Ius et Praxis
ISSN: 0717-2877
revista-praxis@utalca.cl
Universidad de Talca
Chile

Cerda Silva, Alberto
Mecanismos de Control en la Protección de Datos en Europa
Ius et Praxis, vol. 12, núm. 2, 2006, pp. 221- 251
Universidad de Talca
Talca, Chile

Mecanismos de Control en la Protección de Datos en Europa
Alberto Cerda Silva
páginas 221 - 251

MECANISMOS DE CONTROL EN LA PROTECCIÓN DE DATOS EN EUROPA

Alberto Cerda Silva *

RESUMEN

El artículo considera los diversos elementos sobre los cuales se ha producido aproximación normativa en materia de protección de las personas frente al tratamiento de los datos personales que es conciernen, tales como el ámbito de aplicación de las leyes sobre datos personales, los principios rectores de la normativa, los derechos que se confieren al titular de datos y la responsabilidad originada en el tratamiento de tales datos. Enseguida, el artículo profundiza en la precisión de los diversos mecanismos de control adoptados en Europa, para concluir en que el reconocimiento y promoción de mecanismos de autocontrol no garantizan la obtención de un nivel de protección adecuado en la materia, de ahí la necesidad de disponer de una autoridad de control, un organismo público encargado de promover e informar a la comunidad sobre la legislación aplicable al tratamiento de datos personales, fiscalizar el cumplimiento de la normativa y sancionar su infracción, o bien instar por la sanción del infractor, en su caso. Tal institucionalidad contribuye a la efectiva implementación de una política pública coherente con un Estado democrático que promueve las condiciones que garantizan el pleno desarrollo de las personas.

* Abogado y Magíster en Derecho Público por la Universidad de Chile.
Profesor Asistente de Derecho Informático e Investigador de Centro de Estudios en Derecho Informático de la Universidad de Chile. Es, además, Asesor Jurídico de la Corporación Administrativa del Poder Judicial - Corte Suprema, en relación con la implementación de los tribunales de familia y sistemas de litigación electrónica para los juzgados de cobranza laboral y previsional, y los nuevos juzgados del trabajo. Correo electrónico: acerda@uchile.cl. Presentado el 31 de agosto y aprobada su publicación el 2 de octubre.

PALABRAS CLAVES

Datos personales; Derecho informático; Protección de datos; Tratamiento de datos; Vida privada.

ABSTRACT

The article considers the diverse elements on which the normative approach in the matter of public protection, processing of personal data-such as the scope of the application of the law, the governing principles of the norm, the rights conferred to the data subject and the responsibility initiated in the process of the data have taken place. Immediately, the article digs deeper into the diverse mechanisms of control adopted in Europe, concluding that the recognition and promotion of self-control mechanisms do not guarantee an adequate level of protection. Therefore it is necessary to make a control authority available; a public organism which will promote and inform the community about the appropriate legislation of personal data processing; to control the completion of the norm and to sanction its infraction, or rather to insist on the sanction of the transgressor. Such institutions contribute to the effective implementation of a coherent public policy on a democratic state that promotes the conditions guaranteeing the total development of the people.

KEYWORDS

Personal data; Cyber Law; Data protection; Data processing; Privacy.

I.- EL RÉGIMEN JURÍDICO DE LA PROTECCIÓN DE DATOS EN EUROPA

La protección de los datos personales, a través de un adecuado marco jurídico que reglamente su tratamiento ha constituido un asunto central en la agenda normativa europea desde comienzos de la década de los setenta, cuando sólo algunos de sus Estados disponían de leyes específicas en la materia.

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.

Los progresos habidos en la informática y la creciente capacidad de almacenamiento de información, dieron lugar a una nueva generación de leyes, que fijaron menos trabas para la constitución de bases de datos, pero, en contrapartida, confirieron un abanico de facultades al titular de los datos a fin de velar por aquellos que le conciernen: información, acceso, rectificación y cancelación. Además, en ellas existe una preocupación adicional por brindar garantía ante el tratamiento de los denominados "datos sensibles", aquellos que por su naturaleza suponen un riesgo en su tratamiento, ya sea porque lesionan la intimidad de la persona, o bien porque le exponen a prácticas discriminatorias. Es el caso de 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.

Sin embargo, el correr de los años evidenció la necesidad de aproximar las experiencias legislativas, con miras a obtener un adecuado nivel de protección de los derechos fundamentales de las personas y, a la vez, concretar la libre circulación de bienes, personas y servicios en el mercado común. En efecto, la necesidad de disponer de una normativa comunitaria en la materia venía siendo sostenida por el Parlamento Europeo desde 1973, cuando se instó al Consejo a explicar si contaba con alguna política al respecto y en 1974 el mismo Parlamento elaboró un estudio que proponía el diseño de una Directiva en la materia.

