medidas Cautelares*

Se pueden conceder medidas cautelares y de suspensión del acto violatorio en los procesos de amparo, *habeas data* y de cumplimiento. Para su expedición se exigirá apariencia del derecho, peligro en la demora y que el pedido cautelar sea adecuado para garantizar la eficacia de la pretensión. Se dictan sin conocimiento de la contraparte y la apelación sólo es concedida

sin efecto suspensivo. Su procedencia, trámite y ejecución dependen del contenido de la pretensión constitucional intentada y del aseguramiento de la decisión final.

El juez al conceder la medida atenderá al límite de irreversibilidad de la misma.

Cuando la solicitud de medida cautelar tenga por objeto dejar sin efecto actos administrativos dictados en el ámbito de aplicación de la legislación municipal o regional, serán conocidas en primera instancia por la Sala competente de la Corte Superior de Justicia del Distrito Judicial correspondiente.

De la solicitud se corre traslado por el término de tres días, acompañando copia certificada de la demanda y sus recaudos, así como de la resolución que la da por admitida, tramitando el incidente en cuerda separada, con intervención del Ministerio Público. Con la contestación expresa o ficta la Corte Superior resolverá dentro del plazo de tres días, bajo responsabilidad salvo que se haya formulado solicitud de informe oral, en cuyo caso el plazo se computará a partir de la fecha de su realización. La resolución que dicta la Corte será recurrible con efecto suspensivo ante la Corte Suprema de Justicia de la República, la que resolverá en el plazo de diez días de elevados los autos, bajo responsabilidad.

En todo lo no previsto expresamente en el presente Código, será de aplicación supletoria lo dispuesto en el Título IV de la Sección Quinta del Código Procesal Civil, con excepción de los artículos 618, 621, 630, 636 y 642 al 672.

*Artículo modificado por la Ley Nº 28946, publicada el 24 de diciembre del 2006, cuyo texto es el siguiente:

"ART. 15.—Medidas Cautelares

Se pueden conceder medidas cautelares y de suspensión del acto violatorio en los procesos de amparo, *habeas data* y de cumplimiento, sin transgredir lo establecido en el primer párrafo del artículo 3 de este Código. Para su expedición se exigirá apariencia del derecho, peligro en la demora y que el pedido cautelar sea adecuado o razonable para garantizar la eficacia de la pretensión. Se dictan sin conocimiento de la contraparte y la apelación sólo es concedida sin efecto suspensivo; salvo que se trate de resoluciones de medidas cautelares que declaren la inaplicación de normas legales autoaplicativas, en cuyo caso la apelación es con efecto suspensivo.

Su procedencia, trámite y ejecución dependerán del contenido de la pretensión constitucional intentada y del adecuado aseguramiento de la decisión final, a cuyos extremos deberá limitarse. Por ello mismo, el Juez al conceder en todo o en parte la medida solicitada deberá atender a la irreversibilidad de la misma y al perjuicio que por la misma se pueda ocasionar en armonía con el orden público, la finalidad de los procesos constitucionales y los postulados constitucionales.

Cuando la solicitud de medida cautelar tenga por objeto dejar sin efecto actos administrativos dictados en el ámbito de aplicación de la legislación municipal o regional, se correrá traslado por el término de tres días, acompañando copia certificada de la demanda y sus recaudos, así como la resolución que la da por admitida, tramitando el incidente por cuerda separada, con intervención del Ministerio Público. Con la contestación expresa o ficta, el Juez resolverá dentro del plazo de tres días, bajo responsabilidad.

En todo lo no previsto expresamente en el presente Código, será de aplicación supletoria lo dispuesto en el Título IV de la Sección Quinta del Código Procesal Civil, con excepción de los artículos 618, 621, 630, 636 y 642 al 672.

ART. 16.—*Extinción de la medida cautelar*

La medida cautelar se extingue de pleno derecho cuando la resolución que concluye el proceso ha adquirido la autoridad de cosa juzgada.

Si la resolución final constituye una sentencia estimatoria, se conservan los efectos de la medida cautelar, produciéndose una conversión de pleno derecho de la misma en medida ejecutiva. Los efectos de esta medida permanecen hasta el momento de la satisfacción del derecho reconocido al demandante, o hasta que el juez expida una resolución modificatoria o extintiva durante la fase de ejecución.

Si la resolución última no reconoce el derecho reclamado por el demandante, se procede a la liquidación de costas y costos del procedimiento cautelar. El sujeto afectado por la medida cautelar puede promover la declaración de responsabilidad. De verificarse la misma, en modo adicional a la condena de costas y costos, se procederá a la liquidación y ejecución de los daños y, si el juzgador lo considera necesario, a la imposición de una multa no mayor de diez Unidades de Referencia Procesal.

La resolución que fija las costas y costos es apelable sin efecto suspensivo; la que establece la reparación indemnizatoria y la multa lo es con efecto suspensivo.

En lo que respecta al pago de costas y costos se estará a lo dispuesto por el artículo 56.

ART. 17.—*Sentencia*

La sentencia que resuelve los procesos a que se refiere el presente título, deberá contener, según sea el caso:

1) La identificación del demandante;

2) La identificación de la autoridad, funcionario o persona de quien provenga la amenaza, violación o que se muestre renuente a acatar una norma legal o un acto administrativo;

3) La determinación precisa del derecho vulnerado, o la consideración de que el mismo no ha sido vulnerado, o, de ser el caso, la determinación de la obligación incumplida;

4) La fundamentación que conduce a la decisión adoptada;

5) La decisión adoptada señalando, en su caso, el mandato concreto dispuesto.

Concordancias: R.ADM. N° 095-2004-P-TC, Reg. Normativo del T.C., Art. 47

ART. 18.—*Recurso de agravio constitucional*

Contra la resolución de segundo grado que declara infundada o improcedente la demanda, procede recurso de agravio constitucional ante el Tribunal Constitucional, dentro del plazo de diez días contados desde el día siguiente de notificada la resolución. Concedido el recurso, el Presidente de la Sala remite al Tribunal Constitucional el expediente dentro del plazo máximo de tres días, más el término de la distancia, bajo responsabilidad.

ART. 19.—*Recurso de queja*

Contra la resolución que deniega el recurso de agravio constitucional procede recurso de queja. Este se interpone ante el Tribunal Constitucional dentro del plazo de cinco días siguientes a la notificación de la denegatoria. Al escrito que contiene el recurso y su fundamentación, se anexa copia de la resolución recurrida y de la denegatoria, certificadas por abogado, salvo el caso del proceso de *habeas corpus*. El recurso será resuelto dentro de los diez días de recibido, sin dar lugar a trámite. Si el Tribunal Constitucional declara fundada la queja, conoce también el recurso de agravio constitucional, ordenando al juez superior el envío del expediente dentro del tercer día de oficiado, bajo responsabilidad.

ART. 20.—*Pronunciamiento del Tribunal Constitucional*

Dentro de un plazo máximo de veinte días tratándose de las resoluciones denegatorias de los procesos de *habeas corpus*, y treinta cuando se trata de los procesos de amparo, *ha-*

beas data y de cumplimiento, el Tribunal Constitucional se pronunciará sobre el recurso interpuesto.

Si el Tribunal considera que la resolución impugnada ha sido expedida incurriéndose en un vicio del proceso que ha afectado el sentido de la decisión, la anulará y ordenará se reponga el trámite al estado inmediato anterior a la ocurrencia del vicio. Sin embargo, si el vicio incurrido sólo alcanza a la resolución impugnada, el Tribunal la revoca y procede a pronunciarse sobre el fondo.

ART. 21.—*Incorporación de medios probatorios sobre hechos nuevos al proceso*

Los medios probatorios que acreditan hechos trascendentes para el proceso, pero que ocurrieron con posterioridad a la interposición de la demanda, pueden ser admitidos por el Juez a la controversia principal o a la cautelar, siempre que no requieran actuación. El Juez pondrá el medio probatorio en conocimiento de la contraparte antes de expedir la resolución que ponga fin al grado.

ART. 22.—*Actuación de Sentencias*

La sentencia que cause ejecutoria en los procesos constitucionales se actúa conforme a sus propios términos por el juez de la demanda. Las sentencias dictadas por los jueces constitucionales tienen prevalencia sobre las de los restantes órganos jurisdiccionales y deben cumplirse bajo responsabilidad.

La sentencia que ordena la realización de una prestación de dar, hacer o no hacer es de actuación inmediata. Para su cumplimiento, y de acuerdo al contenido específico del mandato y de la magnitud del agravio constitucional, el Juez podrá hacer uso de multas fijas o acumulativas e incluso disponer la destitución del responsable. Cualquiera de estas medidas coercitivas debe ser incorporada como apercibimiento en la sentencia, sin perjuicio de que, de oficio o a pedido de parte, las mismas puedan ser modificadas durante la fase de ejecución.

El monto de las multas lo determina discrecionalmente el Juez, fijándolo en Unidades de Referencia Procesal y atendiendo también a la capacidad económica del requerido. Su cobro se hará efectivo con el auxilio de la fuerza pública, el recurso a una institución financiera o la ayuda de quien el Juez estime pertinente.

El Juez puede decidir que las multas acumulativas asciendan hasta el cien por ciento por cada día calendario, hasta el acatamiento del mandato judicial.

El monto recaudado por las multas constituye ingreso propio del Poder Judicial, salvo que la parte acate el mandato judicial dentro de los tres días posteriores a la imposición de la multa. En este último caso, el monto recaudado será devuelto en su integridad a su titular.

ART. 23.—*Procedencia durante los regímenes de excepción*

Razonabilidad y proporcionalidad. Los procesos constitucionales no se suspenden durante la vigencia de los regímenes de excepción. Cuando se interponen en relación con derechos suspendidos, el órgano jurisdiccional examinará la razonabilidad y proporcionalidad del acto restrictivo, atendiendo a los siguientes criterios:

1) Si la demanda se refiere a derechos constitucionales que no han sido suspendidos;

2) Si tratándose de derechos suspendidos, las razones que sustentan el acto restrictivo del derecho no tienen relación directa con las causas o motivos que justificaron la declaración del régimen de excepción; o,

3) Si tratándose de derechos suspendidos, el acto restrictivo del derecho resulta manifiestamente innecesario o injustificado atendiendo a la conducta del agraviado o a la situación de hecho evaluada sumariamente por el juez.

La suspensión de los derechos constitucionales tendrá vigencia y alcance únicamente en los ámbitos geográficos especificados en el decreto que declara el régimen de excepción.

ART. 24.—*Agotamiento de la jurisdicción nacional*

La resolución del Tribunal Constitucional que se pronuncie sobre el fondo agota la jurisdicción nacional.

TÍTULO II
Proceso de habeas corpus

CAPÍTULO I
Derechos protegidos

ART. 25.—*Derechos protegidos*

Procede el *habeas corpus* ante la acción u omisión que amenace o vulnere los siguientes derechos que, enunciativamente, conforman la libertad individual:

1) La integridad personal, y el derecho a no ser sometido a tortura o tratos inhumanos o humillantes, ni violentado para obtener declaraciones.

2) El derecho a no ser obligado a prestar juramento ni compelido a declarar o reconocer culpabilidad contra sí mismo, contra su cónyuge, o sus parientes dentro del cuarto grado de consanguinidad o segundo de afinidad.

3) El derecho a no ser exiliado o desterrado o confinado sino por sentencia firme.

4) El derecho a no ser expatriado ni separado del lugar de residencia sino por mandato judicial o por aplicación de la Ley de Extranjería.

5) El derecho del extranjero, a quien se ha concedido asilo político, de no ser expulsado al país cuyo gobierno lo persigue, o en ningún caso si peligrase su libertad o seguridad por el hecho de ser expulsado.

6) El derecho de los nacionales o de los extranjeros residentes a ingresar, transitar o salir del territorio nacional, salvo mandato judicial o aplicación de la Ley de Extranjería o de Sanidad.

7) El derecho a no ser detenido sino por mandato escrito y motivado del Juez, o por las autoridades policiales en caso de flagrante delito; o si ha sido detenido, a ser puesto dentro de las 24 horas o en el término de la distancia, a disposición del juzgado que corresponda, de acuerdo con el acápite "f" del inciso 24) del artículo 2 de la Constitución sin perjuicio de las excepciones que en él se consignan.

8) El derecho a decidir voluntariamente prestar el servicio militar, conforme a la ley de la materia.

9) El derecho a no ser detenido por deudas.

10) El derecho a no ser privado del documento nacional de identidad, así como de obtener el pasaporte o su renovación dentro o fuera de la República.

11) El derecho a no ser incomunicado sino en los casos establecidos por el literal "g" del inciso 24) del artículo 2 de la Constitución.

12) El derecho a ser asistido por un abogado defensor libremente elegido desde que se es citado o detenido por la autoridad policial u otra, sin excepción.

13) El derecho a retirar la vigilancia del domicilio y a suspender el seguimiento policial, cuando resulten arbitrarios o injustificados.

14) El derecho a la excarcelación de un procesado o condenado, cuya libertad haya sido declarada por el juez.

15) El derecho a que se observe el trámite correspondiente cuando se trate del procedimiento o detención de las personas, a que se refiere el artículo 99 de la Constitución.

16) El derecho a no ser objeto de una desaparición forzada.

17) El derecho del detenido o recluso a no ser objeto de un tratamiento carente de razonabilidad y proporcionalidad, respecto de la forma y condiciones en que cumple el mandato de detención o la pena.

También procede el *habeas corpus* en defensa de los derechos constitucionales conexos con la libertad individual, especialmente cuando se trata del debido proceso y la inviolabilidad del domicilio.

CAPÍTULO II
Procedimiento

ART. 26.—*Legitimación*

La demanda puede ser interpuesta por la persona perjudicada o por cualquier otra en su favor, sin necesidad de tener su representación. Tampoco requerirá firma del letrado, tasa o alguna otra formalidad. También puede interponerla la Defensoría del Pueblo.

ART. 27.—*Demanda*

La demanda puede presentarse por escrito o verbalmente, en forma directa o por correo, a través de medios electrónicos de comunicación u otro idóneo. Cuando se trata de una demanda verbal, se levanta acta ante el Juez o Secretario, sin otra exigencia que la de suministrar una sucinta relación de los hechos.

ART. 28.—*Competencia*

La demanda de *habeas corpus* se interpone ante cualquier Juez Penal, sin observar turnos.

ART. 29.—*Competencia del Juez de Paz*

Cuando la afectación de la libertad individual se realice en lugar distinto y lejano o de difícil acceso de aquel en que tiene su sede el Juzgado donde se interpuso la demanda este dictará orden perentoria e inmediata para que el Juez de Paz del distrito en el que se encuentra el detenido cumpla en el día, bajo responsabilidad, con hacer las verificaciones y ordenar las medidas inmediatas para hacer cesar la afectación.

ART. 30.—*Trámite en caso de detención arbitraria*

Tratándose de cualquiera de las formas de detención arbitraria y de afectación de la integridad personal, el Juez resolverá de inmediato. Para ello podrá constituirse en el lugar de los hechos, y verificada la detención indebida ordenará en el mismo lugar la libertad del agraviado, dejando constancia en el acta correspondiente y sin que sea necesario notificar previamente al responsable de la agresión para que cumpla la resolución judicial.

ART. 31.—*Trámite en casos distintos*

Cuando no se trate de una detención arbitraria ni de una vulneración de la integridad personal, el Juez podrá constituirse en el lugar de los hechos, o, de ser el caso, citar a quien o quienes ejecutaron la violación, requiriéndoles expliquen la razón que motivó la agresión, y resolverá de plano en el término de un día natural, bajo responsabilidad.

La resolución podrá notificarse al agraviado, así se encontrare privado de su libertad. También puede notificarse indistintamente a la persona que interpuso la demanda así como a su abogado, si lo hubiere.

ART. 32.—*Trámite en caso de desaparición forzada*

Sin perjuicio del trámite previsto en los artículos anteriores, cuando se trate de la desaparición forzada de una persona, si la autoridad, funcionario o persona demandada no proporcionan elementos de juicio satisfactorios sobre su paradero o destino, el Juez deberá adoptar todas las medidas necesarias que conduzcan a su hallazgo, pudiendo incluso comisionar a jueces del Distrito Judicial donde se presuma que la persona pueda estar detenida para que las practiquen. Asimismo, el Juez dará aviso de la demanda de *habeas corpus* al Ministerio Público para que realice las investigaciones correspondientes.

Si la agresión se imputa a algún miembro de la Policía Nacional o de las Fuerzas Armadas, el juez solicitará, además, a la autoridad superior del presunto agresor de la zona en la cual la desaparición ha ocurrido, que informe dentro del plazo de veinticuatro horas si es cierta o no la vulneración de la libertad y proporcione el nombre de la autoridad que la hubiere ordenado o ejecutado.

ART. 33.—*Normas especiales de procedimiento*

Este proceso se somete además a las siguientes reglas:

1) No cabe recusación, salvo por el afectado o quien actúe en su nombre.

3) No caben excusas de los jueces ni de los secretarios.

4) Los jueces deberán habilitar día y hora para la realización de las actuaciones procesales.

5) No interviene el Ministerio Público.

6) Se pueden presentar documentos cuyo mérito apreciará el juez en cualquier estado del proceso.

7) El Juez o la Sala designará un defensor de oficio al demandante, si lo pidiera.

8) Las actuaciones procesales son improrrogables.

ART. 34.—Contenido de sentencia fundada

La resolución que declara fundada la demanda de *habeas corpus* dispondrá alguna de las siguientes medidas:

1) La puesta en libertad de la persona privada arbitrariamente de este derecho; o

2) Que continúe la situación de privación de libertad de acuerdo con las disposiciones legales aplicables al caso, pero si el Juez lo considerase necesario, ordenará cambiar las condiciones de la detención, sea en el mismo establecimiento o en otro, o bajo la custodia de personas distintas de las que hasta entonces la ejercían; o

3) Que la persona privada de libertad sea puesta inmediatamente a disposición del Juez competente, si la agresión se produjo por haber transcurrido el plazo legalmente establecido para su detención; o

4) Que cese el agravio producido, disponiendo las medidas necesarias para evitar que el acto vuelva a repetirse.

Concordancias: R.ADM. N° 095-2004-P-TC, Reg. Normativo del T.C., Art. 47, Últ. párrafo

ART. 35.—*Apelación*

Sólo es apelable la resolución que pone fin a la instancia. El plazo para apelar es de dos días.

ART. 36.—*Trámite de Apelación*

Interpuesta la apelación el Juez elevará en el día los autos al Superior, quien resolverá el proceso en el plazo de cinco días bajo responsabilidad. A la vista de la causa los abogados podrán informar.

TÍTULO III
Proceso de amparo

CAPÍTULO I
Derechos protegidos

ART. 37.—Derechos protegidos

El amparo procede en defensa de los siguientes derechos:

1) De igualdad y de no ser discriminado por razón de origen, sexo, raza, orientación sexual, religión, opinión, condición económica, social, idioma, o de cualquier otra índole;

2) Del ejercicio público de cualquier confesión religiosa;

3) De información, opinión y expresión;

4) A la libre contratación;

5) A la creación artística, intelectual y científica;

6) De la inviolabilidad y secreto de los documentos privados y de las comunicaciones;

7) De reunión;

8) Del honor, intimidad, voz, imagen y rectificación de informaciones inexactas o agraviantes;

9) De asociación;

10) Al trabajo;

11) De sindicación, negociación colectiva y huelga;

12) De propiedad y herencia;

13) De petición ante la autoridad competente;

14) De participación individual o colectiva en la vida política del país;

15) A la nacionalidad;

16) De tutela procesal efectiva;

17) A la educación, así como el derecho de los padres de escoger el centro de educación y participar en el proceso educativo de sus hijos;

18) De impartir educación dentro de los principios constitucionales;

19) A la seguridad social;

20) De la remuneración y pensión;

21) De la libertad de cátedra;

22) De acceso a los medios de comunicación social en los términos del artículo 35 de la Constitución;

23) De gozar de un ambiente equilibrado y adecuado al desarrollo de la vida;

24) A la salud; y

25) Los demás que la Constitución reconoce.

ART. 38.—*Derechos no protegidos*

No procede el amparo en defensa de un derecho que carece de sustento constitucional directo o que no está referido a los aspectos constitucionalmente protegidos del mismo.

CAPÍTULO II
Procedimiento

ART. 39.—*Legitimación*

El afectado es la persona legitimada para interponer el proceso de amparo.

ART. 40.—*Representación Procesal*

EI afectado puede comparecer por medio de representante procesal. No es necesaria la inscripción de la representación otorgada.

Tratándose de personas no residentes en el país, la demanda será formulada por representante acreditado. Para este efecto, será suficiente el poder fuera de registro otorgado ante el Cónsul del Perú en la ciudad extranjera que corresponda y la legalización de la firma del Cónsul ante el Ministerio de Relaciones Exteriores, no siendo necesaria la inscripción en los Registros Públicos.

Asimismo, puede interponer demanda de amparo cualquier persona cuando se trate de amenaza o violación del derecho al medio ambiente u otros derechos difusos que gocen de reconocimiento constitucional, así como las entidades sin fines de lucro cuyo objeto sea la defensa de los referidos derechos.