Tal proceso de aproximación normativa se concreta inicialmente con el Convenio 108 adoptado por la Comunidad Económica Europea en 1981, primer instrumento internacional que procura reglar el fenómeno del tratamiento automatizado de datos correspondientes a personas naturales desde una perspectiva que trasciende a la legislación interna y cuyo contenido informará diversas legislaciones europeas originadas durante la década de los ochenta, con miras a disponer de una normativa comunitaria para hacer frente a una previsible proliferación de leyes nacionales que en su día hicieran difícil su armonización.[1]

El ámbito de aplicación del Convenio era comprensivo del procesamiento de datos –desde su almacenamiento hasta borrado inclusive– verificado en el sector público y privado, con tal que él se refiriese a personas naturales y fuese realizado por medios informáticos; sin embargo, el Convenio admitía que los Estados miembros facultativamente extendiesen sus disposiciones a agrupaciones de personas con o sin personalidad jurídica, así como a los datos personales que fueren objeto de tratamiento no automatizado.

El Convenio también se ocupa del flujo internacional de datos de carácter personal, abogando por disponer de una *"protección equivalente"* en la legislación aplicable a quienes participan de la transmisión, a efectos de evitar que se soslaye la aplicación de la normativa de los Estados partes. De igual modo, el Convenio presta especial atención al auxilio mutuo que impone a los Estados signatarios, para cuyos efectos supone la existencia de una o varias autoridades en el derecho interno de cada uno de ellos, las que encausan la cooperación institucional entre las partes, así como la asistencia en el ejercicio de sus derechos a los interesados residentes en el extranjero.

Los Estados partes del Convenio se obligaban a adoptar en su derecho interno las medidas necesarias para dar efecto a los principios fundamentales de protección de datos a que adscribía el instrumento. Así sucedió con la *Data Protection Act de 1984* adoptada por Reino Unido, así como con la *Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD)*, adoptada por España en 1992, que constituiría la piedra angular sobre la cual se diseñó nuestra Ley 19.628, e igualmente con la Ley de Datos de la República Federal Alemana de 1990, que cuenta con un largo trabajo preparatorio que trae por causa la declaración de inconstitucionalidad de la Ley de Censo de Población de 1982.

Sin embargo, con el transcurso del tiempo la eficacia del Convenio se fue agotando, pues hasta entrada la década de los noventa no hubo nuevas ratificaciones y sólo se adoptaron

[1] Convenio de 28 de enero de 1981, del Consejo de Europa para la protección de las personas en lo referente al tratamiento automatizado de los datos personales.

tres nuevas leyes nacionales en la materia. Por otro lado, su sola ratificación no mostraba eficacia alguna, tal como sucedía con España que, pese a haber ratificado en 1984, no procuró trasponer las normas del Convenio a su legislación interna sino hasta 1992. Estimando pues la Comisión del Parlamento Europeo que tal instrumento resultaba poco coactivo, habiéndose dilucidado las dudas preexistentes por lo concerniente a la competencia de la Comunidad en la materia y visualizándose la concreción de un mercado interior con el consiguiente incremento en la circulación de los datos personales en su seno, la Unión Europea adopta la Directiva 95/46/CE.[2]

La Directiva 95/46/CE 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. No obstante, si bien la Directiva establece condiciones generales de licitud en el tratamiento de los datos, deja a los Estados miembros un margen de maniobra de que podrán servirse para precisar en el derecho interno tales condiciones. Al efecto, se establece un plazo de tres años para la transposición de sus previsiones en el derecho interno por los Estados miembros.

El proceso de implementación en el derecho interno de los Estados miembros dio lugar a intensos procesos legislativos que cristalizaron en la adopción de nuevas leyes en la materia: en Italia, la *Ley 675 de 1996 sobre la tutela de las personas y otros sujetos respecto al tratamiento de datos personales*; en Suecia, la nueva *Ley 1998/204 sobre Protección de Datos de Carácter Personal*; en Reino Unido, la *Data Protection Act de 1998;* en España, *Ley de Protección de Datos de Carácter Personal de 1999*, por mencionar algunas.

A la fecha, tras la reciente adopción de una nueva ley por Irlanda y las modificaciones introducidas por Francia en su normativa, todos los estados miembros han adecuado su derecho interno a las exigencias de la Directiva; ello ha permitido alcanzar un notable grado de homogeneización, aun cuando la normativa de cada Estado guarda peculiaridades que la propia Directiva tolera, al admitir un margen de maniobra en la transposición de sus disposiciones al derecho interno. Tal aproximación normativa no ha alcanzado sólo a los Estados miembros de la Unión Europea, sino también a los países candidatos a integrar la misma, los que, de conformidad con los criterios de Copenhague, están comprometidos a transponer la Directiva con antelación a su adhesión. Inclusive más, los efectos reflejos de la Directiva se proyectan a otras latitudes, en este sentido es notable su impronta en la *Ley 25.326 sobre Protección de los Datos Personales* aprobada el 2001 en la Argentina.

[2] Directiva 95/46/EC del Parlamento Europeo y el Consejo de 24 de Octubre de 1995 relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La Comisión ha evacuado un primer informe sobre la transposición de la Directiva, basado en una amplia consulta efectuada durante 2002, el cual arriba a la conclusión que tal instrumento ha logrado asegurar una fuerte protección hacia los datos personales movidos en la Unión. Sin embargo, los retrasos en la transposición por ciertos Estados miembros y las diferencias observadas en la aplicación de ciertas previsiones –en particular aquellas relativas a derecho aplicable, suministro de información a los interesados, notificación a autoridades de control, entre otros– han evitado que la economía de Europa consiga las ventajas a que apunta la Directiva. Para hacer frente a ellas, el informe propone un plan de trabajo destinado a reducir esas diferencias, basadas en la cooperación entre Estados miembros y la propia Comisión.[3]

Actualmente, disponen de leyes específicas relativas al tratamiento de datos personales la totalidad de los Estados miembros de la Unión Europea, así como los países candidatos de la misma. Sin embargo, la protección de los derechos que se confieren al titular de los datos personales en Europa no se ha detenido en el marco legislativo y progresivamente ha cobrado carta de ciudadanía en diversas Constituciones y aún ha merecido un sitial en la reciente Carta de Derechos Fundamentales de la Unión Europea.[4]

En efecto, una de las primeras constituciones en reconocer a los ciudadanos derechos respecto de la información contenida en registros o bases de datos fue la de Portugal de 1976, cuyo contenido fue ampliado en la modificación introducida a la misma en 1989. Otras revisiones constitucionales o nuevas cartas fundamentales han hecho igual, reconociendo la protección de los derechos que corresponden a las personas frente al tratamiento de sus datos personales, sea asociado o no al derecho a la vida privada; es el caso, entre otras, de la Constitución de España de 1978, de los Países Bajos de 1983, de Hungría de 1989, de Suecia de 1993 y de Finlandia de 1999.

Por su parte, la Carta de Derechos Fundamentales de la Unión Europea, después de asegurar en su artículo 7 el derecho a la vida privada, consagra, como categoría autónoma, la protección de los datos de carácter personal, en los siguientes términos:

> *"... la Unión reconoce los derechos, libertades y principios enunciados a continuación.*
>
> *Artículo 8. Protección de los bienes de carácter personal*

[3] Cf. Comisión de las Comunidades Europeas, "Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)", Bruselas, 15 de mayo de 2003; y, también, "Analysis and impact study on the implementation of Directive EC 95/46 in Member States".

[4] Carta de Derechos Fundamentales de la Unión Europea, proclamada por el Parlamento Europeo, el Consejo y la Comisión, en Niza el 7 de diciembre de 2000.

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

Del mismo modo, la doctrina y la jurisprudencia progresivamente han reconocido la existencia de un derecho específico en relación con la protección de las personas ante el tratamiento de los datos personales que les conciernen. Corresponde al Tribunal Constitucional Alemán el esbozo de este denominado derecho a la autodeterminación informativa, con motivo del pronunciamiento sobre la Ley de Censo de Población de 1982.[5] Lo propio aconteció en la jurisprudencia del Tribunal Constitucional de España.[6] En doctrina, se alude a este derecho como "*autodeterminación informativa*" o "*libertad informativa*".[7]

En lo que sigue consideraremos el régimen jurídico aplicable al tratamiento de datos personales a la luz de las previsiones de la Directiva comunitaria, en atención a la aproximación normativa producida entre los Estados miembros y candidatos de la Unión Europea urdida en torno a la misma: el ámbito de aplicación, los principios informadores, los derechos irrogados

---

5 Vid. Tribunal Constitucional Alemán, sentencia de 15 de diciembre de 1983, publicada en *BJC Boletín de Jurisprudencia Constitucional*, núm. 33, Enero 1984, Publicaciones de las Cortes Generales, Madrid. Trad. Manuel Daranas. pp. 126 – 170.

6 Cabe destacar los siguientes pronunciamientos del Tribunal Constitucional de España, sentencia 254/1993, de 20 de julio de 1993 y sentencia 124/1998, de 15 de junio de 1998. Este pronunciamiento, con matices, se encuentra en las sentencias 11/1998, de 13 de enero de 1998 y 105/1998, de 18 de mayo de 1998.