La Defensoría del Pueblo puede interponer demanda de amparo en ejercicio de sus competencias constitucionales.

ART. 41.—*Procuración Oficiosa*

Cualquier persona puede comparecer en nombre de quien no tiene representación procesal, cuando esta se encuentre imposibilitada para interponer la demanda por sí misma, sea por atentado concurrente contra la libertad individual, por razones de fundado temor o amenaza, por una situación de inminente peligro o por cualquier otra causa análoga. Una vez que el afectado se halle en posibilidad de hacerlo, deberá ratificar la demanda y la actividad procesal realizada por el procurador oficioso.

ART. 42.—*Demanda*

La demanda escrita contendrá, cuando menos, los siguientes datos y anexos:

1) La designación del Juez ante quien se interpone;

2) El nombre, identidad y domicilio procesal del demandante;

3) El nombre y domicilio del demandado, sin perjuicio de lo previsto en el artículo 7 del presente Código;

4) La relación numerada de los hechos que hayan producido, o estén en vías de producir la agresión del derecho constitucional;

5) Los derechos que se consideran violados o amenazados;

6) El petitorio, que comprende la determinación clara y concreta de lo que se pide;

7) La firma del demandante o de su representante o de su apoderado, y la del abogado.

En ningún caso la demanda podrá ser rechazada por el personal administrativo del Juzgado o Sala correspondiente.

ART. 43.—*Acumulación subjetiva de oficio*

Cuando de la demanda apareciera la necesidad de comprender a terceros que no han sido emplazados, el juez podrá integrar la relación procesal emplazando a otras personas, si de la demanda o de la contestación aparece evidente que la decisión a recaer en el proceso los va a afectar.

ART. 44.—*Plazo de interposición de la demanda*

El plazo para interponer la demanda de amparo prescribe a los sesenta días hábiles de producida la afectación, siempre que el afectado hubiese tenido conocimiento del acto lesivo y se hubiese hallado en posibilidad de interponer la demanda. Si esto no hubiese sido posible, el plazo se computará desde el momento de la remoción del impedimento.

Tratándose del proceso de amparo iniciado contra resolución judicial, el plazo para interponer la demanda se inicia cuando la resolución queda firme. Dicho plazo concluye treinta días hábiles después de la notificación de la resolución que ordena se cumpla lo decidido.

Para el cómputo del plazo se observarán las siguientes reglas:

1) El plazo se computa desde el momento en que se produce la afectación, aun cuando la orden respectiva haya sido dictada con anterioridad.

2) Si la afectación y la orden que la ampara son ejecutadas simultáneamente, el cómputo del plazo se inicia en dicho momento.

3) Si los actos que constituyen la afectación son continuados, el plazo se computa desde la fecha en que haya cesado totalmente su ejecución.

4) La amenaza de ejecución de un acto lesivo no da inicio al cómputo del plazo. Sólo si la afectación se produce se deberá empezar a contar el plazo.

5) Si el agravio consiste en una omisión, el plazo no transcurrirá mientras ella subsista.

6) El plazo comenzará a contarse una vez agotada la vía previa, cuando ella proceda.

ART. 45.—*Agotamiento de las vías previas*

El amparo sólo procede cuando se hayan agotado las vías previas. En caso de duda sobre el agotamiento de la vía previa se preferirá dar trámite a la demanda de amparo.

ART. 46.—*Excepciones al agotamiento de las vías previas*

No será exigible el agotamiento de las vías previas si:

1) Una resolución, que no sea la última en la vía administrativa, es ejecutada antes de vencerse el plazo para que quede consentida;

2) Por el agotamiento de la vía previa la agresión pudiera convertirse en irreparable;

3) La vía previa no se encuentra regulada o ha sido iniciada innecesariamente por el afectado; o

4) No se resuelve la vía previa en los plazos fijados para su resolución.

ART. 47.—*Improcedencia liminar*

Si el Juez al calificar la demanda de amparo considera que ella resulta manifiestamente improcedente, lo declarará así expresando los fundamentos de su decisión. Se podrá rechazar liminarmente una demanda manifiestamente improcedente en los casos previstos por el artículo 5 del presente Código. También podrá hacerlo si la demanda se ha interpuesto en defensa del derecho de rectificación y no se acredita la remisión de una solicitud cursada por conducto notarial u otro fehaciente al director del órgano de comunicación o, a falta de éste, a quien haga sus veces, para que rectifique las afirmaciones consideradas inexactas o agraviantes.

Si la resolución que declara la improcedencia fuese apelada, el Juez pondrá en conocimiento del demandado el recurso interpuesto.

ART. 48.—*Inadmisibilidad*

Si el Juez declara inadmisible la demanda, concederá al demandante tres días para que subsane la omisión o defecto, bajo apercibimiento de archivar el expediente. Esta resolución es apelable.

ART. 49.—*Reconvención, abandono y desistimiento*

En el amparo no procede la reconvención ni el abandono del proceso. Es procedente el desistimiento.

ART. 50.—*Acumulación de procesos y resolución inimpugnable*

Cuando un mismo acto, hecho, omisión o amenaza afecte el interés de varias personas que han ejercido separadamente su derecho de acción, el Juez que hubiese prevenido, a pedido de parte o de oficio, podrá ordenar la acumulación de los procesos de amparo.

La resolución que concede o deniega la acumulación es inimpugnable.

ART. 51.—*Juez Competente y plazo de resolución en Corte*

Son competentes para conocer del proceso de amparo, a elección del demandante, el Juez civil del lugar donde se afectó el derecho, o donde tiene su domicilio el afectado, o donde domicilia el autor de la infracción.

Si la afectación de derechos se origina en una resolución judicial, la demanda se interpondrá ante la Sala Civil de turno de la Corte Superior de Justicia respectiva, la que designará a uno de sus miembros, el cual verificará los hechos referidos al presunto agravio.

La Sala Civil resolverá en un plazo que no excederá de cinco días desde la interposición de la demanda.

*Artículo modificado por la Ley Nº 28946, publicada el 24 de diciembre del 2006, cuyo texto es el siguiente:

"ART. 51.—*Juez Competente y plazo de resolución en Corte*

Es competente para conocer del proceso de amparo, del proceso de *habeas data* y del proceso de cumplimiento el Juez civil o mixto del lugar donde se afectó el derecho, o donde tiene su domicilio principal el afectado, a elección del demandante.

En el proceso de amparo, *habeas data* y en el de cumplimiento no se admitirá la prórroga de la competencia territorial, bajo sanción de nulidad de todo lo actuado.

Promovida la excepción de incompetencia, el Juez le dará el trámite a que se refieren los artículos 10 y 53 de este Código.

De comprobarse malicia o temeridad en la elección del Juez por el demandante, éste será pasible de una multa no menor de 3 URP ni mayor a 10 URP, sin perjuicio de remitir copias al Ministerio Público, para que proceda con arreglo a sus atribuciones.

Si la afectación de derechos se origina en una resolución judicial, la demanda se interpondrá ante la Sala Civil de turno de la Corte Superior de Justicia de la República respectiva, la que designará a uno de sus miembros, el cual verificará los hechos referidos al presunto agravio.

La Sala Civil resolverá en un plazo que no excederá de cinco días desde la interposición de la demanda."

ART. 52.—*Impedimentos*

El Juez deberá abstenerse cuando concurran las causales de impedimento previstas en el Código Procesal Civil. En ningún caso será procedente la recusación.

El Juez que intencionalmente no se abstiene cuando concurre una causal de impedimento, o lo hace cuando no concurre una de ellas, incurre en responsabilidad de naturaleza disciplinaria y penal.

ART. 53.—*Trámite*

En la resolución que admite la demanda, el juez concederá al demandado el plazo de cinco días para que conteste. Dentro de cinco días de contestada la demanda, o de vencido el plazo para hacerlo, el juez expedirá sentencia, salvo que se haya formulado solicitud de informe oral, en cuyo caso el plazo se computará a partir de la fecha de su realización. Si se presentan excepciones, defensas previas o pedidos de nulidad del auto admisorio, el Juez dará traslado al demandante por el plazo de dos días. Con la absolución o vencido el plazo para hacerlo, quedan los autos expeditos para ser sentenciados.

Si el Juez lo considera necesario, realizará las actuaciones que considere indispensables, sin notificación previa a las partes. Inclusive, puede citar a audiencia única a las partes y a sus abogados para realizar los esclarecimientos que estime necesarios. El Juez expedirá sentencia en la misma audiencia o, excepcionalmente, en un plazo que no excederá los cinco días de concluida ésta.

Si considera que la relación procesal tiene un defecto subsanable, concederá un plazo de tres días al demandante para que lo remedie, vencido el cual expedirá sentencia. Si estima que la relación procesal tiene un defecto insubsanable, declarará improcedente la demanda en la sentencia. En los demás casos, expedirá sentencia pronunciándose sobre el mérito.

Los actos efectuados con manifiesto propósito dilatorio, o que se asimilen a cualquiera de los casos previstos en el artículo 112 del Código Procesal Civil, serán sancionados con una multa no menor de diez ni mayor de cincuenta Unidades de Referencia Procesal. Dicha sanción no excluye la responsabilidad civil, penal o administrativa que pudiera derivarse del mismo acto.

*Artículo modificado por la Ley Nº 28946, publicada el 24 de diciembre del 2006, cuyo texto es el siguiente:

"ART. 53.—*Trámite*

En la resolución que admite la demanda, el Juez concederá al demandado el plazo de cinco días para que conteste. Dentro de cinco días de contestada la demanda, o de vencido el plazo para hacerlo, el Juez expedirá sentencia, salvo que se haya formulado solicitud de informe oral, en cuyo caso el plazo se computará a partir de la fecha de su realización. Si se presentan excepciones, defensas previas o pedidos de nulidad del auto admisorio, el Juez dará traslado al demandante por el plazo de dos días; con la absolución o vencido el plazo para hacerlo, dictará un Auto de Saneamiento Procesal en el que se anule lo actuado y se dé por concluido el proceso, en el caso de que se amparen las excepciones de incompetencia, litispendencia, cosa juzgada y caducidad. La apelación de la resolución que ampare una o más de las excepciones propuestas es concedida con efecto suspensivo. La apelación de la resolución que desestima la excepción propuesta es concedida sin efecto suspensivo.

Si el Juez lo considera necesario, realizará las actuaciones que considere indispensables, sin notificación previa a las partes. Inclusive, puede citar a audiencia única a las partes y a sus abogados para realizar los esclarecimientos que estime necesarios.

El Juez expedirá sentencia en la misma audiencia o, excepcionalmente, en un plazo que no excederá los cinco días de concluida ésta.

El Juez en el auto de saneamiento, si considera que la relación procesal tiene un defecto subsanable, concederá un plazo de tres días al demandante para que lo subsane, vencido el cual expedirá una sentencia. En los demás casos, expedirá sentencia pronunciándose sobre el mérito.

Los actos efectuados con manifiesto propósito dilatorio, o que se asimilen a cualquiera de los casos previstos en el artículo 112 del Código Procesal Civil, serán sancionados con una multa no menor de diez ni mayor de cincuenta Unidades de Referencia Procesal. Dicha sanción no excluye la responsabilidad civil, penal o administrativa que pudiera derivarse del mismo acto."

ART. 54.—*Intervención litisconsorcial*

Quien tuviese interés jurídicamente relevante en el resultado de un proceso, puede apersonarse solicitando ser declarado litisconsorte facultativo. Si el Juez admite su incorporación ordenará se le notifique la demanda. Si el proceso estuviera en segundo grado, la solicitud

será dirigida al Juez superior. El litisconsorte facultativo ingresa al proceso en el estado en que éste se encuentre. La resolución que concede o deniega la intervención litisconsorcial es inimpugnable.

ART. 55.—*Contenido de la Sentencia fundada*

La sentencia que declara fundada la demanda de amparo contendrá alguno o algunos de los pronunciamientos siguientes:

1) Identificación del derecho constitucional vulnerado o amenazado;

2) Declaración de nulidad de decisión, acto o resolución que hayan impedido el pleno ejercicio de los derechos constitucionales protegidos con determinación, en su caso, de la extensión de sus efectos;

3) Restitución o restablecimiento del agraviado en el pleno goce de sus derechos constitucionales ordenando que las cosas vuelvan al estado en que se encontraban antes de la violación;

4) Orden y definición precisa de la conducta a cumplir con el fin de hacer efectiva la sentencia.

En todo caso, el Juez establecerá los demás efectos de la sentencia para el caso concreto.

Concordancias: R.ADM. N° 095-2004-P-TC, Reg. Normativo del T.C., Art. 47, Últ. párrafo.

ART. 56.—*Costas y Costos*

Si la sentencia declara fundada la demanda, se impondrán las costas y costos que el Juez establezca a la autoridad *Rectificado por Fe de erratas, funcionario o persona demandada. Si el amparo fuere desestimado por el Juez, éste podrá condenar al demandante al pago de costas y costos cuando estime que incurrió en manifiesta temeridad.

En los procesos constitucionales el Estado sólo puede ser condenado al pago de costos.

En aquello que no esté expresamente establecido en la presente Ley, los costos se regulan por los artículos 410 al 419 del Código Procesal Civil.

ART. 57.—*Apelación*

La sentencia puede ser apelada dentro del tercer día siguiente a su notificación. El expediente será elevado dentro de los tres días siguientes a la notificación de la concesión del recurso.

ART. 58.—*Trámite de la apelación*

El superior concederá tres días al apelante para que exprese agravios. Recibida la expresión de agravios o en su rebeldía, concederá traslado por tres días, fijando día y hora para la vista de la causa, en la misma resolución. Dentro de los tres días siguientes de recibida la notificación, las partes podrán solicitar que sus abogados informen oralmente a la vista de la causa. El superior expedirá sentencia dentro del plazo de cinco días posteriores a la vista de la causa, bajo responsabilidad.

ART. 59.—*Ejecución de Sentencia*

Sin perjuicio de lo establecido en el artículo 22 del presente Código, la sentencia firme que declara fundada la demanda debe ser cumplida dentro de los dos días siguientes de notificada. Tratándose de omisiones, este plazo puede ser duplicado.

Si el obligado no cumpliera dentro del plazo establecido, el Juez se dirigirá al superior del responsable y lo requerirá para que lo haga cumplir y disponga la apertura del procedimiento administrativo contra quien incumplió, cuando corresponda y dentro del mismo plazo. Transcurridos dos días, el Juez ordenará se abra procedimiento administrativo contra el supe-

rior conforme al mandato, cuando corresponda, y adoptará directamente todas las medidas para el cabal cumplimiento del mismo. El Juez podrá sancionar por desobediencia al responsable y al superior hasta que cumplan su mandato, conforme a lo previsto por el artículo 22 de este Código, sin perjuicio de la responsabilidad penal del funcionario.

En todo caso, el Juez establecerá los demás efectos del fallo para el caso concreto, y mantendrá su competencia hasta que esté completamente restablecido el derecho.

Cuando el obligado a cumplir la sentencia sea un funcionario público el Juez puede expedir una sentencia ampliatoria que sustituya la omisión del funcionario y regule la situación injusta conforme al decisorio de la sentencia. Para efectos de una eventual impugnación, ambas sentencias se examinarán unitariamente.

Cuando la sentencia firme contenga una prestación monetaria, el obligado que se encuentre en imposibilidad material de cumplir deberá manifestarlo al Juez quien puede concederle un plazo no mayor a cuatro meses, vencido el cual, serán de aplicación las medidas coercitivas señaladas en el presente artículo.

ART. 60.—*Procedimiento para represión de actos homogéneos*

Si sobreviniera un acto sustancialmente homogéneo al declarado lesivo en un proceso de amparo, podrá ser denunciado por la parte interesada ante el juez de ejecución.

Efectuado el reclamo, el Juez resolverá éste con previo traslado a la otra parte por el plazo de tres días. La resolución es apelable sin efecto suspensivo.

La decisión que declara la homogeneidad amplía el ámbito de protección del amparo, incorporando y ordenando la represión del acto represivo sobreviniente.

TÍTULO IV
Proceso de habeas data

ART. 61.—*Derechos protegidos*

El *habeas data* procede en defensa de los derechos constitucionales reconocidos por los incisos 5) y 6) del artículo 2 de la Constitución. En consecuencia, toda persona puede acudir a dicho proceso para:

1) Acceder a información que obre en poder de cualquier entidad pública, ya se trate de la que generen, produzcan, procesen o posean, incluida la que obra en expedientes terminados o en trámite, estudios, dictámenes, opiniones, datos estadísticos, informes técnicos y cualquier otro documento que la administración pública tenga en su poder, cualquiera que sea la forma de expresión, ya sea gráfica, sonora, visual, electromagnética o que obre en cualquier otro tipo de soporte material.

2) Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales.

ART. 62.—*Requisito especial de la demanda*

Para la procedencia del *habeas data* se requerirá que el demandante previamente haya reclamado, por documento de fecha cierta, el respeto de los derechos a que se refiere el artículo anterior, y que el demandado se haya ratificado en su incumplimiento o no haya contestado dentro de los diez días útiles siguientes a la presentación de la solicitud tratándose del

derecho reconocido por el artículo 2 inciso 5) de la Constitución, o dentro de los dos días si se trata del derecho reconocido por el artículo 2 inciso 6) de la Constitución. Excepcionalmente se podrá prescindir de este requisito cuando su exigencia genere el inminente peligro de sufrir un daño irreparable, el que deberá ser acreditado por el demandante. Aparte de dicho requisito, no será necesario agotar la vía administrativa que pudiera existir.

ART. 63.—*Ejecución Anticipada*

De oficio o a pedido de la parte reclamante y en cualquier etapa del procedimiento y antes de dictar sentencia, el Juez está autorizado para requerir al demandado que posee, administra o maneja el archivo, registro o banco de datos, la remisión de la información concerniente al reclamante; así como solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime conveniente. La resolución deberá contener un plazo máximo de tres días útiles para dar cumplimiento al requerimiento expresado por el Juez.

ART. 64.—*Acumulación*

Tratándose de la protección de datos personales podrán acumularse las pretensiones de acceder y conocer informaciones de una persona, con las de actualizar, rectificar, incluir, suprimir o impedir que se suministren datos o informaciones.

ART. 65.—*Normas aplicables*

El procedimiento de *habeas data* será el mismo que el previsto por el presente Código para el proceso de amparo, salvo la exigencia del patrocinio de abogado que será facultativa en este proceso. El Juez podrá adaptar dicho procedimiento a las circunstancias del caso.

TÍTULO V
PROCESO DE CUMPLIMIENTO

ART. 66.—*Objeto*

Es objeto del proceso de cumplimiento ordenar que el funcionario o autoridad pública renuente:

1) Dé cumplimiento a una norma legal o ejecute un acto administrativo firme; o

2) Se pronuncie expresamente cuando las normas legales le ordenan emitir una resolución administrativa o dictar un reglamento.

ART. 67.—*Legitimación y representación*

Cualquier persona podrá iniciar el proceso de cumplimiento frente a normas con rango de ley y reglamentos. Si el proceso tiene por objeto hacer efectivo el cumplimiento de un acto administrativo, sólo podrá ser interpuesto por la persona a cuyo favor se expidió el acto o quien invoque interés para el cumplimiento del deber omitido.

Tratándose de la defensa de derechos con intereses difusos o colectivos, la legitimación corresponderá a cualquier persona. Asimismo, la Defensoría del Pueblo puede iniciar procesos de cumplimiento.

ART. 68.—*Legitimación pasiva*

La demanda de cumplimiento se dirigirá contra la autoridad o funcionario renuente de la administración pública al que corresponda el cumplimiento de una norma legal o la ejecución de un acto administrativo.

Si el demandado no es la autoridad obligada, aquél deberá informarlo al juez indicando la autoridad a quien corresponde su cumplimiento. En caso de duda, el proceso continuará con las autoridades respecto de las cuales se interpuso la demanda. En todo caso, el juez

deberá emplazar a la autoridad que conforme al ordenamiento jurídico, tenga competencia para cumplir con el deber omitido.

ART. 69.—*Requisito especial de la demanda*

Para la procedencia del proceso de cumplimiento se requerirá que el demandante previamente haya reclamado, por documento de fecha cierta, el cumplimiento del deber legal o administrativo, y que la autoridad se haya ratificado en su incumplimiento o no haya contestado dentro de los diez días útiles siguientes a la presentación de la solicitud. Aparte de dicho requisito, no será necesario agotar la vía administrativa que pudiera existir.

ART. 70.—Causales de Improcedencia

No procede el proceso de cumplimiento:

1) Contra las resoluciones dictadas por el Poder Judicial, Tribunal Constitucional y Jurado Nacional de Elecciones;

2) Contra el Congreso de la República para exigir la aprobación o la insistencia de una ley;

3) Para la protección de derechos que puedan ser garantizados mediante los procesos de amparo, *habeas data* y *habeas corpus*;

4) Cuando se interpone con la exclusiva finalidad de impugnar la validez de un acto administrativo;

5) Cuando se demanda el ejercicio de potestades expresamente calificadas por la ley como discrecionales por parte de una autoridad o funcionario;

6) En los supuestos en los que proceda interponer el proceso competencial;

7) Cuando no se cumplió con el requisito especial de la demanda previsto por el artículo 69 del presente Código; y,

8) Si la demanda se interpuso luego de vencido el plazo de sesenta días contados desde la fecha de recepción de la notificación notarial.