7 Vid., entre otros, Frossini, Vittorio. "Los derechos humanos en la sociedad tecnológica", en *Anuario de Derechos Humanos*, núm. 2, 1983, pp. 101 – 115; Pérez-Luño, Antonio, "Los Derechos Humanos en la Sociedad Tecnológica", en *Cuadernos y Debates*, Nº21, Centro de Estudios Constitucionales, Madrid, 1989, pp. 133 – 213; Lucas Murillo de la Cueva, Pablo, **"El Derecho a la Autodeterminación Informativa. La Protección de los Datos Personales frente a la Informática"**, Ed. Tecnos. Madrid, 1990, passim; Hassemer, Winfried y Chirino, Alfredo, **"El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales"**, Ed. Del Puerto, Argentina, 1997. En el mismo sentido, Del Rey Guanter, Salvador. "Tratamiento automatizado de datos de carácter personal y contrato de trabajo", en *Relaciones Laborales*, t. II/1993, p. 141, y Fernández Villazón, Luis Antonio, "Tratamiento automatizado de datos personales en los procesos de selección de trabajadores" en *Relaciones Laborales*, t. I/1994, pp. 535 – 536. Por su parte, entre nosotros, es de la opinión que el enfoque de la autodeterminación informativa es complementario a la configuración del derecho al respeto de la vida privada, Noguera Alcalá, Humberto, **"El derecho a la libertad de opinión e información y sus límites"**, Lexis-Nexis, Chile, 2002, pp.152 – 153. Por la autodeterminación informativa, vid. Cerda Silva, Alberto, "Autodeterminación Informativa y Leyes sobre Protección de Datos", en *Revista Chilena de Derecho Informático*, núm. 3, 2003, pp. 47 – 75.

al titular de datos y las normas sobre responsabilidad en la materia, para posteriormente revisar los mecanismos de control de que se sirve el sistema para resguardar el cumplimiento de la normativa. Con todo, considerando el tantas veces mencionado *"margen de maniobra"* que la propia Directiva confiere a los Estados para la transposición de sus disposiciones en el derecho interno, consignaremos, en cuanto resulte pertinente, aquellos matices que puedan ser relevantes.

1.- Ámbito de aplicación

Mientras las primeras leyes sobre la materia circunscribían sus efectos al tratamiento automatizado de datos personales correspondientes a personas naturales verificado por organismos del sector público, actualmente, la totalidad de las legislaciones de los países miembros y candidatos de la Unión Europea extienden su ámbito al tratamiento de datos realizados por medios informáticos y manuales, ya sea por entidades del sector público o privado, e inclusive son varios los países que han extendido sus previsiones al tratamiento de aquellos datos referentes a personas jurídicas, como acontece con Italia y Dinamarca.

En cuanto al ámbito de aplicación de la Directiva, nos parece del caso destacar que sus pretensiones son generales, en el sentido de ser aplicable cualquiera sea el contexto en que se verifique tratamiento de datos personales, cualquiera sea el tipo de operaciones que recaiga sobre ellos y con prescindencia de la naturaleza de la entidad responsable del tal tratamiento. Lo que en doctrina se denomina una técnica legislativa *omni bus*, mediante la cual se pretende extender la protección a la persona concernida por los datos cualquiera sea la hipótesis en que el tratamiento de ellos tiene lugar, por oposición a una técnica legislativa *by sector*, en la cual se genera normativa específica para ser aplicada tan sólo a las concretas circunstancias en que tiene lugar el procesamiento de datos.

Sin embargo, la abstracción y generalidad que supone una normativa del tipo *omni bus*, tal como sucede con la Directiva, ha evidenciado ciertas falencias a la hora de interpretar y aplicar sus previsiones a contextos específicos en los cuales se realiza tratamiento de datos; aún cuando unos mismos sean los principios y derechos reconocidos legalmente, parece no ser similar las condiciones en que se verifica tratamiento de datos para fines de marketing, para efectos de prestaciones de salud o con motivo de una relación de carácter laboral. Ello ha dado lugar, a nivel comunitario e igualmente en el derecho interno de los Estados miembros de la Unión Europea, a la adopción de normativas específicas relativa al tratamiento de datos personales para determinados fines.

En efecto, así, por ejemplo, ante la evolución tecnológica, la Unión Europea ha adoptado la Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, que sirviéndose de los principios desarrollados por la Directiva 95/46/CE les ha especificado para el sector de las telecomunicaciones; aquélla

ha sido actualizada por la Directiva 2002/58/CE, relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas, mediante la cual se ha pretendido recoger la evolución de los mercados y tecnologías de servicios de comunicación electrónica, como Internet, con el fin de ofrecer el mismo nivel de protección de los datos personales y la intimidad para todas las tecnologías utilizadas.[8]

Por otro lado, siempre en cuanto a la transposición de las previsiones generales de la Directiva a contextos específicos en que se verifica tratamiento de datos, la Comisión ha estimado que, ante la intensificación de la recogida de datos personales de los trabajadores en relación con el empleo, pueda resultar oportuno tomar como base los principios generales ya existentes de la Directiva y aportando a dichos principios complementos y aclaraciones para adaptarlos al contexto laboral. Una decisión definitiva sobre el particular ha sido pospuesta por la Comisión. Sobre el punto, nos parece del caso consignar que las dificultades que representa el tratamiento de datos de las personas en el contexto de una relación de trabajo y ante la insuficiencia de las leyes generales de carácter nacional, se ha dado pie a la adopción de disposiciones legales específicas en Finlandia y otro tanto se considera actualmente en Suecia; el tema ha sido también considerado por las autoridades de control de Italia y Francia, así como por los tribunales de España.

En el mismo sentido, la propuesta de Directiva del Parlamento Europeo y del Consejo, relativa a la armonización de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de crédito a los consumidores, la Comisión ha establecido disposiciones específicas sobre protección de datos en la materia, cuyo objetivo es reforzar aún más la protección de los consumidores.

2.- Principios Informativos

El afán del Convenio 108 por introducir un nivel de protección equivalente entre los Estados partes del mismo, pese al mosaico de diseños jurídicos de Europa, obligó a acudir a principios generales, a la espera de que fuesen los propios Estados signatarios quienes plasmarán apropiadamente los mismos en su legislación interna a la hora de transponer los contenidos del Convenio.

En este sentido, los Estados partes se obligaban a adoptar en su derecho interno las medidas

[8] Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones; y la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas.

necesarias para dar efecto a los principios fundamentales de protección de datos a que adscribía el Convenio, a saber: la calidad de los datos y lealtad en las operaciones de tratamiento sobre ellos; una protección especial hacia clases especiales de datos (datos sensibles), en los cuales se prohibía por principio su tratamiento, salvo excepción y oportunas garantías; la adopción de medidas de seguridad física y lógica respecto de los datos; el reconocimiento de los derechos de información, acceso, rectificación y cancelación; y la garantía de un recurso a favor de quien fuere desestimada una petición formulada en ejercicio de sus derechos.

Posteriormente, la Directiva, al considerar las condiciones generales de tratamiento, insiste en la aplicación de ciertos principios, junto con elevar a tal rango otros tantos que no habían merecido tal reconocimiento. Una breve reseña de los principios asumidos por la Directiva permite identificar los siguientes:

Principio de la licitud y lealtad. La Directiva no impide las operaciones de tratamiento de datos, pero repudia la libertad absoluta al respecto, antes, al contrario, aboga porque él se ajuste a las disposiciones legales vigentes, sin perjuicio de la aplicación del principio general del derecho de la buena fe, que cobra el sentido de un tratamiento leal de los datos personales.

Principio de la calidad de los datos. El tratamiento de los datos personales supone que la información que proporcionan los datos debe representar fielmente la realidad que predican y, a su vez, que ellos deben ser pertinentes, adecuados y no excesivos respecto del ámbito y objetivo para los cuales fueron recogidos. A diferencia de cuanto acontecía con el Convenio 108, la Directiva impone a los responsables de tratamiento la obligación de velar por la exactitud de los datos.

Principio del consentimiento informado del titular de los datos. Al conferir facultades al titular de los datos personales para controlar la información que le concierne, la Directiva ha debido condicionar la legitimidad del tratamiento de sus datos al consentimiento previo, libre e informado prestado por él mismo. Es así como el tratamiento de los datos personales sólo puede efectuarse cuando el titular consienta expresamente en ello, más aún tal persona debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación a terceros. Sin embargo, pese al carácter central que reviste el consentimiento informado de parte del titular de los datos personales como condición para efectuar tratamiento sobre ellos, la propia Directiva ha admitido hipótesis en que es posible prescindir de él, en atención a la naturaleza de la fuente de la cual ha sido tomada la información o de los intereses individuales o sociales estimados prevalecientes.

Principio de la seguridad de los datos. Junto con brindarse ciertas garantías jurídicas, adjetivas y sustantivas, para el efectivo resguardo de los derechos de los titulares de datos personales frente a los riesgos que representa su tratamiento, en especial cuando él es realizado por medios automatizados, suele imponerse por el legislador la adopción por parte del

responsable del banco de datos de medidas de seguridad de diversa índole: físicas, referida a la infraestructura que las resguarda; lógicas, relativas a las precauciones técnicas adoptadas (soporte, acceso, etc.); y, jurídicas, o sea, de índole normativo. La concreción precisa de las medidas necesarias queda entregada a la legislación interna de los Estados miembros de la Unión Europea. En este sentido, mientras unos países, como Francia y España, confieren a la autoridad de control la precisión de las misma, otros, como acontece con Alemania, formulan en la propia ley ciertas previsiones al respecto.

Principio de la confidencialidad de los datos. La Directiva impone a los Estados miembros establecer una obligación de reserva respecto del contenido de la información procesada, la cual recae tanto sobre el responsable del banco, como sobre las personas que intervienen directamente en el tratamiento de los datos, obligación que habitualmente no termina por el hecho de haber concluido tales personas sus actividades en este campo, sino que persiste después de haber cesado en ellas. Asimismo, es frecuente que las legislaciones internas extiendan tal deber a los funcionarios de la autoridad de control que intervienen en las actividades fiscalizadoras de la misma.