ART. 71.—*Desistimiento de la pretensión*

El desistimiento de la pretensión se admitirá únicamente cuando ésta se refiera a actos administrativos de carácter particular.

ART. 72.—*Contenido de la Sentencia fundada*

La sentencia que declara fundada la demanda se pronunciará preferentemente respecto a:

1) La determinación de la obligación incumplida;

2) La orden y la descripción precisa de la conducta a cumplir;

3) El plazo perentorio para el cumplimiento de lo resuelto, que no podrá exceder de diez días;

4) La orden a la autoridad o funcionario competente de iniciar la investigación del caso para efecto de determinar responsabilidades penales o disciplinarias, cuando la conducta del demandado así lo exija.

Concordancias: R.ADM. N° 095-2004-P-TC, Reg. Normativo del T.C., Art. 47, Últ. párrafo.

ART. 73.—*Ejecución de la Sentencia*

La sentencia firme que ordena el cumplimiento del deber omitido, será cumplida de conformidad con lo previsto por el artículo 22 del presente Código.

ART. 74.—*Normas aplicables*

El procedimiento aplicable a este proceso será el mismo que el previsto por el presente Código para el proceso de amparo, en lo que sea aplicable. El Juez podrá adaptar dicho procedimiento a las circunstancias del caso.

TÍTULO VI
Disposiciones generales de los procesos de acción popular e inconstitucionalidad

ART. 75.—*Finalidad*

Los procesos de acción popular y de inconstitucionalidad tienen por finalidad la defensa de la Constitución frente a infracciones contra su jerarquía normativa. Esta infracción puede ser, directa o indirecta, de carácter total o parcial, y tanto por la forma como por el fondo.

Por contravenir el artículo 106 de la Constitución, se puede demandar la inconstitucionalidad, total o parcial, de un decreto legislativo, decreto de urgencia o ley que no haya sido aprobada como orgánica, si dichas disposiciones hubieren regulado materias reservadas a ley orgánica o impliquen modificación o derogación de una ley aprobada como tal.

ART. 76.—*Procedencia de la demanda de acción popular*

La demanda de acción popular procede contra los reglamentos, normas administrativas y resoluciones de carácter general, cualquiera que sea la autoridad de la que emanen, siempre que infrinjan la Constitución o la ley, o cuando no hayan sido expedidas o publicadas en la forma prescrita por la Constitución o la ley, según el caso.

ART. 77.—*Procedencia de la demanda de inconstitucionalidad*

La demanda de inconstitucionalidad procede contra las normas que tienen rango de ley: leyes, decretos legislativos, decretos de urgencia, tratados que hayan requerido o no la aprobación del Congreso conforme a los artículos 56 y 57 de la Constitución, Reglamento del Congreso, normas regionales de carácter general y ordenanzas municipales.

ART. 78.—*Inconstitucionalidad de normas conexas*

La sentencia que declare la ilegalidad o inconstitucionalidad de la norma impugnada, declarará igualmente la de aquella otra a la que debe extenderse por conexión o consecuencia.

ART. 79.—*Principios de interpretación*

Para apreciar la validez constitucional de las normas el Tribunal Constitucional considerará, además de las normas constitucionales, las leyes que, dentro del marco constitucional, se hayan dictado para determinar la competencia o las atribuciones de los órganos del Estado o el ejercicio de los derechos fundamentales de la persona.

ART. 80.—*Relaciones institucionales con ocasión a los procesos de control de normas*

Los Jueces deben suspender el trámite de los procesos de acción popular sustentados en normas respecto de las cuales se ha planteado demanda de inconstitucionalidad ante el Tribunal, hasta que éste expida resolución definitiva.

ART. 81.—*Efectos de la Sentencia fundada*

Las sentencias fundadas recaídas en el proceso de inconstitucionalidad dejan sin efecto las normas sobre las cuales se pronuncian. Tienen alcances generales y carecen de efectos retroactivos. Se publican íntegramente en el Diario Oficial El Peruano y producen efectos desde el día siguiente de su publicación.

Cuando se declare la inconstitucionalidad de normas tributarias por violación del artículo 74 de la Constitución, el Tribunal debe determinar de manera expresa en la sentencia los efectos de su decisión en el tiempo. Asimismo, resuelve lo pertinente respecto de las situaciones jurídicas producidas mientras estuvo en vigencia.

Las sentencias fundadas recaídas en el proceso de acción popular podrán determinar la nulidad, con efecto retroactivo, de las normas impugnadas. En tal supuesto, la sentencia determinará sus alcances en el tiempo. Tienen efectos generales y se publican en el *Diario Oficial El Peruano*.

ART. 82.—*Cosa juzgada*

Las sentencias del Tribunal Constitucional en los procesos de inconstitucionalidad y las recaídas en los procesos de acción popular que queden firmes tienen autoridad de cosa juzgada, por lo que vinculan a todos los poderes públicos y producen efectos generales desde el día siguiente a la fecha de su publicación.

Tiene la misma autoridad el auto que declara la prescripción de la pretensión en el caso previsto en el inciso 1) del artículo 104.

La declaratoria de inconstitucionalidad o ilegalidad de una norma impugnada por vicios formales no obsta para que ésta sea demandada ulteriormente por razones de fondo, siempre que se interponga dentro del plazo señalado en el presente Código.

ART. 83.—*Efectos de la irretroactividad*

Las sentencias declaratorias de ilegalidad o inconstitucionalidad no conceden derecho a reabrir procesos concluidos en los que se hayan aplicado las normas declaradas inconstitucionales, salvo en las materias previstas en el segundo párrafo del artículo 103 y último párrafo del artículo 74 de la Constitución.

Por la declaración de ilegalidad o inconstitucionalidad de una norma no recobran vigencia las disposiciones legales que ella hubiera derogado.

TÍTULO VII
Proceso de acción popular

ART. 84.—*Legitimación*

La demanda de acción popular puede ser interpuesta por cualquier persona.

ART. 85.—*Competencia*

La demanda de acción popular es de competencia exclusiva del Poder Judicial. Son competentes:

1) La Sala correspondiente, por razón de la materia de la Corte Superior del Distrito Judicial al que pertenece el órgano emisor, cuando la norma objeto de la acción popular es de carácter regional o local; y

2) La Sala correspondiente de la Corte Superior de Lima, en los demás casos.

ART. 86.—Demanda

La demanda escrita contendrá cuando menos, los siguientes datos y anexos:

1) La designación de la Sala ante quien se interpone.

2) El nombre, identidad y domicilio del demandante.

3) La denominación precisa y el domicilio del órgano emisor de la norma objeto del proceso.

4) El petitorio, que comprende la indicación de la norma o normas constitucionales y/o legales que se suponen vulneradas por la que es objeto del proceso.

5) Copia simple de la norma objeto del proceso precisándose el día, mes y año de su publicación.

6) Los fundamentos en que se sustenta la pretensión.

7) La firma del demandante, o de su representante o de su apoderado, y la del abogado.

ART. 87.—*Plazo*

El plazo para interponer la demanda de acción popular prescribe a los cinco años contados desde el día siguiente de publicación de la norma.

ART. 88.—*Admisibilidad e improcedencia*

Interpuesta la demanda, la Sala resuelve su admisión dentro de un plazo no mayor de cinco días desde su presentación. Si declara la inadmisibilidad, precisará el requisito incumplido y el plazo para subsanarlo. Si declara la improcedencia y la decisión fuese apelada, pondrá la resolución en conocimiento del emplazado.

ART. 89.—*Emplazamiento y publicación de la demanda*

Admitida la demanda, la Sala confiere traslado al órgano emisor de la norma objeto del proceso y ordena la publicación del auto admisorio, el cual incluirá una relación sucinta del contenido de la demanda, por una sola vez, en el *Diario Oficial El Peruano* si la demanda se promueve en Lima, o en el medio oficial de publicidad que corresponda si aquella se promueve en otro Distrito Judicial.

Si la norma objeto del proceso ha sido expedida con participación de más de un órgano emisor, se emplazará al de mayor jerarquía. Si se trata de órganos de igual nivel jerárquico, la notificación se dirige al primero que suscribe el texto normativo. En el caso de normas dictadas por el Poder Ejecutivo, el emplazamiento se hará al Ministro que la refrenda; si fuesen varios, al que haya firmado en primer término.

Si el órgano emisor ha dejado de operar, corresponde notificar al órgano que asumió sus funciones.

ART. 90.—*Requerimiento de antecedentes*

La Sala puede, de oficio, ordenar en el auto admisorio que el órgano remita el expediente conteniendo los informes y documentos que dieron origen a la norma objeto del proceso, dentro de un plazo no mayor de diez días, contado desde la notificación de dicho auto, bajo responsabilidad. La Sala dispondrá las medidas de reserva pertinentes para los expedientes y las normas que así lo requieran.

ART. 91.—*Contestación de la demanda*

La contestación deberá cumplir con los mismos requisitos de la demanda, en lo que corresponda. El plazo para contestar la demanda es de diez días.

ART. 92.—*Vista de la Causa*

Practicados los actos procesales señalados en los artículos anteriores, la Sala fijará día y hora para la vista de la causa, la que ocurrirá dentro de los diez días posteriores a la contestación de la demanda o de vencido el plazo para hacerlo.

A la vista de la causa, los abogados pueden informar oralmente. La Sala expedirá sentencia dentro de los diez días siguientes a la vista.

ART. 93.—*Apelación y trámite*

Contra la sentencia procede recurso de apelación el cual contendrá la fundamentación del error, dentro de los cinco días siguientes a su notificación. Recibidos los autos, la Sala Constitucional y Social de la Corte Suprema dará traslado del recurso concediendo cinco días para su absolución y fijando día y hora para la vista de la causa, en la misma resolución. Dentro de los tres días siguientes de recibida la notificación las partes podrán solicitar que sus abogados informen oralmente a la vista de la causa.

ART. 94.—*Medida Cautelar*

Procede solicitar medida cautelar una vez expedida sentencia estimatoria de primer grado. El contenido cautelar está limitado a la suspensión de la eficacia de la norma considerada vulneratoria por el referido pronunciamiento.

ART. 95.—*Consulta*

Si la sentencia que declara fundada la demanda no es apelada, los autos se elevarán en consulta a la Sala Constitucional y Social de la Corte Suprema. La consulta se absolverá sin trámite y en un plazo no mayor de cinco días desde que es recibido el expediente.

ART. 96.—*Sentencia*

La sentencia expedida dentro de los diez días posteriores a la vista de la causa será publicada en el mismo medio de comunicación en el que se publicó el auto admisorio.

Dicha publicación no sustituye la notificación de las partes. En ningún caso procede el recurso de casación.

ART. 97.—*Costos*

Si la sentencia declara fundada la demanda se impondrán los costos que el juez establezca, los cuales serán asumidos por el Estado. Si la demanda fuere desestimada por el Juez, éste podrá condenar al demandante al pago de los costos cuando estime que incurrió en manifiesta temeridad. En todo lo no previsto en materia de costos, será de aplicación supletoria lo previsto en el Código Procesal Civil.

TÍTULO VIII
Proceso de inconstitucionalidad

ART. 98.—*Competencia y Legitimación*

La demanda de inconstitucionalidad se interpone ante el Tribunal Constitucional y sólo puede ser presentada por los órganos y sujetos indicados en el artículo 203 de la Constitución.

ART. 99.—*Representación Procesal Legal*

Para interponer una demanda de inconstitucionalidad el Presidente de la República requiere del voto aprobatorio del Consejo de Ministros. Concedida la aprobación, designa a uno de sus Ministros para que presente la demanda de inconstitucionalidad y lo represente en el proceso. El Ministro designado puede delegar su representación en un Procurador Público.

El Fiscal de la Nación y el Defensor del Pueblo interponen directamente la demanda.

Pueden actuar en el proceso mediante apoderado.

Los Congresistas actúan en el proceso mediante apoderado nombrado al efecto.

Los ciudadanos referidos en el inciso 5) del artículo 203 de la Constitución deben actuar con patrocinio de letrado y conferir su representación a uno solo de ellos.

Los Presidentes de Región con acuerdo del Consejo de Coordinación Regional o los Alcaldes Provinciales con acuerdo de su Concejo, actúan en el proceso por sí o mediante apoderado y con patrocinio de letrado.

Para interponer la demanda, previo acuerdo de su Junta Directiva, los Colegios Profesionales deben actuar con el patrocinio de abogado y conferir representación a su Decano.

El órgano demandado se apersona en el proceso y formula obligatoriamente su alegato en defensa de la norma impugnada, por medio de apoderado nombrado especialmente para el efecto.

ART. 100.—*Plazo prescriptorio*

La demanda de inconstitucionalidad de una norma debe interponerse dentro del plazo de seis años contado a partir de su publicación, salvo el caso de los tratados en que el plazo es de seis meses. Vencido los plazos indicados, prescribe la pretensión, sin perjuicio de lo dispuesto por el artículo 51 y por el segundo párrafo del artículo 138 de la Constitución.

ART. 101.—*Demanda*

La demanda escrita contendrá, cuando menos, los siguientes datos y anexos:

1) La identidad de los órganos o personas que interponen la demanda y su domicilio legal y procesal.

2) La indicación de la norma que se impugna en forma precisa.

3) Los fundamentos en que se sustenta la pretensión.

4) La relación numerada de los documentos que se acompañan.

5) La designación del apoderado si lo hubiere.

6) Copia simple de la norma objeto de la demanda, precisándose el día, mes y año de su publicación.

ART. 102.—*Anexos de la Demanda*

A la demanda se acompañan, en su caso:

1) Certificación del acuerdo adoptado en Consejo de Ministros, cuando el demandante sea el Presidente de la República;

2) Certificación de las firmas correspondientes por el Oficial Mayor del Congreso si los actores son el 25% del número legal de Congresistas;

3) Certificación por el Jurado Nacional de Elecciones, en los formatos que proporcione el Tribunal, y según el caso, si los actores son cinco mil ciudadanos o el uno por ciento de los ciudadanos del respectivo ámbito territorial, conforme al artículo 203 inciso 5) de la Constitución;

4) Certificación del acuerdo adoptado en la Junta Directiva del respectivo Colegio Profesional; o

5) Certificación del acuerdo adoptado en el Consejo de Coordinación Regional o en el Concejo Provincial, cuando el actor sea Presidente de Región o Alcalde Provincial, respectivamente.

ART. 103.—*Inadmisibilidad de la Demanda*

Interpuesta la demanda, el Tribunal resuelve su admisión dentro de un plazo que no puede exceder de diez días.

El Tribunal resuelve la inadmisibilidad de la demanda, si concurre alguno de los siguientes supuestos:

1) Que en la demanda se hubiera omitido alguno de los requisitos previstos en el artículo 101; o

2) Que no se acompañen los anexos a que se refiere el artículo 102.

El Tribunal concederá un plazo no mayor de cinco días si el requisito omitido es susceptible de ser subsanado. Si vencido el plazo no se subsana el defecto de inadmisibilidad, el Tribunal, en resolución debidamente motivada e inimpugnable, declara la improcedencia de la demanda y la conclusión del proceso.

ART. 104.—*Improcedencia liminar de la demanda*

El Tribunal declarará improcedente la demanda cuando concurre alguno de los siguientes supuestos:

1) Cuando la demanda se haya interpuesto vencido el plazo previsto en el artículo 100;

2) Cuando el Tribunal hubiere desestimado una demanda de inconstitucionalidad sustancialmente igual en cuanto al fondo; o

3) Cuando el Tribunal carezca de competencia para conocer la norma impugnada.

En estos casos, el Tribunal en resolución debidamente motivada e inimpugnable declara la improcedencia de la demanda.

ART. 105.—*Improcedencia de Medidas Cautelares*

En el proceso de inconstitucionalidad no se admiten medidas cautelares.

ART. 106.—*Efecto de la Admisión e Impulso de oficio*

Admitida la demanda, y en atención al interés público de la pretensión discutida, el Tribunal Constitucional impulsará el proceso de oficio con prescindencia de la actividad o interés de las partes.

El proceso sólo termina por sentencia.

ART. 107.—*Tramitación*

El auto admisorio concede a la parte demandada el plazo de treinta días para contestar la demanda. El Tribunal emplaza con la demanda:

1) Al Congreso o a la Comisión Permanente, en caso de que el Congreso no se encuentre en funciones, si se trata de Leyes y Reglamento del Congreso.

2) Al Poder Ejecutivo, si la norma impugnada es un Decreto Legislativo o Decreto de Urgencia.

3) Al Congreso, o a la Comisión Permanente y al Poder Ejecutivo, si se trata de Tratados Internacionales.

4) A los órganos correspondientes si la norma impugnada es de carácter regional o municipal.

Con su contestación, o vencido el plazo sin que ella ocurra, el Tribunal tendrá por contestada la demanda o declarará la rebeldía del emplazado, respectivamente. En la misma resolución el Tribunal señala fecha para la vista de la causa dentro de los diez días útiles siguientes. Las partes pueden solicitar que sus abogados informen oralmente.

ART. 108.—*Plazo para dictar sentencia*

El Tribunal dicta sentencia dentro de los treinta días posteriores de producida la vista de la causa.

TÍTULO IX
Proceso competencial

ART. 109.—*Legitimación y representación*

El Tribunal Constitucional conoce de los conflictos que se susciten sobre las competencias o atribuciones asignadas directamente por la Constitución o las leyes orgánicas que delimiten los ámbitos propios de los poderes del Estado, los órganos constitucionales, los gobiernos regionales o municipales, y que opongan:

1) Al Poder Ejecutivo con uno o más gobiernos regionales o municipales;

2) A dos o más gobiernos regionales, municipales o de ellos entre sí; o

3) A los poderes del Estado entre sí o con cualquiera de los demás órganos constitucionales, o a éstos entre sí.

Los poderes o entidades estatales en conflicto actuarán en el proceso a través de sus titulares. Tratándose de entidades de composición colegiada, la decisión requerirá contar con la aprobación del respectivo pleno.

ART. 110.—*Pretensión*

El conflicto se produce cuando alguno de los poderes o entidades estatales a que se refiere el artículo anterior adopta decisiones o rehuye deliberadamente actuaciones, afectando competencias o atribuciones que la Constitución y las leyes orgánicas confieren a otro.

Si el conflicto versare sobre una competencia o atribución expresada en una norma con rango de ley, el Tribunal declara que la vía adecuada es el proceso de inconstitucionalidad.

ART. 111.—*Medida Cautelar*

El demandante puede solicitar al Tribunal la suspensión de la disposición, resolución o acto objeto de conflicto. Cuando se promueva un conflicto constitucional con motivo de una disposición, resolución o acto cuya impugnación estuviese pendiente ante cualquier juez o tribunal, éste podrá suspender el procedimiento hasta la resolución del Tribunal Constitucional.

ART. 112.—*Admisibilidad y procedencia*

Si el Tribunal Constitucional estima que existe materia de conflicto cuya resolución sea de su competencia, declara admisible la demanda y dispone los emplazamientos correspondientes.

El procedimiento se sujeta, en cuanto sea aplicable, a las disposiciones que regulan el proceso de inconstitucionalidad.

El Tribunal puede solicitar a las partes las informaciones, aclaraciones o precisiones que juzgue necesarias para su decisión. En todo caso, debe resolver dentro de los sesenta días hábiles desde que se interpuso la demanda.

ART. 113.—*Efectos de las Sentencias*

La sentencia del Tribunal vincula a los poderes públicos y tiene plenos efectos frente a todos. Determina los poderes o entes estatales a que corresponden las competencias o atribuciones controvertidas y anula las disposiciones, resoluciones o actos viciados de incompetencia. Asimismo resuelve, en su caso, lo que procediere sobre las situaciones jurídicas producidas sobre la base de tales actos administrativos.

Cuando se hubiera promovido conflicto negativo de competencias o atribuciones, la sentencia, además de determinar su titularidad, puede señalar, en su caso, un plazo dentro del cual el poder del Estado o el ente estatal de que se trate debe ejercerlas.

TÍTULO X
Jurisdicción internacional

ART. 114.—*Organismos internacionales competentes*

Para los efectos de lo establecido en el artículo 205 de la Constitución, los organismos internacionales a los que puede recurrir cualquier persona que se considere lesionada en los derechos reconocidos por la Constitución, o los tratados sobre derechos humanos ratificados por el Estado peruano, son: el Comité de Derechos Humanos de las Naciones Unidas, la Comisión Interamericana de Derechos Humanos de la Organización de Estados Americanos y aquellos otros que se constituyan en el futuro y que sean aprobados por tratados que obliguen al Perú.

ART. 115.—*Ejecución de resoluciones*

Las resoluciones de los organismos jurisdiccionales a cuya competencia se haya sometido expresamente el Estado peruano no requieren, para su validez y eficacia, de reconocimiento, revisión, ni examen previo alguno. Dichas resoluciones son comunicadas por el Ministerio de Relaciones Exteriores al Presidente del Poder Judicial, quien a su vez, las remite al tribunal

donde se agotó la jurisdicción interna y dispone su ejecución por el juez competente, de conformidad con lo previsto por la Ley N° 27775, que regula el procedimiento de ejecución de sentencias emitidas por tribunales supranacionales.