Principio del consentimiento para la cesión de datos. Bastante menguados serían los resultados que podrían abrigarse en la protección de los datos personales si se prescindiera del consentimiento del titular al ser transmitidos los datos a terceros, particularmente si a éste no le fuere exigible un tratamiento lícito. En razón de ello, la Directiva adscribe al principio de que toda cesión requiere del consentimiento del interesado, salvo excepciones.

Principio de la finalidad. Si los datos son proporcionados por su titular, autorizando el tratamiento de los mismos con determinados objetivos, estima la Directiva que su uso para fines diversos de aquellos que justificaron su recogida es ilegal, salvo excepción legal en contrario. La doctrina ha relevado el rol de la finalidad, particularmente tratándose de aquellos casos en que la legitimidad del tratamiento ha prescindido del consentimiento del titular de los datos personales. En el mismo sentido, el uso de los datos conforme a su finalidad se ha relevado en términos tales de hacer de él un derecho subjetivo, sosteniéndose que el titular dispone del derecho a un uso conforme a fin de los datos que le conciernen.

Adicionalmente, la Directiva ha contemplado el *principio de especial protección* hacia aquella categoría de datos especialmente reveladores de circunstancias íntimas de su titular o que le exponen a actos de discriminación arbitraria. Se trata de los denominados *datos sensibles.* Es en este sentido la Directiva en principio aboga por la prohibición de su tratamiento, si bien establece un sistema reglado de excepciones, algunas de las cuales ameritan su notificación a la Comisión; además, considera que el tratamiento de datos sensibles requiere el consentimiento explícito de su titular, atendido que por su naturaleza pueden atentar contra las libertades fundamentales o la intimidad de aquél a quien conciernen.

Por su parte, la doctrina, a partir de la constitucionalización e internacionalización de los derechos que la ley irroga al titular de los datos personales, ha esbozado el *principio de derecho fundamental*, en tal sentido es comprendido por la Directiva y como tal se concibe en la Carta de Derechos Fundamentales de la Unión Europea. Como tal, la protección de los datos personales debe comenzar en la ley, no en un nivel normativo inferior, tal como decretos u ordenes administrativas. Aún más importante, el punto de partida para la interpretación de la ley es precisamente la protección de un derecho fundamental o, más bien, de los derechos fundamentales en general.[9]

3.- Derechos del titular de datos personales

En Alemania, la Ley de Datos de 1977 confería ya ciertos derechos al afectado para obtener acceso, rectificación, cancelación o bloqueo de sus datos, según los casos. Sin embargo, tales derechos se encontraban insuficientemente perfilados y el propio texto de ley hacia prevalecer el rol que competía al Comisario Federal de Protección de Datos y a las autoridades de tutela estatal en la protección de los derechos del afectado.

En cambio, a partir de la legislación adoptada en Francia en 1978 se observa un enriquecimiento de los derechos del titular –así, por ejemplo, el derecho a impugnar las decisiones adoptadas exclusivamente sobre la base del tratamiento automatizado de datos personales–, ciertos matices –tales como la posibilidad de ejercer el derecho de acceso por medios indirectos–, y, a la vez, un mayor celo en la precisión de las circunstancias que conducen a la eliminación o modificación de los datos.

Con posterioridad, el Convenio 108 ha brindado reconocimiento a los derechos de información, acceso, rectificación y cancelación, si bien deja su configuración a la normativa adoptada por los Estados partes de él. Igualmente, el Convenio garantiza una acción judicial a favor de quien vea desestimada una petición formulada en ejercicio de sus derechos.

Por su parte, la Directiva ha brindado un amplio reconocimiento a los derechos que habitualmente se confieren a los titulares de datos; de este modo, aparecen reconocidos en ella los siguientes derechos:

- El derecho a información, esto es, a la comunicación al titular de los datos, sea que éstos se recaben de él o de terceros, de un cierto contenido mínimo relativo a las operaciones de tratamiento.

[9] Saarenpää, Ahti. "Europa y la Protección de los Datos Personales", en *Revista Chilena de Derecho Informático*, núm. 3, 2003, pp. 15 – 29.

- El derecho de acceso al interesado, mediante el cual el titular se puede imponer de los datos que le conciernen que son objeto de tratamiento, así como la finalidad del procesamiento y destinatario de sus datos, entre otros. La Directiva proyecta inclusive este derecho al conocimiento de la lógica que subyace al tratamiento automatizado de los datos que conciernen al titular, resguardando el menoscabo al secreto de los negocios, la propiedad intelectual y los derechos de autor.

- 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; sin embargo, la Directiva no precisa los eventos que dan lugar a uno u otro derecho, dejando su desarrollo a la legislación interna adoptada por los Estados miembros en la transposición de la normativa comunitaria.

- El derecho del interesado a oponerse a ciertos tratamientos de datos que le conciernen.

- La prohibición de que el titular de los datos sea sometido a decisiones con efectos jurídicos fundadas únicamente en un tratamiento automatizado de sus datos, aún cuando con ciertos matices sobre los cuales se ha implementado en la legislación interna de los Estados miembros.