ART. 116.—*Obligación de proporcionar documentos y antecedentes*

La Corte Suprema de Justicia de la República y el Tribunal Constitucional deberán remitir a los organismos a que se refiere el artículo 114, la legislación, las resoluciones y demás documentos actuados en el proceso o los procesos que originaron la petición, así como todo otro elemento que a juicio del organismo internacional fuere necesario para su ilustración o para mejor resolver el asunto sometido a su competencia.

TÍTULO XI
Disposiciones generales aplicables a los procedimientos ante el Tribunal Constitucional

ART. 117.—*Acumulación de procesos*

El Tribunal Constitucional puede, en cualquier momento, disponer la acumulación de procesos cuando éstos sean conexos.

ART. 118.—*Numeración de las sentencias*

Las sentencias dictadas por el Tribunal Constitucional se enumeran en forma correlativa y anualmente.

ART. 119.—*Solicitud de información*

El Tribunal puede solicitar a los poderes del Estado y a los órganos de la Administración Pública todos los informes y documentos que considere necesarios para la resolución de los procesos de su competencia. En tal caso, el Tribunal habilita un plazo para que las partes conozcan de ellos y puedan alegar lo que convenga a su derecho.

El Tribunal dispone las medidas necesarias para preservar el secreto que legalmente afecta a determinada documentación, y el que, por decisión motivada, acuerda para su actuación.

Concordancias: R.ADM. N° 095-2004-P-TC, Reg. Normativo del T.C., Art. 20, Num. 2

ART. 120.—*Subsanación de vicios en el procedimiento*

El Tribunal, antes de pronunciar sentencia, de oficio o a instancia de parte, debe subsanar cualquier vicio de procedimiento en que se haya incurrido.

ART. 121.—*Carácter inimpugnable de las sentencias del Tribunal Constitucional*

Contra las sentencias del Tribunal Constitucional no cabe impugnación alguna. En el plazo de dos días a contar desde su notificación o publicación tratándose de las resoluciones recaídas en los procesos de inconstitucionalidad, el Tribunal, de oficio o a instancia de parte, puede aclarar algún concepto o subsanar cualquier error material u omisión en que hubiese incurrido.

Estas resoluciones deben expedirse, sin más trámite, al segundo día de formulada la petición.

Contra los decretos y autos que dicte el Tribunal, sólo procede, en su caso, el recurso de reposición ante el propio Tribunal. El recurso puede interponerse en el plazo de tres días a contar desde su notificación. Se resuelve en los dos días siguientes.

Lo anterior no afecta el derecho a recurrir a los tribunales u organismos internacionales constituidos según tratados de los que el Perú es parte.

TÍTULO XII
Disposiciones finales

PRIMERA.—*Denominaciones empleadas*

Para los efectos de este Código, se adoptarán las siguientes denominaciones:

1) Proceso de *habeas corpus*, a la acción de *habeas corpus*;
2) Proceso de amparo, a la acción de amparo;
3) Proceso de *habeas data*, a la acción de *habeas data*;
4) Proceso de inconstitucionalidad, a la acción de inconstitucionalidad;
5) Proceso de acción popular, a la acción popular;
6) Proceso de cumplimiento, a la acción de cumplimiento; y,
7) Proceso competencial, a los conflictos de competencias o atribuciones.

SEGUNDA.—*Vigencia de normas*

Las normas procesales previstas por el presente Código son de aplicación inmediata, incluso a los procesos en trámite. Sin embargo, continuarán rigiéndose por la norma anterior: las reglas de competencia, los medios impugnatorios interpuestos, los actos procesales con principio de ejecución y los plazos que hubieran empezado.

TERCERA.—*Jueces Especializados*

Los procesos de competencia del Poder Judicial a que se refiere el presente Código se iniciarán ante los jueces especializados que correspondan en aquellos distritos judiciales que cuenten con ellos, con la sola excepción del proceso de *habeas corpus* que podrá iniciarse ante cualquier juez penal.

CUARTA.—*Publicación de sentencias*

Las sentencias finales y las resoluciones aclaratoria de las mismas, recaídas en los procesos constitucionales deben remitirse, dentro de las cuarentiocho horas siguientes a la fecha de su expedición, al *Diario Oficial El Peruano* para su publicación gratuita, dentro de los diez días siguientes a su remisión. La publicación debe contener la sentencia y las piezas del expediente que sean necesarias para comprender el derecho invocado y las razones que tuvo el Juez para conceder o denegar la pretensión.

Las sentencias recaídas en el proceso de inconstitucionalidad, el proceso competencial y la acción popular se publican en el diario oficial dentro de los tres días siguientes al de la recepción de la transcripción remitida por el órgano correspondiente. En su defecto, el Presidente del Tribunal ordena que se publique en uno de los diarios de mayor circulación nacional, sin perjuicio de las responsabilidades a que hubiere lugar.

Cuando las sentencias versan sobre normas regionales o municipales, además de la publicación a que se refiere el párrafo anterior, el Tribunal ordena la publicación en el diario donde se publican los avisos judiciales de la respectiva circunscripción. En lugares donde no exista diario que se publique los avisos judiciales, la sentencia se da a conocer, además de su publicación en el diario oficial o de circulación nacional, mediante carteles fijados en lugares públicos.

QUINTA.—*Exoneración de tasas judiciales*

Los procesos constitucionales se encuentran exonerados del pago de tasas judiciales.

SEXTA.—*Enseñanza de los derechos y de los procesos constitucionales*

En todos los centros de enseñanza, de cualquier nivel, civiles, o militares, se impartirán cursos obligatorios sobre derechos fundamentales y procesos constitucionales.

Compete promover y supervisar esta tarea al Ministerio de Educación; a la Asamblea Nacional de Rectores, y a los Ministerios de Defensa y del Interior. El Ministerio de Justicia queda encargado de la labor de publicación y difusión de la Constitución y textos básicos conexos. Queda encargado igualmente de editar, periódicamente, una versión fidedigna de todas las constituciones históricas del Perú y de la vigente Constitución. Adicionalmente editará y patrocinará estudios, publicaciones, textos, jurisprudencia y legislación Constitucional.

SÉPTIMA.—*Gaceta Constitucional*

La Gaceta Constitucional es el órgano oficial del Tribunal Constitucional y será editada periódicamente, sin perjuicio de otras compilaciones oficiales y de la publicación electrónica de su jurisprudencia. En ella el Tribunal Constitucional dará cuenta de sus actividades, publicará los documentos relacionados con su marcha institucional, así como las resoluciones finales de los procesos constitucionales de su competencia. Esta publicación se hace con independencia de la que efectúe obligatoriamente el *Diario Oficial El Peruano*.

TÍTULO XIII
Disposiciones transitorias y derogatorias

PRIMERA.—*Normas derogadas*

Quedan derogadas:

1) La Ley Nº 23506, Ley de *Habeas Corpus* y Amparo.

2) La Ley Nº 25398, Ley complementaria de la Ley de *Habeas Corpus* y Amparo.

3) La Ley Nº 24968, Ley Procesal de la Acción Popular.

4) La Ley Nº 25011, que modifica parcialmente la Ley Nº 23506.

5) La Ley Nº 25315, que modifica parcialmente la Ley Nº 23506.

6) El Decreto Ley Nº 25433, que modifica la Ley Nº 23506 y la Ley Nº 24968.

7) La Ley Nº 26248, que modifica parcialmente la Ley Nº 23506.

8) La Ley Nº 26301, Ley de *Habeas Data* y Acción de Cumplimiento.

9) Los artículos 20 al 63, con excepción del artículo 58, así como la primera y segunda disposición general de la Ley Nº 26435, Ley Orgánica del Tribunal Constitucional.

10) La Ley Nº 26545, que modifica parcialmente los procesos de *habeas data* y acción de cumplimiento.

11) El Decreto Legislativo Nº 824, que modifica parcialmente la Ley Nº 23506. (*)

12) La Ley Nº 27053, que modifica parcialmente la Ley Nº 23506.

13) La Ley Nº 27235, que modifica parcialmente la Ley Nº 23506.

14) La Ley Nº 27959, que modifica parcialmente la Ley Nº 23506.

15) Todas las disposiciones que se opongan al presente Código.

*De conformidad con el Artículo Único de la Ley N° 28400, publicada el 27-11-2004, se precisa que el presente numeral, deroga únicamente el artículo 17 del Decreto Legislativo Nº 824 - Ley de Lucha contra el Tráfico Ilícito de Drogas, sin perjuicio de la vigencia de todos los demás artículos del referido Decreto Legislativo Nº 824 y sus normas modificatorias.

SEGUNDA.—*Vigencia del Código*

El presente Código entra en vigencia a los seis meses de su publicación en el *Diario Oficial El Peruano*.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los siete días del mes de mayo de dos mil cuatro.

Henry Pease García.—Presidente del Congreso de la República.—*Marciano Rengifo Ruiz*.—Primer Vicepresidente del Congreso de la República.

Al señor Presidente Constitucional de la República
Por tanto:
Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los veintiocho días del mes de mayo del año dos mil cuatro.

ALEJANDRO TOLEDO, Presidente Constitucional de la República

CARLOS FERRERO, Presidente del Consejo de Ministros

BALDO KRESALJA ROSELLÓ, Ministro de Justicia *Rectificado por Fe de erratas

Modifican artículo 1° del Decreto Supremo N° 043-2005-PCM

DECRETO SUPREMO N° 060-2006-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, de acuerdo con el artículo 109° del Código Procesal Constitucional, el Tribunal Constitucional conoce de los conflictos que se susciten sobre las competencias o atribuciones asignadas directamente por la Constitución o las leyes orgánicas, que delimiten los ámbitos propios de los poderes del Estado, los órganos constitucionales, los gobiernos regionales o municipales y que opongan, entre otros, a los poderes del Estado entre sí o con cualquiera de los demás órganos constitucionales, o a éstos entre sí;

Que, el mismo dispositivo establece para el caso de los poderes o entidades estatales en conflicto, que éstos actuarán a través de sus titulares;

Que, no existe normatividad que establezca el procedimiento previo a la interposición de un proceso competencial por parte del Poder Ejecutivo contra otro Poder del Estado o demás órganos constitucionales al amparo del articulo 109° del Código Procesal Constitucional, antes citado;

Que, mediante el artículo 1° del Decreto Supremo N° 043-2005-PCM, se estableció el trámite previo a la interposición de procesos constitucionales de inconstitucionalidad y competencial, por parte de los sectores del Gobierno Nacional, contra normas, y actos emitidos por Gobiernos Regionales y Locales; trámite que es necesario ampliar a fin de que abarque de modo general el procedimiento que debe seguirse para la interposición de un proceso competencial por parte del Poder Ejecutivo contra otro Poder del Estado y demás órganos constitucionales, al amparo del numeral 3 del artículo 10911 del Código Procesal Constitucional;

De conformidad con lo establecido en el artículo 118° numeral 8) de la Constitución Política del Perú, artículo 3° numeral 2) del Decreto Legislativo N° 560 - Ley del Poder Ejecutivo, el artículo 2° del Decreto Ley N° 17537 - Ley que crea el Consejo de Defensa Judicial del Estado y su Reglamento aprobado por Decreto Supremo N° 0022000-JUS;

Con el voto aprobatorio del Consejo de Ministros;

DECRETA:

ART. 1°.—*Modificación del artículo 1° del Decreto Supremo N° 043-2005-PCM*

Modificase el artículo 1° del Decreto Supremo N° 043-2005-PCM, el mismo que queda redactado en los siguientes términos:

"Para la interposición de procesos constitucionales de inconstitucionalidad y competencial por parte de los sectores del Gobierno Nacional, contra normas y actos emitidos por Gobiernos Regionales y Locales, así como para la interposición de procesos competencia les por parte del Poder Ejecutivo contra normas y actos emitidos por otro Poder del Estado o demás órganos constitucionales, se deberá cumplir el siguiente procedimiento:

1.1. El Sector del Gobierno Nacional que considere afectada una competencia o lo dispuesto por el ordenamiento jurídico por una norma aprobada por un Gobierno Regional o Local, y el Sector del Poder Ejecutivo cuya competencia se vea afectada por una norma o acto emanado de otro Poder del Estado u órgano constituciol1al, deberán emitir los informes técnico y legal acerca de la vulneración que contenga la norma o acto, según sea el caso.

1.2. Los informes técnico y legal deberán ser elevados al Ministro del Sector correspondiente para su evaluación.

1.3. El Ministro del Sector, previa evaluación de los informes y si considera viable la interposición del proceso constitucional, deberá sustentarlo ante el Consejo de Ministros y proponer se interponga la demanda correspondiente. Concedida la aprobación mediante voto aprobatorio del Consejo de Ministros, el Presidente de la República designa a uno de sus Ministros o al Ministro del Sector afectado por la norma o acto, para que presente la demanda y lo represente en el proceso.

1.4. El Ministro designado, mediante Resolución Ministerial, puede delegar su representación en el Procurador Público de su Sector o en un Procurador Público *Ad Hoc*, para que ejerza la defensa de los intereses del Poder Ejecutivo en el proceso competencial".

ART. 2°.—El presente Decreto Supremo será refrendado por el Presidente del Consejo de Ministros y por el Ministro de Justicia.

Dado en la Casa de Gobierno, en Lima, a los veintiún días del mes de setiembre del año dos mil seis.

Alan García Pérez.—Presidente Constitucional de la República.—*Jorge del Castillo Gálvez*.—Presidente del Consejo de Ministros.—*María Zavala Valladares*.—Ministra de Justicia.

1612 blanca

Bibliografía

Bibliografía general

AAVV (obra dirigida por FERRER MAC GREGOR, Eduardo), *Derecho Procesal Constitucional*, tomos I a IV, Porrúa, México, varias ediciones.

AAVV (obra dirigida por MANILI, Pablo L.), *Derecho Procesal Constitucional*, tomos I a III, La Ley, Buenos Aires, 2010.

AAVV (obra dirigida por BAZÁN, Víctor), *Derecho Procesal Constitucional, americano y europeo*, tomos I y II, Abeledo Perrot, Buenos Aires, 2009.

FALCÓN, Enrique M., *Derecho Procesal Constitucional*, tomo I (II y III en prensa), Rubinzal Culzoni, Buenos Aires, 2010.

Revista Iberoamericana de Derecho Procesal Constitucional, números 1 a 13, Porrúa, México.

"Biblioteca Porrúa de Derecho Procesal Constitucional", 32 libros aparecidos.

Bibliografía de la obra

ABAD YUPANQUI, Samuel B., DANÓS ORDOÑEZ, Jorge, EGUIGUREN PRAELI, Francisco J., GARCÍA BELAÚNDE, Domingo, MONROY GÁLVEZ, Juan, ORÉ GUARDIA, Arsenio, *Código Procesal Constitucional*, Tribunal Constitucional del Perú-Centro de Estudios Constitucionales, Lima, 2008 (3ª ed.).

ABAD YUPANQUI, Samuel B., "El proceso constitucional de amparo en el Perú: un análisis desde la teoría general del proceso", *Boletín Mexicano de Derecho Comparado*, nº 85, enero-abril 1986.

ABRAMOVICH, Víctor y COURTIS, Christian, Los derechos sociales como derechos exigibles. Madrid, Trotta, 2002.

ALBANESE, Susana, *Garantías Judiciales*, Ediar, Buenos Aires, 2000.

——, "La internacionalización del derecho constitucional y la constitucionalización del derecho internacional", en *El control de convencionalidad*, Albanese, Susana (coordinadora), Ediar, Buenos Aires, 2008.

ALDASORO, Héctor, *El derecho procesal constitucional mexicano*, conferencia en el Ilustre Colegio Nacional de México, passim

ALEXY, Robert, *El concepto y la validez del Derecho*, trad. de J. M. Seña, Gedisa, Barcelona, 1994.

——, *Teoría de los derechos fundamentales*, trad. de Ernesto Garzón, Centro de Estudios Constitucionales, Madrid, 1993.

——, *Tres escritos sobre los derechos fundamentales y la teoría de los principios*, Universidad Externado de Colombia (Serie de teoría jurídica y filosofía de derecho), nº 28, Bogotá, 2003.

ALMAGRO NOSETE, José, *Constitución y Proceso*, Bosch, Barcelona, 1984.

——, "El libre derecho a la jurisdicción", *Revista de la Facultad de Derecho* de la Universidad de Madrid, 1970, p. 95 y ss.

ALMAGRO NOSETE. José, TOMÉ PAULE, José, *Instituciones de Derecho Procesal*, tomo I (Proceso Civil, 1), Trivium, Madrid, 1993.

ALPA, Giuseppe, *Compendio del nuovo Diritto Privato*, UTET, Torino, 1985.

ALSINA, Hugo, "Naturaleza jurídica de la acción", *Revista de Derecho Procesal*, 1952-I, p. 189.

——, *Tratado teórico práctico de Derecho Procesal Civil y Comercial*, Tomos I a VI, Ediar, Buenos Aires, 1963.

ALVARADO VELLOSO, Adolfo, *El juez: sus deberes y facultades*, Depalma, Buenos Aires, 1982.

——, *Introducción al estudio del Derecho Procesal*, tomo I, Rubinzal Culzoni, Santa Fe, 1989.

ALVARADO VELLOSO, Adolfo,"La imparcialidad judicial y la función del juez en el proceso civil", en *Proceso Civil. Hacia una nueva justicia civil*", AAVV, coordinada por De la Oliva Santos, Andrés y Palomo Vélez, Diego Iván, Editorial Jurídica de Chile, Santiago, 2007, p. 286

ALVEAR, CAROS Salmón, "Régimen procesal del *habeas data* en Ecuador", *Revista Jurídica de de Jurisprudencia, Ciencias Sociales y Políticas*, Universidad Católica de Santiago de Guayaquil, versión online.

ARAGÓN REYES, Manuel, *Constitución, democracia y control*, Porrúa-UNAM, México, 2002.

——, "El juez ordinario entre legalidad y constitucionalidad", en la obra colectiva *Jueces y derecho. Problemas contemporáneos*, compiladores Miguel Carbonell, Héctor Fix Fierro y Rodolfo Vázquez, UNAM-Porrúa, México, 2004, pp. 151 y ss.

ARANGUREN, Beatriz E., *Procesos urgentes: medidas autosatisfactivas*, LL Litoral 2006 (junio), 555.

ARIAS GRILLO, Rodrigo, "La actividad cautelar en los procesos constitucionales de protección de derechos fundamentales, control de constitucionalidad y conflictos de competencia, con especial referencia al ordenamiento jurídico costarricense", en *Revista de Ciencias Jurídicas* nº 116, mayo-agosto, 2008, p. 110.

ARIÑO ORTIZ, Gaspar, *Teoría del equivalente económico en los contratos administrativos, Instituto de Estudios Administrativos*, Madrid, 1968.

ASÍS ROIG, Rafael de, *Jueces y Normas (La decisión judicial desde el Ordenamiento)*, Marcial Pons, Madrid, 1995.

ASTUDILLO REYES, César I, "La Justicia Constitucional en México. Presupuestos, sistemas y problemas"*, Boletín Mexicano de Derecho Comparado* nº 115 (2006), pp. 23 y ss.

——, "Doce tesis en torno al derecho procesal constitucional", en *La ciencia del derecho procesal constitucional. Estudios en homenaje a Héctor Fix Zamudio*, tomo I *(Teoría General del derecho procesal constitucional)*, cit., p. 260.

ATIENZA RODRÍGUEZ, Manuel, "Sobre lo razonable en el derecho", en *Revista Española de Derecho Constitucional*, nº 27 (septiembre/diciembre 1989).

ÁVALOS DÍAZ, Sofía Verónica, *La inconstitucionalidad por omisión legislativa. Su tutela en el derecho mexicano*, cfr. http://www.scjn.gob.mx/SiteCollectionDocuments/ PortalSCJN/RecJur/ Becarios/pdf/lic-Sofia-Veronica-Avalos-Diaz.pdf

AYALA CORAO, Carlos, *Del amparo constitucional al amparo interamericano como institutos para la protección de los derechos humanos*, editorial Jurídica Venezolana, Instituto Interamericano de Derechos Humanos, Caracas / San José de Costa Rica, 1998.

"La Justicia Constitucional en Venezuela", en *Ley Orgánica sobre derechos y garantías constitucionales*, Caracas, 1988.

AZNAR GÓMEZ, Hugo, "Intimidad e información en la sociedad contemporánea", en *Sobre la intimidad*, Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

BACARIA MARTRUS, Jordi, *El secreto estadístico* (contenido jurídico), Informática y Derecho nº 6/7, UNED, Mérida, 1994.

BADENI, Gregorio, "El caso 'Simón' y la supremacía constitucional, suplemento de Jurisprudencia Penal y Procesal Penal", *La Ley* del 29 de Julio de 2005, pp. 9 y ss.

BARBOSA MOREIRA, José Carlos, "La legitimación para la defensa de los intereses difusos en el derecho brasileño", en *Revista Jus*, nº. 34 p. 61.

BARRA, Rodolfo C., "La acción de amparo en la Constitución reforma: la legitimación para accionar", *La Ley*, 1994-E, 1087 y ss.

BARRANCOS Y VEDIA, Fernando N., *Recurso Extraordinario y gravedad institucional*, Abeledo Perrot, Buenos Aires, 1969.