Con todo, la Directiva 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.

4.- Responsabilidad en el tratamiento de datos personales

La Directiva comunitaria impone a los Estados miembros la obligación de que sus respectivas legislaciones nacionales deben prever que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito, o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la Directiva, han de ser reparados por el responsable del tratamiento de datos, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra que no se le puede imputar el hecho que ha provocado el daño, sea por responsabilidad del propio interesado o un caso de fuerza mayor.

Sobre el particular, se estima que el sistema de responsabilidad alentado por la Directiva es objetivo, ya que prescinde de la culpa o dolo con que haya obrado el responsable de tratamiento, exigiendo como factor de imputabilidad el procesamiento indebido de datos personales; tal juicio se sustenta fundamentalmente en la pretensión de la Directiva por establecer un estándar uniforme de protección al titular de los datos dentro de la Unión Europea, lo que

guarda oposición con la admisión de una responsabilidad subjetiva en la materia.[10] Sin embargo, existen también algunas voces que estiman que la Directiva insta a los Estados miembros a contemplar un sistema de responsabilidad por culpa.[11]

La discusión en torno al sistema de responsabilidad civil adoptado por la Directiva se proyecta igualmente a la legislación interna adoptada por los Estados miembros de la Unión Europea, salvo respecto de aquellos que, como acontece con Alemania, han explicitado sin equívocos su adscripción a un sistema de responsabilidad civil fundado en el riesgo creado u objetiva.

Sin embargo, la Directiva no sólo admite la existencia de una responsabilidad civil originada del tratamiento indebido de los datos personales, sino que también aboga por el establecimiento en las legislaciones internas de sanciones aplicables en caso de incumplimiento de las disposiciones adoptadas en ejecución de la misma Directiva.

En este sentido, los Estados miembros de la Unión Europea han hecho uso del margen de maniobra que tolera la Directiva; de tal modo, la tipificación de ilícitos es de resorte de las legislaciones nacionales, observándose mayor acuciosidad en unas que otras, a la par de apreciarse diferencias en torno a la sanción atribuida a tales conductas, ya que en unos se ha privilegiado la imposición de sanciones de naturaleza administrativa –tales como multas y apercibimiento–, mientras otros han puesto énfasis en las sanciones de naturaleza criminal. Entre los primeros se encuentra España e Italia, en tanto que entre los últimos cabe mencionar Francia y Alemania.

En efecto, la legislación española ha establecido un extenso catálogo de infracciones de mayor a menor gravedad, sancionadas con la aplicación de multas de un monto variable, para cuya precisión se admite una graduación según las diversas circunstancias que permiten aquilatar el grado de antijuridicidad y culpabilidad presentes en la conducta infractora.

En cambio, en Francia el texto original de la Ley relativa a la Informática, los Ficheros y las Libertades contemplaba diversas infracciones y sanciones de naturaleza penal, entre los que destacaban: el tratamiento de datos sin que medie acto habilitante o notificación previa a la Comisión; el tratamiento ilegítimo y fraudulento de datos nominativos; la divulgación sin autorización de su titular de datos nominativos lesivos a la reputación o consideración de la

[10] Grimalt Servera, Pedro. **"La responsabilidad civil en el tratamiento automatizado de datos personales".** Ed. Comares, Granada, 1999, pp. 160 y ss.

[11] Heredero Higueras, Manuel, **"La Directiva Comunitaria de Protección de Datos de Carácter Personal"**, Editorial Aranzadi, Pamplona, 1997, pp. 183.

persona o la intimidad de la vida privada; la desviación de finalidad en el tratamiento de datos. Todas estas figuras eran sancionadas con penas privativas de libertad y multas, acumulativa o alternativamente según los casos. Posteriormente, a raíz de la incorporación de las diversas figuras de delitos informáticos en el Código Penal, se ha prescindido de diversos tipos y remitido a las disposiciones de tal codificación, mas si se ha tipificado hipótesis específicas, tales como la utilización del registro nacional de identificación de las personas físicas sin la autorización del Consejo de Estado, quien la emite previo dictamen de la Comisión, con penas de prisión y multa, y la adopción de medidas que obstaculicen el accionar fiscalizador de la misma Comisión, con similares penas.

Por su parte, en Alemania, la Ley de Datos de 1977 contemplaba algunos tipos penales e infracciones de policía asociados al tratamiento de datos, los primeros sancionados inclusive con penas privativas de libertad, los segundos con multas de monto variable. Entre estos últimos, a efectos de resguardar la vigencia de los propios medios de control contemplados en la ley, se sanciona la omisión y extemporánea designación de comisario de protección de datos o notificación de inicio de actividades de procesamiento de datos, y obstaculizar las labores de fiscalización de la autoridad de tutela estatal. Mientras, la nueva Ley de Datos de 1990 abundó en la tipificación de los ilícitos penales e infraccionales asociados al tratamiento de datos.