BARRIOS DE ANGELIS, Dante, *Introducción al estudio del proceso*, Depalma, Buenos Aires, 1983.

BARRIOS GONZÁLEZ, Boris, *Derecho Procesal Constitucional*, Ancón, Panamá, 1999 2ª ed.

BARTOLOMÉ Clavero, *Codificación y Constitución: paradigmas de un binomio (quaderni fiorentini per la storia del pensiero giuridico moderno)*, Firenze, Italia, 1989.

BASTERRA, Marcela I, *Habeas data: derechos tutelados, Doctrina Judicial*, 1993-3, pp. 77 y ss.

——, La "opinión política" o la "idea política" es un dato sensible. La "afiliación partidaria" no, *La Ley* del 4 de mayo de 2005, p. 1.

——, *Protección de datos personales*, Ediar – Instituto de Investigaciones Jurídicas de la UNAM, Buenos Aires, 2008.

BAUM CORTE, Erica, "La propiedad de la información", *Revista de Derecho Informático*, versión on line.

BAZÁN, Víctor, "El *habeas data* y sus particularidades frente al amparo", en *Revista de Derecho Procesa*l nº 4, Rubinzal Culzoni, Buenos Aires, 2000, pp. 215 y ss.

——, *Las omisiones inconstitucionales y su corrección a través de distintas técnicas normativas y modalidades de sentencias constitucionales*, ponencia presentada en las II Jornadas Iberoamericanas de Derecho Procesal Constitucional, San José, Costa Rica, julio/2004.

——, *Vicisitudes de la convivencia entre la acción meramente declarativa y la acción declarativa de inconstitucionalidad en el orden federal*, ponencia al XXI Congreso Nacional de Derecho Procesal, Tomo II, San Juan, 2001, pp. 775/6.

BEDAQUE, José Roberto, *Tutela cautelar e tutela antecipada: tutelas sumárias e de urgência (tentativa de sistematização)*, Malheiros, São Paulo, 1998.

BÉHÉRAN, Roberto, *El amparo y las acciones de ejecución y prohibición de Entre Ríos, Delta, Santa Fe / Paraná*, 1995.

BEKERMAN, Jorge, "Bases de datos y bancos de datos. Producto o servicio (consideraciones sobre la responsabilidad)", *La Ley*, 1990-C, 943.

BELTRAMONE, Guillermo, ZABALE, Ezequiel, "El Derecho en la era digital–Derecho informático a fin de siglo", *Juris*, Rosario (Argentina), 1997, p. 54.

BERIZONCE, Roberto O., *Efectivo acceso a la justicia*, Platense, La Plata, 1987.

——, *Tutela anticipada y definitoria*, J.A. 1996- IV, 741.

——, *Tutelas procesales diferenciadas*, Rubinzal Culzoni, Buenos Aires / Santa Fe, 2009.

——, "Recientes tendencias en la posición del juez", en *El juez y la Magistratura* (Tendencias en los albores del siglo XXI), AAVV, Instituto Iberoamericano de Derecho Procesal, Rubinzal Culzoni, Buenos Aires / Santa Fe, 1999.

BERTOLINO, Pedro, "*Habeas corpus*", en *Tutela procesal de las libertades fundamentales*, Platense, 1988.

BIANCHI, Alberto B., *De la acción declarativa de certeza a la acción declarativa de inconstitucionalidad (La conversión del caso federal en caso judicial)*, ED, 2001 p. 577 y ss.

——, *Habeas data y derecho a la privacidad*, ED, 161-866.

——, *Las acciones de clase*, Ábaco, Buenos Aires, 2001.

BIDART CAMPOS, Germán J. *El derecho de la constitución y su fuerza normativa*, Ediar, Buenos Aires, 1995

——, *El "certiorari" y la "avocación" en la Competencia de la Corte Suprema (Innovaciones en un proyecto de reforma)*, ED, 115-805.

——, "¿*Habeas data* o qué? ¿Derecho a la verdad o qué?", *La Ley*, 1999-A, 212.

——, *El derecho a la jurisdicción en Argentina*, ED, 11-969.

——, "La tipología de la Constitución Argentina", en *Constitución de la Nación Argentina* (Sabsay, Daniel, Director, Manili, Pablo L., coordinador), tomo I (ver Sabsay).

——, *Las obligaciones en el derecho constitucional*, Ediar, Buenos Aires, 1987.

——, *Régimen legal y jurisprudencial del amparo*, Ediar, Buenos Aires, 1968.

——, "Tratado elemental de derecho constitucional argentino", Tomo 1: *El derecho constitucional de la libertad*, Ediar, Buenos Aires, 1986.

BISCARETTI DE RUFFIA, Paolo, *Derecho Constitucional*, Tecnos, Madrid, 1987.

BLANCO Z., Gilberto Augusto, "La acción de incumplimiento. Comentarios a las limitaciones de su ejercicio", *Revista de Derecho* Universidad del Norte n° 19 (2003), pp. 142 y ss.

BLASCO SOTO, María del Carmen, *La sentencia en la cuestión de constitucionalidad*, Bosch, Barcelona, 1995.

BOCANEGRA SIERRA, Raúl, *El valor de las sentencias del Tribunal Constitucional*, Instituto de Estudios de la Administración Local, Madrid, 1982.

BOMFIM Marins, Víctor A., *Anticipaçao da tutela e tutela cautelar*, Jurua, Curitiba, 2001.

BORCHARD, Edwin M., "Las sentencias declarativas", *Revista de Derecho Procesa*l, 1947 I parte, Año V, p. 581).

BORDALÍ SALAMANCA, Andrés, "El modelo chileno de jurisdicción constitucional de las libertades. Análisis en el marco de los valores de seguridad jurídica e igualdad constitucional", *Revista de Derecho* (Valdivia), Vol. XVIII - N° 1 - Julio 2005, pp. 89 y ss.

BRAGE CAMAZANO, Joaquín, *La acción abstracta de inconstitucionalidad*, UNAM, México, 2005.

BREWER CARÍAS, Allan R., NAVEJA MACÍAS, José de Jesús, "La situación general de la acción de amparo contra particulares en el derecho latinoamericano", *Revista Trilogía* n° 4 pp. 18 y ss.

BREWER CARÍAS, Allan R., "El derecho de amparo y la acción de amparo", en *Revista de Derecho Público* n° 22, editorial jurídica venezolana, Caracas, 1985 pp. 51 y ss.

El sistema de la justicia constitucional en la Constitución de 1999, Editora Jurídica Venezolana, Caracas, 2000, pp. 25 y ss.

BRICOLA, F., "La tutela degli interessi colletivi nel processo penale", en *Le azione a tutela di interessi colletivi*, Padova, 1976, p. 133.

BRISEÑO SIERRA, Humberto, *Derecho Procesal*, Harla (2ª ed.), 1995.

BRÜEHANN, Ulf, *La escena internacional y la directiva comunitaria: 5 semanas antes de su entrada en vigor*, en XX Conferencia Internacional de autoridades de protección de datos (1998), Agencia de Protección de Datos, Madrid, 1999.

BUJOSA VADELL, Lorenzo, *La protección jurisdiccional de los intereses de grupo*, Bosch, Barcelona, 1995.

BURGOA, Ignacio, *Juicio de Amparo*, Porrúa, México, varias ediciones.

——, *Las garantías individual*es, Porrúa, México, 1978..

BUSTAMANTE ALSINA, Jorge, "Responsabilidad civil por daño ambiental", *La Ley* 1994-C, 1052.

BUSTILLOS, Julio, "La realidad de la justicia constitucional local mexicana en el siglo XXI", *Revista Cuestiones Constitucionales* n° 21 (2009), ps 67 y ss.

CALAMANDREI, Piero, *Derecho procesal civil*, trad. de Santiago Sentís Melendo, Ejea, Buenos Aires, 1986 (tres volúmenes), se siguió el tomo III que es la traducción de La illegitimità costituzionale delle leggi nel processo civile (Cedam, Padova, 1950).

——, *Estudios sobre el Proceso Civil*, Bibliográfica Argentina, Buenos Aires, 1945.

——, *Instituciones de Derecho Procesal Civil*, tomo I, Ejea, Buenos Aires, 1986.

CALSAMIGLIA, A., "Sobre el principio de igualdad", en *El fundamento de los derechos humanos*, de Muguerza J. y otros, Debate, Madrid, 1989.

CAMARGO, Pedro Pablo, *Las acciones populares y de grupo*, Leyer, Bogotá, 2002 (3ª ed.).

CANOSA USERA, Raúl, "Dificultades para la articulación de la Justicia Constitucional y la Jurisdicción ordinaria en España", en el libro colectivo coordinado por Castañeda Otsu, Susana Inés, *Derecho Procesal constitucional*, tomo I, Jurista, (2ª ed.), Lima, 2004, pp. 153 y ss.

CAPARROZ, Luciano, "La Legitimación de los Legisladores Nacionales y la motivación del DNU 296/2010", *La Ley*, 10/03/2010, 1

CAPPELLETTI, Mauro, *Dimensión de la justicia en el mundo contemporáneo*, trad. de Héctor Fix Fierro, Porrúa, México, 1993.

——, "Formaciones sociales e intereses de grupo frente a la justicia civil", en *Boletín Mexicano de derecho comparado*, nueva serie, año XI nums.. 31/32 enero/agosto, 1978-.

——, *La giurisdizione della libertà*, Giuffrè, Milano. Hay varias ediciones posteriores y una traducción al español de Héctor Fix Zamudio en 1961.

——, *La justicia constitucional (Estudios de derecho comparado)*, UNAM, México, 1987.

CARBONE, Carlos, Los despachos interinos de fondo, en "Sentencias anticipadas", AAVV (obra dirigida por Peyrano, Jorge W.), Rubinzal Culzoni, Buenos Aires / Santa Fe, 2000.

CÁRDENAS GRACIA, Jaime, "El municipio en las controversias constitucionales", *Boletín Mexicano de Derecho Comparado* Nueva Serie Año III N° 8 (Mayo-Agosto), 1970, pp. 177 y ss.

CARNELUTTI, Francesco, *Derecho y Proceso*, Ejea, Buenos Aires, 1971.

——, *Estudios de derecho procesal*, tomo II, Ejea, Buenos Aires, 1952.

——, *Instituciones de derecho procesal civil*, tomo I, Ejea, Buenos Aires, 1986.

CAROCCA PÉREZ, Alex, *Garantía Constitucional de la defensa procesal*, Bosch, Barcelona, 1997.

CARPIO MARCOS, Edgar, "El proceso de cumplimiento en el Código Procesal Constitucional", en *Introducción a los procesos constitucionales* AAVV, Jurista, Lima, 2005.

CARRILLO, Marc, "Libertad de expresión, personas jurídicas y derecho al honor", en *Derecho Privado y Constitución*, nº 10 (1996).

CARRIÓ, Genaro R., "Nuevas fronteras del recurso extraordinario", en *Temas de casación y recurso extraordinario (en honor a Augusto Mario Morello)*, Platense, La Plata, 1982, pp. 212/213.

"Don Quijote en el Palacio de Justicia (La Corte Suprema y sus problemas)", *La Ley*, 1989-E, 1131.

CASALLO LÓPEZ, Juan Martín, "Protección de datos", en *Temas de Interés*, nº 3, Escuela Nacional de Inteligencia (Argentina), Buenos Aires, 1999.

CASCAJO CASTRO, José L., GIMENO SENDRA, Vicente, *El recurso de amparo*, Tecnos, Madrid, 1992.

CASSIANO LOSSIO, Ivan, "La acción procesal constitucional de inconstitucionalidad por omisión a raíz de los silencios legislativos", Pontificia Universidad Católica del Perú, *Revista de la Maestría en Derecho Procesal* n° 74.

CASTILLO CÓRDOVA, Luis F., "Primer código procesal constitucional de alcance nacional en Latinoamérica: Comentarios a la ley 28.237", *Revista Cuestiones Constitucionales*, nº 14, Instituto de Investigaciones Jurídicas – UNAM, México, año 2006 (Enero/junio).

CATALÁN GONZÁLEZ, Miguel, "Descrédito, intimidad y encubrimiento", en *Sobre la intimidad*, Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

CAVOUKIAN, Ann, *Comercio electrónico: las personas necesitan protección, no perfección, en XX Conferencia Internacional de autoridades de protección de datos* (1998), Agencia de Protección de Datos, Madrid, 1999.

CERDA SILVA, Alberto, "Autodeterminación informativa y leyes sobre protección de datos", *Revista Chilena de Derecho Informático* nº 3, diciembre de 2003, pp. 26 y ss.

——, "Mecanismos de control en la protección de datos en Europa", *Revista Ius et Praxis*, 12 (2), Talca, 2006, pp. 221/251.

CHIOVENDA, Giuseppe, "Acciones y sentencias de declaración de mera certeza", *Revista de Derecho Procesal,* 1947 I parte, Año V, pp. 528 y ss.

——, *Principios de Derecho Procesal Civil*, tomo 2, Reus, Madrid, 1925..

CHRISTENSEN, Eduardo Alberto, "El *habeas data* como tutela en el derecho tributario", en *Libro de Ponencias* del XX Congreso Nacional de Derecho Procesal, celebrado en la ciudad de San Martín de los Andes del 5 al 9 de octubre de 1999.

CIFUENTES MUÑOZ, Eduardo, "El *habeas data* en Colombia"*, Revista Ius et praxis* nº 1, año 3, Talca, 1997, pp. 81/106.

——, "Informe sobre la jurisdicción constitucional en Colombia", *Ius et praxis*, vol. 6 n° 2, 2000, Universidad de Talca, Chile, p. 64.

——, "La jurisdicción constitucional en Colombia", *Ius et Praxis*, v.8 n° 1, Talca, 2002, pp. 283 y ss.

CIFUENTES, Santos, *Derechos personalísimos*, Astrea, Buenos Aires, 19956.

CIPRIANI, Franco, *Batallas por la Justicia Civil*, Cultural Cuzco, Lima, 2003.

COLAÇO ANTUNES, Luis Felipe, *A tutela dos interesses difusos em direito administrativo*, Livraría Almedina, Coimbra, 1989.

COLOMBO CAMPBELL, Juan, "Funciones del derecho procesal constitucional", *Ius et Praxis*, v.8, n°2, Talca, 2002.

COLOMER HERNÁNDEZ, Ignacio, *La motivación de las sentencias: sus exigencias constitucionales y legales*, Tirant lo Blanch, Valencia, 2003.

CONCEPCIÓN RODRÍGUEZ, José Luis, *Honor, intimidad e imagen*, Bosch, Barcelona, 1996.

CORDÓN MORENO, Faustino, "El proceso de amparo constitucional", *La Ley*, Madrid, 1992 (2ª ed.).

COSSÍO DÍAZ, José Ramón, "Las partes en las controversias constitucionales", en *Cuestiones Constitucionales* n° 16, enero-junio 2007, *Revista de la Universidad Nacional Autónoma de México: Instituto de Investigaciones Jurídicas*.

——, "La función constitutiva de los tribunales constitucionales y la división de poderes", en *Anuario de Derecho Constitucional Latinoamericano* n° 14, Fundación Konrad Adenauer, Montevideo, 2008, pp. 103 y ss.

COUTURE, Eduardo J., *Estudios de derecho procesal civil*, Tomo III, Depalma, Buenos Aires, 1979.

——, *Fundamentos de derecho procesal*, Depalma, Buenos Aires, 1987 (3ª edición póstuma)..

CREO BAY, Horacio, *Amparo por mora de la Administración Pública*, Astrea, Buenos Aires, 2006 (3ª edición).

CRETELLA JUNIOR, José, *Os writs na Constituiçao de 1988*, Forense, Río de Janeiro, 1989.

CUENCA, Humberto, *Proceso civil romano*, Ejea, Buenos Aires, 1957.

Cuervo, José, "Autodeterminación informativa"*, Revista Informática Jurídica*, versión on line

DALLA VÍA, Alberto R., BASTERRA, Marcela Izascum, *Habeas data y otras garantías constitucionales*, Némesis, Buenos Aires, 1999.

DAVARA RODRÍGUEZ, Miguel Angel, *La protección de datos en Europa*, Universidad Pontificia COMILLAS, MADRID, 1998.

David, Rene, *Les grands systèmes de Droit contemporains*, 6ª ed. París, 1974. VÉSCOVI, Enrique, "Nuevas tendencias y realidades del proceso civil", en *Revista Uruguaya de Derecho Procesal*, nº 4, Montevideo, 1994, pp. 461 y ss.

DE BERNARDIS, Luis Marcelo, *La garantía procesal del debido proceso*, Cuzco S.A., Lima, 1995.

DE CUPIS, Adriano, *I diritti della personalità*,editorial Giuffrè, Milan, 1982.

DE LA OLIVA SANTOS, Andrés, *Sobre el derecho a la tutela jurisdiccional*, Bosch, Barcelona, 1980.

DE LÁZZARI, Eduardo, *Medidas Cautelares*, Tomo I, editora Platense, La Plata, 1989

DE LOS SANTOS, Mabel A., *Algunas pautas para la regulación normativa de los procesos colectivos*, ponencia presentada al XXIII Congreso Nacional de Derecho Procesal, Mendoza, 2005 (J.A. 2005-IV, 1269).

——, "Medida autosatisfactiva y medida cautelar (Semejanzas y diferencias entre ambos institutos procesales)", en *Revista de Derecho Procesal*, nº 1, Rubinzal Culzoni, Buenos Aires, 1998.

DE SLAVIN, Diana, *Mercosur: La protección de los datos personales*, Depalma, Buenos Aires, 1999.

DE TRAZEGNIES GRANDA, Fernando, *Postmodernidad y Derecho*, Ara, Lima, Perú, 1996.

DEL PESO NAVARRO, Emilio, "La protección y la seguridad de los datos automatizados de carácter médico", en *Actas del II Congreso Internacional de Informática y Derecho*, Mérida, 1995.

DEL VECCHIO, Giorgio, *Derecho y vida*, Ariel, Barcelona, 1942.

DESCALZI, José Pablo, "El control de constitucionalidad. Repaso de la situación en La Pampa", *La Ley Patagonia*, 2006, pp. 507 y ss.

DEVIS ECHANDÍA, Hernando, *Teoría de la prueba judicial*, tomo I, Temis, Bogota, 2004.

——, *Teoría General del Proceso*, Tomo I, Universidad, Buenos Aires, 1984.

DI IORIO, Alfredo J., *Temas de derecho procesal*, Depalma, Buenos Aires.

——, "Una nueva formulación de la teoría de la acción y las pretensiones procesales", *La Ley,* 1988-A, p. 667.

DÍAZ REVORIO, Francisco Javier, "Tribunal Constitucional y procesos constitucionales en España: Algunas reflexiones tras la reforma de la Ley Orgánica del Tribunal Constitucional de 2007", *Estudios Constitucionales*, Año 7, N° 2, 2009, pp. 81-108

DÍAZ RICCI, Sergio, "El Tribunal Constitucional 'non nato' de Tucumán", en *Proceso y Constitución*, AAVV (Director: Osvaldo A. Gozaíni), Ediar, Buenos Aires, 2009, pp. 111 y ss.

——, "Algunos problemas de la jurisdicción constitucional argentina. Un Código procesal constitucional", en *Anuario de Justicia Constitucional*, Nº 9, 2005, Madrid, CEPC, 2005.

DÍAZ, Clemente A., *Instituciones de Derecho Procesal*, Parte General, tomo I (Introducción), Abeledo Perrot, Buenos Aires, 1968.

DÍEZ PICAZO, Luis, *El régimen constitucional del Poder Judicial*, Cívitas, Madrid, 1991.

DWORKIN, Ronald, *Los derechos en serio*, Ariel, Barcelona, 1984.

EGÜES, Alberto J., "El certiorari argentino", *La Ley*, 1993-C, 661.

EISNER, Isidoro, "Planteos Procesales", *La Ley*, Buenos Aires, 1984..

EKMEKDJIAN, Miguél Angel, PIZZOLO, Calógero, *Habeas Data. El derecho a la intimidad frente a la revolución informática*, Depalma, Buenos Aires, 1996.

Ekmekdjian, Miguel Ángel, "El *habeas data* en la reforma constitucional", en Rev. *La Ley*, 1995-E, 946 y ss.

ESCOBAR FORNOS, Iván, *Introducción al derecho procesal constitucional*, Biblioteca Porrúa de Derecho Procesal Constitucional n° 9, Porrúa, México, 2005.

ESPINAR VICENTE, José María, "La primacía del derecho a la información sobre la intimidad y el honor", en *Estudios sobre el derecho a la intimidad*, Tecnos, Madrid, 1992..

Espinosa-Saldaña Barrera, Eloy, "Código Procesal Constitucional: Estudio introductorio", en *Introducción a los procesos constitucionales* AAVV, Jurista, Lima, 2005.

ESTADELLA YUSTE, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales*, editorial Tecnos, Madrid, 1995.

ETO CRUZ, Gerardo, "John Marshall y la sentencia Marbury vs. Madison", en *Revista Peruana de Derecho Constitucional*, passim, reproducido en *Derecho Procesal Constitucional*, tomo I (coordinador Eduardo Ferrer Mac Gregor), Porrúa, México, 2002.

FAIRÉN GUILLÉN, Víctor, "Acción", *Revista de derecho procesal*, 1950-I, p. 48.

"El procedimiento preferente y sumario y el recurso de amparo", *Revista de la Administración Pública* (RAP) nº 89 (1989)

——, *Ensayo sobre procesos complejos. La complejidad de los litigios*, Tecnos, Madrid, 1991.

——, "La potestad jurisdicciona", en *Revista de Derecho Judicial* (España), 1972, pp. 81 y ss.

——, FALCÓN, Enrique M., "El derecho procesal constitucional (Teoría general, nacimiento y desarrollo de la disciplina, contenido, autonomía científica)", en *La ciencia del derecho procesal constitucional. Estudios en homenaje a Héctor Fix Zamudio*, tomo I *(Teoría General del derecho procesal constitucional)*, cit., p. 451.

——, *Habeas Data*, Abeledo Perrot, Buenos Aires, 1996.

——, *Tratado de derecho procesal civil y comercial*, tomo IV, Rubinzal Culzoni, Buenos Aires / Santa Fe, 2006.

——, *Tratado de la prueba*, tomo I, Astrea, Buenos Aires, 2004.

——, *Código Procesal Civil y Comercial de la Nación*, tomo I, Astrea, Buenos Aires, 2006, .

FALCONI PUIG, Juan, "Amparo Constitucional", publicado en *Diario Hoy*, Guayaquil, del día 5 de junio de 2009.

FAPPIANO, Oscar Luján, "*Habeas data*: Una aproximación a su problemática y a su posible solución normativa", en *Liber Amicorum* Héctor Fix Zamudio, volumen 1, Secretaría de la Corte Interamericana de Derechos Humanos, San José, Costa Rica, 1998, pp. 322 y ss.

FARRELL, Martín D., "La argumentación de las decisiones en los tribunales colectivos", *La Ley,* 2003-F, 1161.

FAVOREAU, Louis, *Los tribunales constitucionales*, trad. de Vicente Villacampa, Ariel, Barcelona, 1994..

FAZZALARI, Elio, *Note in tema di diritto e processo*, Cedam, Milano, 1957.

FENECH, Miguel y CARRERAS, Jorge, "Notas previas al estudio del Derecho Procesal", en *Estudios de Derecho Procesal*, Bosch, Barcelona, 1962..

FERNÁNDEZ-VIAGAS BARTOLOMÉ, Plácido, *El juez imparcial*, Comares, Granada, 1997.

FERNÁNDEZ LÓPEZ, Juan Manuel, "El derecho a la privacidad y su frontera en los demás derechos humanos", en XX *Conferencia Internacional de Autoridades de Protección de Datos* (1998), Agencia de Protección de Datos, Madrid.

FERNÁNDEZ NETO, *Guilherme, La protección de los derechos metaindividuales en el derecho comparado*, Ministerio Público de la República Oriental del Uruguay, Montevideo, 2002, passim.

FERNÁNDEZ RODRÍGUEZ, José Julio: *La inconstitucionalidad por omisión. Teoría general. Derecho Comparado. El caso español,* Cívitas, Madrid, 1998.

FERNÁNDEZ SEGADO, Francisco, "La dinamización de los mecanismos de garantía de los derechos y de los intereses difusos en el Estado social", *Boletín Mexicano de Derecho Comparado* nº 83, Mayo-Agosto, 1985.

FERNÁNDEZ SESSAREGO, Carlos, *Derecho a la identidad personal*, Astrea, Buenos Aires, 1992.

Ferrada Bórquez, Juan Carlos-BORDALÍ SALAMANCA, Andrés-CAZOR ALISTE, Kamel, "El recurso de protección como mecanismo de control jurisdiccional ordinario de los actos administrativos: una respuesta inapropiada a un problema jurídico complejo", *Revista de Derecho*, Vol. XIV, julio 2003, pp. 67 y ss.

Ferrajioli, Luigi, *Derecho y razón. Teoría del garantismo penal*, Trotta, Madrid, 1995.

FERRER MAC GREGOR, Eduardo-GIDI, Antonio, *Procesos colectivos. La tutela de los derechos difusos, colectivos e individuales en una perspectiva comparada*, Porrúa, México, 2004;

FERRER MAC GREGOR, Eduardo, "Aportaciones de Héctor Fix Zamudio al derecho procesal constitucional", en *Derecho Procesal constitucional*, tomo I (coordinador Eduardo Ferrer Mac Gregor), Porrúa, México, 2002.

"Breves notas sobre el amparo iberoamericano (Desde el derecho procesal constitucional comparado)", en *El Derecho de Amparo en el mundo* (Fix Zamudio, Héctor-Ferrer Mac Gregor, Eduardo-coordinadores), Porrúa, 2006.

Ensayos sobre Derecho Procesal Constitucional, Porrúa-Comisión Nacional de los Derechos Humanos, México, 2004.

——, Héctor Fix Zamudio y el origen científico del derecho procesal constitucional (1928 – 1956), en *La ciencia del derecho procesal constitucional. Estudios en homenaje a Héctor Fix Zamudio*, tomo I *(Teoría General del derecho procesal constitucional)*, UNAM, Instituto Mexicano de Derecho Procesal Constitucional, Marcial Pons, México, 2008).

——, *La acción constitucional de amparo en México y España*, Porrúa, México, 2002 (2ª ed.).

——, "La nueva sala constitucional en el Estado de Veracruz", en *Justicia Constitucional Local*, AAVV (Ferrer Mac Gregor, Eduardo-Vega Hernández, Rodolfo, coordinadores), Fundap, Querétaro, 2003.

——, Los Tribunales Constitucionales en Iberoamérica, Fundap, Querétaro (México), 2002.

FIX ZAMUDIO, Héctor, *Derecho Constitucional Mexicano y Comparado*, Porrúa, 2009 (6ª ed.).

——, "El juicio de amparo mexicano y el recurso constitucional federal alemán (breves reflexiones comparativas)", *Boletín Mexicano de Derecho Comparado* nº 77, mayo / agosto, 1993.

——, *Ensayos sobre el derecho de amparo*, Porrúa, México, 2003 (3ª ed.).

——, *Introducción al estudio comparativo de la protección internacional de los derechos humanos*, Instituto de Investigaciones Jurídicas –UNAM-, México, 1974.

——, *Justicia Constitucional, Ombudsman y derechos humanos*, Comisión Nacional de Derechos Humanos, México, 1993..

FLORES DAPKEVICIUS, Rubén, "La nueva ley de *habeas data* en Uruguay" nº 18.331, en *Informática Jurídica*, Punta del Este, 2008, passim.

——, *Furno, Disegno sistematico delle oposizione nel processo executivo*, Apéndice, Firenze, 1936.

G. GARZÓN Clariana, *El marco jurídico de los flujos internacionales de datos*, IBI, Doc. TDF 206, Roma, 1984, passim.

GARCÍA BELAÚNDE, Domingo, "El derecho procesal constitucional y su configuración jurídica", en *Revista Iberoamericana de Derecho Procesal Constitucional-Proceso y Constitución*, nº 2, julio/diciembre 2004, Porrúa, México.

——, *De la jurisdicción constitucional al derecho procesal constitucional*, Grijley, Lima, 2000.

——, *Derecho Procesal Constitucional*, Temis, Bogotá, 2001.

——, *El Derecho Procesal Constitucional en perspectiva*, Biblioteca Porrúa de Derecho Procesal Constitucional n° 24, Porrúa, México, 2008.

——, El *Habeas corpus* latinoamericano", *Boletín Mexicano de Derecho Comparado* nº 104 (mayo/agosto – 2002).

——, "El *Habeas data* y su configuración normativa (con algunas referencias a la Constitución peruana de 1993)", en *Liber Amicorun Héctor Fix Zamudio*, volumen I, Secretaría de la Corte Interamericana de Derechos Humanos, San José de Costa Rica, 1998, pp. 234 y ss.

——, "La interpretación constitucional en Latinoamérica", en *Constitución de la Nación Argentina* (Sabsay, Daniel –Director- Manili, Pablo L. –coordinador-), tomo I, pp. 104 y ss.

——, "La jurisdicción constitucional y el modelo dual o paralelo", en Revista *La Ley*, 1998-F, 1175 y ss.

——, "Sobre la jurisdicción constitucional", en *Jurisdicción constitucional* (coordinador general Aníbal Quiroga León), Pontificia Universidad Católica del Perú, Lima, 1990, p. 90.

García de Enterría, Eduardo, *La Constitución como Norma y el Tribunal Constitucional*, Cívitas, Madrid, 1995.

García González, Aristeo, "La protección de datos personales dentro del ámbito judicial de México. Una visión estatal". *Revista de Derecho Informático*, nº 110 (2006), diciembre, versión on line.

García Laguardia, Jorge Mario, *La Defensa de la Constitución,* Universidad San Carlos-Instituto de Investigaciones Jurídicas <UNAM>, México, 1986.

García Martínez, María Asunción, "El control de constitucionalidad y sus acciones procesales", en *Derecho Procesal Constitucional*, tomo I, obra coordinada por Susana Ynés Castañeda Otsu, Jurista, Lima [Peru], 2004 (2ª ed.).

García Pullés, Fernando R., "Las sentencias que declaran la inconstitucionalidad de las leyes que vulneran derechos de incidencia colectiva. ¿El fin del paradigma de los limites subjetivos de la cosa juzgada? ¿El nacimiento de los procesos de clase?", *La Ley* 04/03/09.

García San Miguel, Luis, *Estudios sobre el derecho a la intimidad*, Tecnos – Universidad de Alcalá de Henares, Madrid, 1992.

Gelli, María Angélica, "Constitución de la Nación Argentina. Comentada y Concordada". *La Ley* (2ª ed.), Buenos Aires, 2003.

——, "Dilemas del recurso extraordinario federal", *La Ley*, 2004-A, 1302.

Gelsi Bidart, Adolfo, *De Derechos, Deberes y Garantías del hombre común*, Fundación de Cultura Universitaria, Montevideo, Uruguay, 1986.

——, "El Derecho Procesal y la protección al consumidor", en *Revista Uruguaya de Derecho Procesal* nº. 1, 1978, pp. 11/25.

Ghersi, Carlos A., *Modernos conceptos de responsabilidad civil*, Ediciones Jurídicas Cuyo, Mendoza, 1995.

Giacomette Ferrer, Ana, "La prueba en los procesos constitucionales", *Señal* – ediciones Uniandes, Bogotá, 2007.

——, *Acciones populares, ponencia presentada en el XVII Encuentro Panamericano de Derecho Procesal*, Barranquilla, Colombia, 2004.

Gil Cremades, Juan José, "La motivación de las decisiones jurídicas", en *Estudios en memoria de los profesores Vicente Herce Quemada y Angel Dique Barragués*, Facultad de Derecho de la Universidad de Zaragoza, 1983, pp. 234 y ss.

Gil Rendón, Raymundo, *Derecho Procesal Constitucional*, Fundap, Querétaro, 2004,.

Gil Robles, Alvaro, *Los nuevos límites de la tutela judicial efectiva*, Centro de Estudios Constitucionales, Madrid, 1996.

Gils Carbó, Alejandra, "Régimen legal de las bases de datos y *habeas data*", *La Ley*, Buenos Aires, 2001.

GIMENO SENDRA, José Vicente, *Fundamentos de Derecho Procesal*, Cívitas, Madrid, 1981.
——, *Constitución y Proceso*, Tecnos, Madrid, 1988.
GIRÓN LARRUCEA, José A., *Cuestiones de Derecho Comunitario Europeo*, pp. Universidad de Sevilla, 1997.
GITRAMA GONZÁLEZ, Manuel, *Derecho a la propia imagen*, SEIX XI, Madrid, 1962
Glasson, Précis *théorique et practique de procedure civile*, 2ª ed., Tomo I, París, 1908.
GOLDSCHMIDT, James, *Derecho Procesal Civil*, traducción Leonardo Prieto Castro, Labor, Barcelona, 1936.
GÓMEZ COLOMER, Juan Luis, *El beneficio de pobreza*, Bosch, Barcelona, 1982..
GÓMEZ GARCÍA, Carlos Fernando. "Las Vías de Hecho como generadoras del Choque de Trenes en la jurisprudencia constitucional. (1992-2008)". Artículo inédito, desarrollado dentro de su permanencia como Joven Investigador en el Grupo de Investigación en Derecho Público *Diego de Torres y Moyachoque, Cacique de Turmequé* de la Universidad de La Sabana.
GOMEZ LOECHES, Luis, *El acceso a la documentación de las actuaciones judiciales*, Universidad Alcalá de Henares, Madrid, Centro de Documentación.
GÓMEZ MONTORO, Ángel J., *El conflicto entre órganos constitucionales*, Madrid, Centro de Estudios Constitucionales, 1992.
GONZÁLEZ CANO, María Isabel, *La tutela colectiva de consumidores y usuarios en el proceso civil*, Tirant lo blanch, Valencia, 2002.
GONZÁLEZ GRANDA, Piedad, *Independencia del juez y control de su actividad*, Tirant lo Blanch, Valencia, 1993.
GONZÁLEZ PÉREZ, Jesús, *Derecho Procesal Constitucional*, Cívitas, Madrid, 1980.
——, *El derecho a la tutela jurisdiccional*, Cívitas, Madrid, 1989 (2ª ed.)
GORDILLO, Agustín A., Tratado de Derecho Administrativo, Tomo 3, Fundación de Derecho Administrativo, Buenos Aires, 1999 (4ª ed.).
GOZAÍNI, Osvaldo Alfredo, *Código Procesal Civil y Comercial de la Nación*, tomo I, La Ley, Buenos Aires, 2006 (2ª ed.),
——, *Costas Procesales*, Ediar, Buenos Aires, 1998 (2ª ed.).
——, *Derecho Procesal Civil*, Tomo I (Jurisdicción, acción y proceso), volumen 1, Ediar, Buenos Aires, 1992
——, *Derecho Procesal Constitucional – Debido proceso*, Rubinzal Culzoni, Santa Fe-Buenos Aires, 2004.
——, *Derecho Procesal Constitucional – Habeas data, Protección de Datos Personales*, Rubinzal Culzoni, Buenos Aires / Santa Fe, 2001.
——, *Derecho Procesal Constitucional – Habeas data*, Rubinzal Culzoni, Buenos Aires, 2001.
——, *Derecho Procesal Constitucional*, tomo 1, editorial de Belgrano, Buenos Aires, 1999.
——, "El alcance de la cosa juzgada en los procesos colectivos", en *La Ley*, 2005-F, 626.
——, *El Derecho de Amparo*, Depalma, Buenos Aires, 1995.
——, "El impacto de la jurisprudencia del sistema interamericano en el derecho interno", en *El control de convencionalidad*, ALBANESE, Susana (coord.), Ediar, Buenos Aires, pp. 104 y 105.
——, *El proceso transnacional*, Ediar, Buenos Aires, 1992.
——, *Introducción al derecho procesal constitucional*, Rubinzal Culzoni, Buenos Aires / Santa Fe, 2006.
——, "La afiliación partidaria como dato sensible que no se puede difundir", *La Ley*, 2002-F, 1437 y ss. (diario del 14 de noviembre de 2002).
——, *La justicia constitucional*, Depalma, Buenos Aires, 1997.

——, "Las decisiones en los conflictos transnacionales", en *Revista Ars Juris*, nº 12, Universidad Panamericana, México, 1994, pp. 347 y ss.

——, "Los efectos de las sentencias de la Corte Interamericana de Derechos Humanos en el derecho interno", en *Liber amicorum Héctor Fix Zamudio*, tomo II, Secretaría de la Corte Interamericana de Derechos Humanos, 1998, p. 828.

——, L*os problemas de legitimación en el proceso constitucional*, Biblioteca Porrúa de Derech Procesal Constitucional n° 4, Porrúa, México, 2005.

——, *Respuestas Procesales*, Segunda Parte, Ediar, Buenos Aires, 1999, pp. 341 y ss.

——, *Tratado de Derecho Procesal Civil*, tomo I, La Ley, Buenos Aires, 2009.

GROPPI, Tania, "¿Hacia una justicia constitucional 'ductil'? Tendencias recientes de las relaciones entre Corte Constitucional y Jueces comunes en la experiencia italiana, *Boletín Mexicano de Derecho Comparado*, 107, Instituto de Investigaciones Jurídicas – UNAM, México, passim).

GUARNIERI, Carlos, *L´independenza della magistratura*, CEDAM, Padua, 1981.

GUASP, Jaime, *Comentarios a la ley de enjuiciamiento civil española*, tomo I, Aguilar, Madrid, 1946.

——, *Derecho Procesal Civil*, Instituto de Estudios Políticos, Madrid, 1956.

——, "La paralización del proceso civil y sus diversas formas", en *Estudios Jurídicos*", edición al cuidado de Aragoneses, Pedro, Cívitas, Madrid.

GUASTAVINO, Elías P., *Recurso extraordinario de inconstitucionalidad*, Tomo I, La Rocca, Buenos Aires, 1992, pp. 79 y ss.

HÄBERLE, Peter *Nueve ensayos constitucionales y una lección jubilar*, Palestra, Lima, 2004,

——, *Derecho Constitucional Común Europeo*, trad. de Emilio Muranda Franco, en *Derechos Humanos y Constitucionalismo ante el tercer milenio*, coordinador Antonio-Enrique Perez Luño, Marcial Pons, Madrid, 1996.

——, "La jurisdicción constitucional institucionalizada en el Estado Constitucional", en *Derecho Procesal Constitucional*, tomo I (coordinador Eduardo Ferrer Mac Gregor), Porrúa, México, 2003 (3ª ed.), pp. 373 y ss.

HABERMAS, Jürgen, *Historia y crítica de la opinión pública*, traducción de Antoni Domenech, Ediciones de Gustavo Gili, Barcelona, 1994.

HAZARD, Jr., Geoffrey C.-Taruffo, Michele, *La justicia civil en los Estados Unidos*, traducción de Fernando Gascón Inchausti, Thomson – Aranzadi, Navarra, 2006.

HELLNER, John, From data proteccion to knowledge machines, Kluwer, Deventer, 1990.

HELLWIG, KLAGERECHT und Klagemoglichkeit, Leipzig, 1905; Weismann, Lehrbuch des deutschen Zivilprocessrechts, Stuttgart, 1903.

HENRÍQUEZ MAIONICA, Giancarlo, *El amparo constitucional: Control de los derechos fundamentales*, Sherwood, Caracas, 2004.

HERNÁNDEZ BATALLER, Bernardo, *Acceso a la justicia del consumidor, en Revista de la Asociación de Usuarios de la Comunicación*,

HERNÁNDEZ MARTÍNEZ, María del Pilar, "Constitución y Derechos Fundamentales", *Boletín Mexicano de Derecho Comparado* nº 84, 1995, pp. 126 y ss.

HERNÁNDEZ VALLE, Rubén, *Derecho Procesal Constitucional, Juricentro*, San José de Costa Rica, 1995.

——, *Introducción al derecho procesal constitucional*, Biblioteca Porrúa de Derecho Procesal Constitucional n° 6, Porrúa, México, 2005.

HERRÁN ORTIZ, Ana Isabel, La violación de la intimidad en la protección de datos personales, Dykinson, Madrid, 1999.

HERRERA GARCÍA, Alfonso, La controversia constitucional mexicana y el proceso competencial peruano (Breves notas comparativas sobre sus reglas generales), en "El derecho procesal constitucional peruano (Estudios en homenaje a Domingo García Belaúnde)", Grijley, Lima, 2005, pp. 1064/6 (tomo II).

HERRERO TEJEDOR, Fernando, Honor, intimidad y propia imagen, Colex, Madrid, 1990.

HIRSCH, Günter, La jurisdicción en el Estado de Derecho: entre la sujeción a la ley y la interpretación cuasilegislativa, en "Anuario de Derecho Constitucional Latinoamericano" n° 14, Fundación Konrad Adenauer, Montevideo, 2008.

HITTERS, Juan Carlos, *Alcance de la cosa juzgada en los procesos colectivos*, ponencia presentada al XXIII Congreso Nacional de Derecho Procesal, Mendoza, 2005.

——, "Control de constitucionalidad y control de convencionalidad. Comparación (criterios fijados por la Corte Interamericana de Derechos Humanos)*", Estudios Constitucionales*, Año 7, N° 2, 2009, pp. 109 y ss.

IBAÑEZ FROCHAM, Manuel, *La jurisdicción*, Depalma, Buenos Aires., 1972.

IBAÑEZ, PERFECTO Andrés, *Acerca de la motivación de los hechos en la sentencia penal*, texto de la conferencia pronunciada por el autor dentro del plan estatal de formación de jueces (1992), Consejo General del Poder Judicial de España, passim.

IMAZ, Esteban – REY, Ricardo E., *El recurso extraordinario*, Nerva, Buenos Aires, 1962 (2ª edición actualizada por Lino E. Palacio y Ricardo E. Rey)3.

IRTI, Natalino Irti, *La edad de la descodificación*, Bosch, Barcelona, 1992.

JIJENA LEIVA, Manuel, "carta…", publicada en *Boletín Hispanoamericano de Informática y Derecho*, año I nº. 5, Octubre-Noviembre, 1998.

JIMÉNEZ CAMPO, Javier, *Derechos Fundamentales. Concepto y garantías*, Trotta, Madrid, 1999.

JIMÉNEZ, Eduardo Pablo, *Los derechos humanos de tercera generación*, Ediar, Buenos Aires, 1996.

JOFRÉ, Tomás, *Código de Procedimiento Penal de la provincia de Buenos Aires, comentado y concordado*, Depalma, Buenos Aires, 1965 (2ª ed.).

KELSEN, Hans, "La garantía jurisdiccional de la Constitución (La Justicia Constitucional)", tomado del *Anuario del Instituto de Derecho Público*, París. Publicado también en *Revue de Droit Public et de la Science Politique* en France e˝al Etranger. París.

——, *General del Estado*, trad. Legaz y Lacambra, Labor, Barcelona, 1934.

——, *Teoría pura del Derecho*, Eudeba, Buenos Aires, 1969 (8a ed.).

LANDA ARROYO, César, "La acción de cumplimiento en el proyecto de Constitución de 1993, Revista del Foro, año LXXXI, nº 1, Lima, 1993, p. 55.

Los procesos constitucionales en la Constitución peruana de 1993, Ius et veritas, año IX nº 18, Lima, 1999, pp. 31/32.

——, "Estudios sobre Derecho Procesal Constitucional", Biblioteca Porrúa de Derecho Procesal Constitucional, n° 15, Porrúa, México, 2006.

——, *Teoría del derecho procesal constitucional*, Palestra), Lima, 2004.

LAZZARINI, José Luis, "El juicio de amparo", *La Ley*, Buenos Aires, 1967 (1ª edición), p. 456.

LEGAZ Y LACAMBRA, Luis, *Humanismo, Estado y Derecho*, Bosch, Barcelona, 1960.

LEGAZ, Luís, *Filosofía del Derecho*, Ariel, Barcelona, 1953.

LIBERATORI, Elena Amanda, "La acción 'Qui tam'", *La Ley actualidad*, 1.04.2004, pp. 1 y ss.

LIEBMAN, Enrico T., *Manual de Derecho Procesal Civil*, traducción de Santiago Sentís Melendo, Ejea, Buenos Aires, 1980.

LIVELLARA, Silvina, "*Habeas data* e información crediticia. La eventual responsabilidad civil de las entidades financieras y del Banco Central de la República Argentina por cesión y

publicidad de datos inexactos", *Revista de Derecho Informático*, versión on line (www.alfa-redi.com).

LOIANNO, "Adelina, Incidencia de la jurisprudencia de la Corte Interamericana y de las recomendaciones de la Comisión en el derecho interno", en *Derechos Humanos*, Fundación de Derecho Administrativo (5ª edición) Buenos Aires, 2005.

LOPES MEIRELLES, Hely, *Mandado de segurança*, Malheiros editores, San Pablo, 1998 (19ª ed. actualizada por Arnoldo Wald).

LÓPEZ DAZA, Germán. *La Justicia Constitucional Colombiana: ¿Un Gobierno de los Jueces?*, en: Corzo Sosa, Edgar (Coordinador). I Congreso Internacional sobre Justicia Constitucional. Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas. Serie Doctrina Jurídica # 476, México, 2009, pp. 291-299.

LÓPEZ GUERRA, Luis, *Democracia y Tribunales Constitucionales*, Foro Constitucional Iberoamericano nº 2/3, abril/junio 2003.

——, *Estudio preliminar a Las Sentencias Básicas del Tribunal Constitucional*, Madrid, 2000 (2ª ed.)

——, "Protección de los derechos fundamentales por la jurisdicción constitucional en Centroamérica y Panamá", en *Justicia constitucional Comparada*, AA.VV., Instituto de Investigaciones Jurídicas, UNAM, 1993, México.

LÓPEZ MEDINA, Diego Eduardo, El derecho de los jueces, Legis, Colombia, 2006 (2ª ed.).

LÓPEZ-MUÑIZ GOÑI, Miguel, La Ley de regulación del Tratamiento automatizado de los datos de carácter personal, en Revista "Informática y Derecho" números 6/7, editorial UNED, Mérida (España), 1994.

LORENZETTI, Ricardo L., "Defensa del Consumidor" *Ley* 24.240, Rubinzal Culzoni, Santa Fé, 1994.

——, "La tutela civil inhibitoria", *La Ley*, 1995-C, 1217.

——, *Las normas fundamentales del derecho privado*, Rubinzal Culzoni, Santa Fé, 1995.

——, *Teoría de la decisión judicial. Fundamentos de derecho*, Rubinzal Culzoni, Buenos Aires / Santa Fe, 2006.

LOUSTEAU HEGUY, Guillermo, *Democracia y control de constitucionalidad*, Dunken, Buenos Aires, 2002.

LUGONES, Narciso, "Antecedentes históricos, crisis y replanteo de la cuestión federal"*, La Ley*, 1985-C, 1236 -Derecho Constitucional - Doctrinas Esenciales, Tomo IV, p. 705.

LYON, David, *El ojo electrónico. El auge de la sociedad de la vigilancia*, Alianza, Madrid, 1995.

MACÍA TORRES, Pedro Jesús, "La figura del supervisor europeo de protección de datos", *Revista Informática Jurídica*, 2007, Sevilla.

MALEM PEÑA, Jorge F., "¿Pueden las malas personas ser buenos jueces?", en *Jueces y Derecho*. Compiladores: Miguel Carbonell, Héctor Fix Fierro y Rodolfo Vázquez, Porrúa UNAM, México, 2004.

MANGANELLI, Claudio, Internet, en "XX Conferencia Internacional de autoridades de protección de datos" (1998), Agencia de Protección de Datos, Madrid, 1999.

MANILI, Pablo L.-LÓPEZ ALFONSÍN, Marcelo A., ¿Quién debe ejercer el control de constitucionalidad en Argentina?, en *Defensa de la Constitución. Garantismo y controles* (Libro en reconocimiento al Dr. Germán J. Bidart Campos, Ediar, Buenos Aires, 2003.

MANILI, Pablo L., "Primeras reflexiones sobre el fallo 'Simón'. Una disidencia ajustada a derecho", en *La Ley*, 2005-F, pp. 15 y ss.

MARFIL, Andrés Manuel, ALLENDE, Germán Federico, *Amparo y otros procedimientos constitucionales en la reforma*, LL Litoral 2008 (noviembre), 1058.

MARÍN LÓPEZ, Juan José, "Las acciones de clase en el derecho español", *Revista Indret*, marzo, 2003, Madrid.

MARÍN PAGEO, Encarnación, *La cuestión de inconstitucionalidad en el proceso civil*, Cívitas, Madrid, 1990.

MARINONI, Luiz Ghilerme, "Tutela específica (arts. 461, CPC e 84, CDC)", *Revista Dos Tribunais*, 1999, San Pablo, Brasil

——, "El derecho fundamental de acción en la Constitución brasileña", *Boletín Mexicano de Derecho Comparado*, 27 de abril de 2008.

——, "La tutela anticipatoria en la reforma del proceso civil brasileño", *Jurisprudencia Santafesina*, nº 25, p. 17.

——, *Novas linhas do Processo Civil,* Malheiros, Sâo Paulo, 1996 (2ª ed.).

MARTÍNEZ MEDRANO, Gabriel, "Responsabilidad Civil de las Entidades Financieras por la generación, difusión y mantenimiento de información crediticia errónea", *Revista de Derecho Informático* nº 80 (2005), versión on line (www.alfa-redi.com).

MARTÍNEZ SOSPEDRA, Manuel, Sobre la intimidad. Derecho a la intimidad, vida privada y privacy. El art. 18 CE in principio en la jurisprudencia del Tribunal Constitucional, en Sobre la intimidad, Fundación Universitaria San Pablo C.E.U., Valencia, 1996.

MARTÍNEZ, Hernán J., El nuevo recurso extraordinario federal, La Ley 1982-A, 740.

MEDINA, Cecilia – Mera Figueroa, Jorge, Sistema jurídico y derechos humanos, Escuela de Derecho de la Universidad Diego Portales, Santiago de Chile, 1996.

MENDOZA NAVARRO, Aída Luz, Base legal sobre el acceso a la información y a los archivos en el Perú, Comunicación presentada en el "Seminario Internacional de Archivos de Tradición Ibérica, Río de Janeiro-Brasil", 3 al 7 de abril del 2000, passim.

MERCADER, Amílcar, *El proceso y la unidad del orden jurídico*, J.A., 1968-III, sec. Doctrina, pp. 744 y ss.

——, *La acción. Su naturaleza dentro del orden jurídico*, Depalma, Buenos Aires, 1944.

MICHELI, GIAN Antonio, *La carga de la prueba*, traducción de Santiago Sentís Melendo, Ejea, Buenos Aires, 1961, p. 62.

MILANTA, Claudia A. M., "Reforma procesal administrativa de la provincia de Buenos Aires. Proceso ordinario y procesos especiales", en *El nuevo proceso contencioso administrativo de la provincia de Buenos Aires*, AA.VV., (obra dirigida por Juan Carlos Cassagne y Agustín A. Gordillo, y coordinada por Carlos A. Botassi), Platense, 2004.

MILL, John S., *On liberty*, Cambridge, 1989.

MONROY CABRA, Marco Gerardo, *Introducción al Derecho*, Temis, Bogotá, 1994.

MONROY Gálvez, Juan, *Introducción al proceso civil*, Temis, Bogotá, 1996.

MONTAÑO DE CARDONA, Julia Victoria, *Instituciones procesales desde el constitucionalismo*, Leyer, Bogotá, 2002.

MONTERO AROCA, Juan, "Del Derecho Procesal al Derecho Jurisdiccional", *Revista Uruguaya de Derecho Procesal*, 1984-1, pp. 40/1.

——, "El proceso civil llamado 'social' como instrumento de 'justicia' autoritaria", en *Revista Iberoamericana de Derecho Procesal*, 2004, nº 6, pp. 15/50.

——, *Proceso civil e ideología*, Tirant lo Blanch, Valencia, 2006.

——, *Introducción al derecho procesal*, Tecnos, Madrid, 1976.

——, *La legitimación en el proceso civil*, Cívitas, Madrid, 1994.

——, *Los principios políticos de la nueva Ley de Enjuiciamiento Civil (Los poderes del juez y la oralidad)*, Tirant lo Blanch, Valencia, 2001.

MORELLO, Augusto Mario, SOSA, Gualberto Lucas, BERIZONCE, Roberto Omar, *Códigos procesales en lo civil y comercial de la provincia de Buenos Aires y la Nación*, Tomo I, Platense, Abeledo Perrot, Buenos Aires, 1982.

MORELLO, Augusto Mario, VALLEFÍN, Carlos, *El amparo. Régimen Procesal*, Librería editora Platense, La Plata, 1992.

MORELLO, Augusto Mario, "Del debido proceso y la defensa en juicio al proceso justo constitucional", *La Ley*, 2003-D, 809 y ss.

——, *El recurso extraordinario*, Abeledo Perrot, Buenos Aires, 1987.

——, *La acción, la jurisdicción y el proceso, en Problemática actual de Derecho Procesal*, Librería Editora Platense, La Plata, 1971.

——, *La prueba. Tendencias modernas*, Platense, Abeledo Perrot, Buenos Aires, 1991.

——, "La sentencia arbitraria; alternativas de la Corte Suprema ante esa manifestación negativa de la jurisdicción", *La Ley,* 1987-B, 921, *Derecho Constitucional* - Doctrinas Esenciales, Tomo IV, p. 717.

——, *Problemática actual de la justicia, Doctrina Judicial*, 1989-II, p. 1053.

MUÑOZ MACHADO, Santiago, "La reserva de jurisdicción", *La Ley*, 1989, Madrid,.

NATARÉN NANDAYAPA, Carlos F., *La tutela de los derechos fundamentales de naturaleza procesal*, UNAM, Instituto de Investigaciones Jurídicas, Serie Doctrina Jurídica, nº 358, México, 2006.

NICOLAU, Noemí L., "La tutela inhibitoria y el nuevo artículo 43 de la Constitución Nacional", *La Ley*, 1996-A, 1245.

NIEVA FENOLL, Jordi, *Enjuiciamiento prima facie*, Atelier, Barcelona, 2007.

NIGRO, M., *Giustizia amministrativa*, Il Mulino, Bologna, 1979.

NOGUEIRA ALCALÁ, Humberto, "Autodeterminación informativa y *habeas data* en Chile e información comparativa", *Anuario de Derecho Constitucional Latinoamericano*, 2005, pp.460 y ss.

——, *Consideraciones sobre las sentencias de los Tribunales Constitucionales y sus efectos en América del Sur*, ponencia presentada en las II Jornadas Iberoamericanas de Derecho Procesal Constitucional, San José, Costa Rica, julio/2004.

——, "El derecho procesal constitucional a inicios del siglo XXI en América Lartina", *Estudios Constitucionales*, Año 7, N° 1, 2009, pp. 13-58

El derecho y acción constitucional de protección (amparo) de los derechos fundamentales en Chile a inicios del siglo XXI, El Derecho de Amparo en el mundo (Fix Zamudio, Héctor, Ferrer Mac Gregor, Eduardo, coordinadores), passim.

——, "El Recurso de Protección en el Contexto del Amparo de los Derechos Fundamentales Latinoamericano e Interamericano", *Revista Ius et Praxis* nº 13 (1), Santiago, 2007. pp. 75 y ss.

——, "La reforma constitucional a la jurisdicción constitucional: Del doble control concentrado de constitucionalidad a la concentración del control en el Tribunal Constitucional," *Revista Ius et Praxis*, v. 8 nº 1, Talca (2002), pp. 337 y ss.

NOVOA MONREAL, Eduardo, *El derecho a la vida privada y libertad de información. Un conflicto de derechos*, Siglo XXI, México, 1979.

NUÑEZ, Carlos Raúl, *Codificación, Tecnología y Modernidad-La muerte de un paradigma*, Ara, Lima Perú, 1996.

NUÑEZ, José Cayetano, *Los orígenes del amparo en la República Bolivariana de Venezuela,* extracto de la conferencia pronunciada en la "Jornada Internacional de Derecho Penal", organizada por el Superior Tribunal de Justicia de Venezuela, 24 de noviembre de 2006.

NUSSBAUM, Marta, *Justicia poética*, trad. de Carlos Gardini, Andrés Bello, Barcelona, 1997.

OLANO GARCÍA, Hernán Alejandro, "El choque de trenes ¿guerra entre cortes? Acercamiento al conflicto entre órganos constitucionales de Colombia", *Doctrina y Ley*, Bogotá, 2010, pp. 22 y ss.

OLANO GARCÍA, Hernán, "La nueva acción de cumplimiento en Perú y su comparación con la colombiana", *Revista International Law*, 15, 2005, p. 542.

ORÉ CHÁVEZ, Iván, *La relación jurídica sustancial en el proceso constitucional*, Ponencia presentada ante el I Congreso de Derecho Procesal Constitucional de la Comunidad Sudamericana de Naciones (26 de mayo de 2006), passim.

OROZCO PARDO, Guillermo, "Los derechos de las personas en la Lortad", en *Revista Informática y Derecho*, números 6/7, UNED, Mérida, 1994, p. 154.

ORTECHO VILLENA, Víctor J, *Procesos constitucionales y su jurisdicción*, Rhodas, Lima, 2004 (9ª edición).

ORTIZ GUTIÉRREZ, Julio César, "La acción de tutela en la Carta Política de 1991.-El derecho de amparo y su influencia en el ordenamiento constitucional de Colombia", en *El Derecho de Amparo en el mundo* (Fix Zamudio, Héctor, Ferrer Mac Gregor, Eduardo, coordinadores).

OTEIZA, Eduardo D., *Información privada y habeas data, comunicación presentada en el XX* Congreso Nacional de Derecho Procesal, San Martín de los Andes (Argentina), 1999.

——, "Información privada y *habeas data*", en *Estudios de Derecho Procesal en homenaje a Adolfo Gelsi Bidart*, Fundación de Cultura Universitaria, Montevideo, 1999.

OTHON SIDOU, J. M., "Las nuevas figuras del derecho procesal constitucional brasileño: mandamiento de ejecución y '*habeas data*' *La Ley*, 1992-E, 1010.

OYARTE MARTÍNEZ, Rafael, "El amparo contra particulares", *Revista Judicial de Ecuador*, en www.derechoecuador.com

PADILLA, Miguel M., *Bancos de datos y acción de habeas data*, editorial Abeledo Perrot, Buenos Aires, 2001.

PALACIO, Lino E., *Derecho Procesal Civil*, tomo I, Abeledo Perrot, Buenos Aires, 1979 (2ª ed. 1ª reimpresión).

——, *El recurso extraordinario federal*, Abeledo Perrot, Buenos Aires, 1992.

——, "La pretensión de amparo en la reforma constitucional de 1994", *La Ley* 1995-D, 1240.

——, *Manual de Derecho Procesal Civil*, Abeledo Perrot, Buenos Aires, 1973.

PALAZZI, Pablo, "El *habeas data* en la Constitución Nacional (La protección de la privacidad en la era de la información)", en *Jurisprudencia Argentina* del 20/12/95.

——, "El *habeas data* y el derecho al olvido", en *Jurisprudencia Argentina*, semanario nº 6030 del 26 de marzo de 1997.

PANUCCIO, Vittorio, *Banche de dati e diritti della persona*, CEDAM, Milan, 1985.

PEGORARO, Lucio, "Clasificaciones y modelos de justicia constitucional en la dinámica de los ordenamientos", en *Revista Iberoamericana de Derecho Procesal Constitucional–Proceso y Constitución-*, nº 2, julio/diciembre 2004, Porrúa, México, pp. 131 y ss.

PEKELIS, Alejandro, "Acción", *Revista de Derecho Procesal*, 1958-I, pp. 115 y ss.;

PELLEGRINI GRINOVER, Ada, "A problemática dos interesses difusos", en *A tutela dos interesses difusos*, 1ª. ed., serie Estudios Jurídicos 1, Max Limonad, San Pablo, Brasil, 1984.

——, *Derecho Procesal Colectivo*, traducción del portugués de Copani, Juan C.,

PELLON RIVERO, R. Cancelación de tarjeta de crédito por error, Actualidad y Derecho, 1995-I, 168.

PEÑARRUBIA IZA, Joaquín María, *El derecho de acceso a los archivos y a los documentos de la Administración Militar,* Cívitas, Madrid, 1999.

PEREIRA CAMPOS, Santiago, "Intereses difusos y colectivos en Uruguay: marco conceptual, legitimación y efectos de la cosa juzgada", *Revista Uruguaya de Derecho Procesal*, 2002-2, pp. 249 y ss.

PEREZ LUÑO, Antonio E., *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 1991 (4ª edición).

——, *Ensayos de informática jurídica*, Fontamara, México, 1996.

——, "Las generaciones de derechos humanos", en *Revista del Centro de Estudios Constitucionales*, n° 10, 1991, p. 207.

——, "Los derechos humanos en la sociedad tecnológica", en *Libertad informática y leyes de protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1989, pp. 1989 y ss.

PÉREZ TREMPS, *La Justicia Constitucional en la actualidad. Especial referencia a América Latina,* cit., Foro Constitucional Iberoamericano nº 2/3, abril/junio 2003.

PETRACCHI, Enrique S., "Jurisdicción Constitucional y Derechos Humanos", *La Ley*, 2005-E, 907.

PEYRANO, Jorge W., *La acción preventiva,* LexisNexis- Abeledo Perrot, Buenos Aires, 2004.

PEYRANO, Jorge Walter, EGUREN, María Carolina, "Medidas autosatisfactivas y la necesidad de su regulación legal", *La Ley*, 2006-E (diario del 28/8/06).

PICO I JUNOY, Joan, *El derecho a la prueba en el proceso civil*, Bosch, Barcelona, 1996.

——, *El Juez y la prueba*, Bosch, Barcelona, 2007.

——, *La imparcialidad judicial y sus garantías: la abstención y la recusación*, Bosch, Barcelona, 1998.

——, "La iniciativa probatoria del juez civil y sus límites", *Revista Peruana de Derecho Procesal*, nº 2, marzo, 1998

PIERANDREI, Franco, "L´interpretazione delle norme costituzionali in Italia", en *Scritti di diritto costituzionale*, tomo II, G. Giapichelli, Turín, 1964, pp. 54 y 655.

PIERINI, Alicia, LORENCES, Valentín, TORNABENE, María Inés, *Habeas Data*, Universidad, Buenos Aires, 1998, p. 38

PINET, Marcel, *Datos públicos o datos a los que puede acceder el público y protección de datos personales*, en XX Conferencia Internacional de autoridades de protección de datos (1998), Agencia de Protección de Datos, Madrid, 1999.

PIZA, Rodolfo E., TREJOS, Gerardo, *Derecho internacional de los derechos humanos: La Convención Americana*, Juricentro, San José de Costa Rica, 1989.

PLANIOL Y RIPERT, *Traité élémentaire de droit civil Françcaise*, Tomo I, París, 1928, pp. 733 y ss.

PLAZA DE GARCÍA, Norma, "Ley de Control Constitucional", *Revista Jurídica Online* de la Facultad de Jurisprudencia, Ciencias Políticas y Sociales de la Universidad Católica de Guayaquil, passim

PLAZA PENADÉS, Javier, *Protección de datos de las personas jurídicas*, publicado el 28 de enero de 2009, en www.legaltoday.com

PODETTI, J. Ramiro, *Tratado de los recursos*, Ediar, Buenos Aires, 1958.

——, *Teoría y Técnica del proceso civil*, Ediar, Buenos Aires, 1942.

PÓLIT MONTES DE OCA, Berenice, "La legitimación activa en la acción de amparo constitucional", *Revista Judicial de Ecuador*, en www.derechoecuador.com

POPKIN, Margaret, *Iniciativas para mejorar la independencia judicial en América Latina: Una perspectiva comparativa, edición de la Fundación para el Debido Proceso Legal*, passim.

PRIETO CASTRO Y FERRANDIZ, Leonardo, *Derecho Procesal Civil*, Tecnos, Madrid, 1988.

PRIETO SANCHÍS, Luís, Ley, "Principios, Derechos", Cuadernos *Bartolomé de las Casas* (Instituto de Derechos Humanos. Universidad Carlos III de Madrid), Dykinson, Madrid, 1998.

——, "Tribunal constitucional y Positivismo Jurídico", en *Derecho Procesal Constitucional*, tomo I (coordinado por Eduardo Ferrer Mac Gregor), Porrúa, México, 2003 (3ª ed.), pp. 453 y ss.

PRITCHETT, C. Herman, *La Constitución americana*, Tea, Buenos Aires, 1965.

PUCCINELLI, Oscar Raúl, "El *habeas data* en Indoiberoamérica", en *El amparo constitucional. Perspectivas y modalidades*, AAVV, Depalma, Buenos Aires, 1999, pp. 187 y ss.

PUCCINELLI, Oscar Raúl, *El habeas data en indoiberoamérica*, Temis, Bogotá, 1999.

PUIG BRUTAU, José, *Fundamentos de derecho civil*, Tomo I, Bosch, Barcelona, 1979.

——, *La Jurisprudencia como fuente del derecho. Interpretación creadora y arbitrio judicial*, Bosch, Barcelona s/f.

QUINTANO RIPOLLÉS, Antonio, *Tratado de la parte especial de derecho penal*, editorial Madrid, 1972.

QUINTERO DE PRIETO, Beatriz, "La legitimación en la causa", en *Revista de Estudios Procesales*, nº 36 (mayo/1983), Rubinzal Culzoni, Santa Fe..

QUIROGA LAVIÉ, Humberto, *Constitución de la Nación Argentina comentada*, Zavalía, Buenos Aires, 2000 (3ª ed.), pp. 134 y ss.

QUIROGA LAVIÉ, Humberto, *El amparo colectivo*, Rubinzal Culzoni, Buenos Aires / Santa Fe, 1998.

RABASA, Emilio, *El derecho angloamericano*. Estudio expositivo y comparado del Common law, Porrúa, México, 1982.

RAMOS MÉNDEZ, Francisco, *Derecho Procesal Civil*, Tomo I, Bosch, Barcelona, 1990 (4ª ed.).

——, *Derecho y Proceso,* Bosch, Barcelona, 1979.

——, *El Sistema Procesal Español*, Bosch, Barcelona, 2000.

——, *Guía para una trancisión ordenada a la LEC*, Bosch, Barcelona, 2000.

——, RAMOS NUÑEZ, Carlos, *Codificación, tecnología y posmodernidad (La muerte de un paradigma)*, Ara, Lima, 1996.

RAMOS ROMEU, Francisco, *Las medidas cautelares civiles*, Atelier, Barcelona, 2006.

RAMOS, Miguel Ángel, "La seguridad y la confidencialidad de la información y la LORTAD", en Revista *Informática y Derecho* números 6/7, UNED, Mérida (España), 1994.

RÁNGEL HERNÁNDEZ Laura, "La acción de inconstitucionalidad por omisión legislativa en la Constitución mexicana. Un avance en el acceso a la justicia constitucional", *Revista Cuestiones Constitucionales* nº 18, Instituto de Investigaciones Jurídicas (UNAM) – Porrua, México, 2008.

RAWLS, John, "Justice as fairness: Political not Metaphisical" (Justicia como imparcialidad: política no metafísica), en *Politicial and Public Affairs*, vol.14, nº 3, 1985, p. 230. También en *Teoría de la justicia*, Fondo de Cultura Económica, México, 1979.

REDENTI, Enrico, *Derecho Procesal Civil*, tomo I, Ejea, Buenos Aires, 1957.

REIMUNDÍN, Ricardo, *Los conceptos de pretensión y acción en la doctrina actual*, Víctor P. de Zavalía, Buenos Aires, 1966.

REY CANTOR, Ernesto, "Acción popular de inconstitucionalidad", *Revista Iberoamericana de Derecho Procesal Constitucional* nº 1, enero/junio 2004, Porrúa, pp. 118 y ss.

——, *Introducción al Derecho Procesal Constitucional*, Universidad Libre, Seccional Cali, 1994.

REYES REYES, Pablo Enrique, *La acción de inconstitucionalidad*, Oxford University Press, México, 2000.

RIASCOS GÓMEZ, Libardo Orlando, "La visión constitucional del *habeas data*", *Revista Informática Jurídica* nº año 2009 (segundo semestre), versión online.

RIBA TREPAT, Cristina, *La eficacia temporal del proceso. El juicio sin dilaciones indebidas*. Bosch, Barcelona, 1997.

RIVAS, Adolfo Armando, *Amparo*, La Rocca, Buenos Aires, 1987.

——, "La acción declarativa de inconstitucionalidad", *La Ley*, 2001-E, 1097.

RIVERA SANTIVAÑEZ, José Antonio, "El amparo constitucional en Bolivia", *El Derecho de Amparo en el mundo* (FIX ZAMUDIO, Héctor, FERRER MAC GREGOR, Eduardo, coordinadores).

RIVERA, Julio César, "Derecho a la intimidad", en *Derecho de Daños*, libro homenaje a Jorge Mosset Iturrapse, La Rocca, Buenos Aires, 1991.

ROA ORTIZ, Emmanuel, *Tratados internacionales y control previo de constitucionalidad*, Ponencias presentadas en el IV Congreso Nacional de Derecho Constitucional, Instituto de Investigaciones Jurídicas (UNAM), 2001, passim.

ROCCO, Alfredo, *La sentencia civil*, traducción Ovejero, México,1945.

RODRÍGUEZ DOMÍNGUEZ, Elvito A., *Derecho Procesal Constitucional*, Grijley, Lima, 1997.

——, "Derecho Procesal Constitucional Peruano", en *Notarius* (Revista de Notarios de Lima, Perú), año 2, Lima, 1991, pp. 265/272.

——, *Manual de Derecho Procesal Constitucional*, Grijley, Lima, 2006 (3ª edición).

RODRÍGUEZ RUIZ, María Carolina, *La acción de cumplimiento en Colombia y Perú*, ponencia presentada en el Curso Superior "Constitución y Derechos Humanos", organizado por la Universidad Antenor Orrego, Trujillo, Perú, en noviembre de 1998.

ROLLA, Giancarlo, *Derechos fundamentales, Estado democrático y justicia constitucional*, UNAM, México, 2002.

RONDÓN DE SANSÓ, Hildegard, *Amparo Constitucional*, Arte, Caracas, 1988.

ROSATTI, Horacio D., *El derecho a la jurisdicción antes del proceso*, Depalma, Buenos Aires, 1984.

ROSENBERG, Leo, *Derecho Procesal Civil*, tomo I, Ejea, Buenos Aires, 1955.

——, *La carga de la prueba*, traducción de Ernesto Krotoschin, Julio César Faira editor, Montevideo (2ª ed.), 2002.

——, "Las sentencias declarativas", *Revista de Derecho Procesal*, 1947 I parte, Año V, p. 562.

ROSSI Edgardo, *La acción de inconstitucionalidad en la Provincia del Chaco*, UNNE, Corrientes, 1997.

RUIZ LANCINA, María José, *La motivación de las sentencias en la nueva Ley de Enjuiciamiento Civil española", Noticias Jurídicas,* página web, 2002.

RUIZ MARTÍNEZ, Esteban, Los informes comerciales y el derecho a la información, Ábaco, Buenos Aires, 2000.

RUIZ MIGUEL, Carlos, "Crítica de la llamada inconstitucionalidad por omisión", en *Revista Iberoamericana de Derecho Procesal Constitucional*, nº 2, julio/diciembre 2004, Porrúa, México, pp. 159 y ss.

SABSAY, Daniel A., *Constitución de la Nación Argentina* (Sabsay, Daniel, Director- Manili, Pablo L., coordinador), tomo I, Hammurabi, Buenos Aires, 2009.

SÁCHICA, Luis Carlos, *La Corte Constitucional y su jurisdicción*, Temis, Bogotá, 1993.

SACRISTÁN, Estela B., "El legitimado pasivo en las acciones declarativas de inconstitucionalidad (El problema de la llamada relación sustancial)", *La Ley*, 2002-E, 351.

SÁENZ DÁVALOS, Luis R., "El proceso constitucional de Amparo", en *Introducción a los procesos constitucionales* (autores: CASTAÑEDA OTSU, Susana, CARPIO MARCOS, Edgar ,ESPINOSA SALDAÑA, Eloy y el citado al comienzo), Jurista, Lima, 2005.

SAGÜÉS, María Sofía, "Garantías de Control de la inconstitucionalidad por omisión", en *Derecho Procesal Constitucional*, coordinado por Eduardo Ferrer Mac-Gregor, tomo IV (pp. 3087 y

ss.), Porrúa-Colegio de Secretarios de la Corte Suprema de Justicia de la Nación, México, 2003.

SAGÜÉS, NÉSTOR Pedro, SERRA, María Mercedes, *Derecho Procesal Constitucional de la provincia de Santa Fe*, Rubinzal Culzoni, Buenos Aaires / Santa Fe, 1998.

SAGÜÉS, Néstor Pedro,Amparo, "*Habeas data* y *habeas corpus* en la reforma constitucional", *La Ley*, 1994-D, 1151 y ss.

——, *Compendio de Derecho Procesal Constitucional*, Astrea, Buenos Aires, 2009.

——, "Constitucionalidad de la apelación 'per saltum', *La Ley*, 1989-B, 318.

——, *Derecho Procesal Constitucional, Recurso Extraordinario*, tomo I, Astrea, Buenos Aires, 1992 (3ª ed.).

——, *Derecho Procesal Constitucional, Acción de Amparo-*, Astrea, Buenos Aires, 1995.

——, "El 'writ of certiorari' argentino (Las reformas de la ley 23.774, respecto al recurso extraordinario)", *La Ley*, 1990-C, 717.

——, *Habeas corpus*, Astrea, Buenos Aires, 1988.

——, "Inconstitucionalidad por omisión de los poderes legislativo y ejecutivo. Su control judicial", en *ED*, 124-865 y ss.

——, "Novedades sobre inconstitucionalidad por omisión: La Corte Constitucional de Ecuador como legislador suplente y precario", *Estudios Constitucionales*, Año 7, N° 2, 2009, pp. 71-79.

——, *Subtipos de habeas data*, J.A., 20/12/95, pp. 2 y ss.

SAHAB, Ricardo J., *El recurso extraordinario por gravedad institucional*, Ediar, 1978, p. 34.

SAIX, Edgardo Ignacio, "Acceso a la tutela de los derechos de incidencia colectiva dentro del nuevo texto constitucional", en Revista de Derecho Privado y Comunitario, nº 7, 1994, pp. 117 y ss.

SAJA, Francesco, "L´efficacia nel tempo delle sentenze di accoglimento", en *Quaderni Costituzionali*, Anno IX nº 1, Aprile 1989, pp. 7 y ss.

SALOM, Jaiver Aparicio, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Aranzadi. Pamplona, 2000.

SÁNCHEZ BRAVO, Álvaro, "La regulación de los datos sensibles en la Lortad", en *Revista Informática y Derecho*, números 6/7, UNED, Mérida, 19947.

SATTA, Salvatore, "Soliloquios y coloquios de un jurista", en *Derecho Procesal Civil*, tomo III, Ejea, Buenos Aires, 1971.

SAVIGNY, Federico Carlos de, *Sistema de derecho romano actual*, traducción de Mesia y Poley, Tomo I, Góngora, Madrid.

SCHEIBLER, Guillermo, "Apuntes sobre autonomía, participación y legitimación en el amparo porteño", en *Amparo en la Ciudad Autónoma de Buenos Aires*" (Daniela, Mabel, directora-), Platense, La Plata, y en la revista *La Ley Ciudad Autónoma de Buenos Aires*, Año 1, Nº 1, Agosto 2008.

SCHMITT, Carl, *La Defensa de la Constitución*, traducido por Manuel Sánchez Sarto, prólogo de Pedro de Vega García, Tecnos, Madrid, 1983..

SCHÖNKE., Adolfo, *Derecho Procesal Civil*, Bosch, Barcelona, 1950.

SENTÍS MELENDO, Santiago, "El juicio de jactancia", *Revista de Derecho Procesal*, 1943-II, pp. 123 y ss.

SERRA DOMÍNGUEZ, Manuel, *Estudios de derecho procesal*, Ariel, Barcelona, 1969.

SERRA, María Mercedes, *Procesos y recursos constitucionales*, Depalma, Buenos Aires, 1992.

SERRANO MIGALLÓN, Fernando, "Jurisdicción constitucional y política", en *La ciencia del derecho procesal constitucional. Estudios en homenaje a Héctor Fix Zamudio*, tomo I (Teoría General del derecho procesal constitucional), passim.

SILGUERO ESTAGNAN, Joaquín, *La tutela jurisdiccional de los intereses colectivos a través de la legitimación de los grupos*, Dykinson, Madrid, 1995.

SILVA MELERO, Valentín, "La prueba procesal", *Revista de Derecho Privado*, Madrid, 1963-1, p. 93.

SILVERO SALGUEIRO, Jorge, "La Constitución de la República del Paraguay de 1992", *Boletín Mexicano de Derecho Comparado* n° 92 (Mayo – Agosto), 1998.

SLANE, Bruce, *Publicación masiva de registros públicos: una perspectiva Neozelandesa*, en "XX Conferencia Internacional de autoridades de protección de datos" (1998), Agencia de Protección de Datos, Madrid, 1999.

SOBERANES DIEZ, José María, "La suspensión en controversias constitucionales respecto de resoluciones no definitivas", *Revista Cuestiones Constitucionales* n° 15, Instituto de Investigaciones Jurídicas, UNAM, México, 2006, p. 333.

SOLÉ RIERA, Jaume, *El recurso de apelación civil*, Bosch, Barcelona, 1998 (2ª edición).

SOSA, Gualberto Lucas, Mancuso, Francisco, "El absurdo en la jurisprudencia de la Suprema Corte de la provincia de Buenos Aires", en *Temas de casación y recursos extraordinarios*, Platense, La Plata, 1982, pp. 265 y ss.

SUÁREZ CAMACHO, Humberto, MORTERA DÍAZ, Antonio Rodrigo, "Reflexiones en torno a la controversia constitucional", *Revista Cuestiones Constitucionales*, n° 17, Instituto de Investigaciones Jurídicas, UNAM, México, 2007, pp. 233 y ss.

TARUFFO, Michele, El vértice ambiguo. Ensayos sobre la Casación Civil, Biblioteca de Derecho Procesal nº 2, colección dirigida por Juan Monroy Gálvez y Juan José Monroy Palacios, Palestra, Lima, 2005, pp. 156/157).

TARUFFO, Michelle, "La giutificazione delle decisión fondate su standards", en *L´Analisi del racionamiento giuridico*, dir. Comanducci, P., Guastini, R., Giappichelli, Torino, 1989.

TAWIL, Guido Santiago, "El recurso extraordinario y las decisiones emitidas por la Administración en ejercicio de funciones materialmente jurisdiccionales", *La Ley*, 1990-E, 908, Derecho Constitucional, Doctrinas Esenciales, Tomo IV, p. 725.

TOCQUEVILLE, Alexis de, *La democracia en América*, Sarpe, Madrid, 1984.

TONIATTI, Roberto, *Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada*, en R.V.A.P. nº 29, 1991, pp. 65 y ss.

TOURAINE, Alain, "Seis hipótesis sobre América Latina", en *Revista de Derecho del Mercosur*, año 1, nº 1, 1997, La Ley, p. 44.

TROPER, Michel, "Del gobierno de los jueces al gobierno por los jueces", traducción de Bernardo Bolaños, en *Jueces y Derechos* (Problemas contemporáneos), Porrúa – UNAM, México, 2004

TULA, María Inés, SOLANO, Mauro, "La difusión de las afiliaciones partidarias frente al derecho de la privacidad", *La Ley Actualidad*, del 6 de septiembre de 2005, p. 1

UICICH, Rodolfo Daniel, *Los bancos de datos y el derecho a la intimidad*, Ad Hoc, Buenos Aires, 1999.

VALLESPÍN PÉREZ, David, *El modelo constitucional de juicio justo en el ámbito del proceso civil*, Atelier, Barcelona, 2002.

VÁZQUEZ ARZAGUET, Gabriel A., MIGHETTI, Carlos M., *Secreto financiero*, Depalma, Buenos Aires, 1999.

VELASCO SAN MARTÍN, Cristos, "Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México?", *Boletín de Política Informática* nº 1, México, 2003, pp. 1 y ss.

VELÁZQUEZ BAUTISTA, Rafael, *Protección jurídica de datos personales automatizados*, Colex, Madrid, 1993

VERBIC, Francisco, *Procesos Colectivos*, Astrea, Buenos Aires, 2007.

VERDAGUER, Alejandro, *La acción de inconstitucionalidad en la Ciudad de Buenos Aires*, Astrea, 2001, documentado rescatado de la página web de la editorial).

VERGARA MESA, Hernán Darío, *Los condicionantes de la acción de cumplimiento, Estudios de Derecho*, Vol. LXIV. Nº 143, junio 2007, p. 242.; Facultad de Derecho y Ciencias Políticas. Universidad de Antioquia. Medellín. Colombia.

VÉSCOVI, Enrique, *Elementos para una teoría general del proceso civil latinoamericano*, UNAM, México, 1978.

VICENTE Y CARAVANTES, José, *Tratado histórico, crítico y filosófico de la ley de enjuiciamiento*, Tomo II, Gaspar y Roig, Madrid, 1856.

VIDAL MARÍN, Tomás, "Derecho al honor, persona jurídica y Tribunal Constitucional", Indret, *Revista para el análisis del derecho*, Barcelona, 2007.

VIGORITI, Vicenzo, "Interessi colletivi e processo. La legitimazione ad agire, Giuffré, Milano, 1979. I diritti constituzionali delle parti nel processo civile italiano", *Revista de Derecho Procesal* (Italia) 1971, p. 622.

VOLTAIRE, "Pensamientos sobre la Administración Pública", en *Opúsculos satíricos y filosóficos*, Alfaguara, Madrid, 1978.

VON BÜLOW, Oskar, *La teoría de las excepciones procesales y los presupuestos procesales*, Ejea, Buenos Aires., 1964.

WACH Adolf, *La pretensión de declaración*, traducción de Juan M. Semon, Ejea, Buenos Aires, 1962. *Manual de Derecho Procesal Civil*, Ejea, Buenos Aires, 1962.

ZAFFARONI, Eugenio Raúl, *Dimensión política de un Poder Judicial democrático, en Jueces y Derecho*, compiladores: Miguel Carbonell, Héctor Fix Fierro y Rodolfo Vázquez.

ZAGREBELSKY, Gustavo *¿Derecho Procesal Constitucional?,* cit., p. 402. Esta obra se encuentra también editada como *¿Derecho procesal constitucional?* y otros ensayos de justicia constitucional, Fundap, Querétaro, 2004.

——, "¿Derecho Procesal Constitucional?", traducción de Giovanni F. Priori Posada, en *Revista Peruana de Derecho Procesal*, nº IV, dirigida por Juan José Monroy Palacios, Lima, diciembre/2001, pp. 400 y ss. También del autor: *El derecho dúctil*, 4ª edición, Trotta, Madrid.

——, *El derecho dúctil*, Trotta, Madrid, 2002 (4ª edición).

ZALDIVAR LELO DE LARREA, Arturo, *Hacia una nueva ley de amparo*, Instituto de Investigaciones Jurídicas, UNAM, 2002.

ZANNONI, Eduardo A., *Derecho subjetivo e interés simple en la responsabilidad civil, en la obra conjunta de homenaje a Isidoro H. Goldenberg, La responsabilidad*, Abeledo Perrot, Buenos Aires, 1995.

ZAVALA DE GONZÁLEZ, Matilde, "La Tutela Inhibitoria contra Daños", en *Revista de Responsabilidad Civil y Seguros*, nº 1, La Ley, 1999.

ZELA VILLEGAS, Aldo, *La tutela preventiva de los derechos*, Palestra, Lima, 2008.

ZUÑIGA URBINA, Francisco, "La acción de inaplicabilidad por inconstitucionalidad" en Chile, en *Derecho Procesal Constitucional Americano y Europeo*, Tomo II (obra coordinada por Víctor Bazán), Abeledo Perrot, Buenos Aires, 2010.

1636 blanca