II. MECANISMOS DE CONTROL EN LA NORMATIVA EUROPEA

1.- Consideraciones previas

El control, aquella actividad desplegada con el afán de comprobar, inspeccionar o fiscalizar el desempeño propio o ajeno, constituye un quehacer no sólo necesario, sino indispensable en todo sistema jurídico organizado; ello supone la concurrencia de dos elementos esenciales: el primero, la existencia de un determinado estándar normativo, de conocimiento tanto del agente controlador, como de quien es objeto de su actividad; el segundo, la formulación por el agente de control de un juicio de adecuación de la actividad de quien es controlado a tal patrón.

En cuanto a los mecanismos de control previstos en Europa, podemos anticipar que el repertorio es nutrido, aunque el cometido de cada uno de ellos no se circunscribe exclusivamente a practicar tal verificación. Todas las legislaciones, bajo la impronta de la Directiva comunitaria, admiten un control jurisdiccional, radicado preferentemente en los tribunales de justicia, al cual adicionan una autoridad pública cuyo cometido específico es fiscalizar el cumplimiento de la ley, la denominada autoridad de control. También gozan de una amplia recepción los códigos de conducta y el agente de control interno, entre otros. Sobre cada uno de ellos nos extenderemos en los acápites siguientes.

2.- Control Jurisdiccional y Habeas Data

Antes de abordar propiamente el control jurisdiccional, y particularmente el habeas data, es preciso formular un distingo en torno a la competencia que las leyes de protección de datos atribuyen al orden jurisdiccional, con especial énfasis en aquél de que gozan los tribunales de justicia.

Es habitual que las leyes confieran a la autoridad de control nacional para la consecución de sus fines ciertas facultades que no suponen un requerimiento judicial previo, tal como disponer una medida cautelar respecto de sistemas de tratamiento de información, conferir o denegar la autorización para procesar determinada categoría de datos, oponerse al registro de cierta información suministrada por el responsable de tratamiento, o dictaminar la implementación de medidas de seguridad determinadas. Indudablemente, la adopción de tales decisiones pueden ser estimadas lesivas por las personas afectadas por ellas, lo cual conducirá a éstas a requerir la intervención judicial, a fin de ver restablecidos los derechos que estiman amagados.

A su turno, con mayor o menor extensión, las leyes de protección de datos conceden a las autoridades de control ciertas facultades cuyo ejercicio supone un previo requerimiento y resolución judicial. Así, por ejemplo, la legislación británica exige que la autoridad de control requiera autorización judicial para disponer la entrada y registro de un establecimiento que trata datos; por su parte, la autoridad de control sueca carece de facultades sancionatorias, de modo que, ante la existencia de una infracción, debe recurrir judicialmente para la imposición de sanciones al infractor. En estos casos, será la autoridad de control quien arrastrará al responsable de tratamiento a sede judicial.

Así pues, la intervención judicial prevista en las leyes sobre protección de datos no alcanza solamente al accionar del titular de datos que estima menoscabados sus derechos por el responsable de tratamiento, sino que también se extiende a las reclamaciones que éste último formula contra las decisiones de la autoridad de control, así como a las acciones emprendidas por ésta en contra de aquél. De todas ellas, sólo nos ocuparemos del primer orden de materias de competencia judicial, aquellas que conciernen al ejercicio de acciones judiciales por el titular de los datos, ya que el tratamiento de las restantes excede los propósitos de este artículo.

La plena realización de los derechos fundamentales, en concepto de Pérez-Luño, supone la disposición de un recurso jurisdiccional destinado a garantizarle, lo cual el autor vincula con la procedualización del derecho moderno; tal fenómeno explica la necesidad de suministrar un recurso al titular de los datos personales para salvaguardar su derecho a la autodeterminación

informativa –libertad informativa, si se prefiere–, cuando ellos se vean amagados por el responsable de tratamiento.[12]

En este orden de consideraciones, la Directiva sostiene que sin perjuicio del recurso administrativo que pueda interponerse ante la autoridad de control, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos de los interesados que le garantice la legislación interna aplicable para los casos en los que el responsable del tratamiento de datos no los respete.

En este sentido, la totalidad de las legislaciones admiten el control jurisdiccional del tratamiento de datos personales a requerimiento del afectado por él. Ahora bien, no satisfechos algunos sistemas con admitir la vía judicial como medio para restablecer los derechos de los titulares de datos menoscabados con un tratamiento ilegítimo de los datos que les conciernen, es recurrente incorporar en las mismas leyes de protección de datos un procedimiento específico, concentrado y de tramitación simplificada, mediante el cual suministrar una respuesta más oportuna al afectado, el que la doctrina, a partir de la elaboración conceptual del constituyente brasileño, ha denominado *habeas data.*

Ahora bien, la expresión habeas data en Europa no se usa para referirse tan sólo a la acción judicial mediante la cual el titular de los datos personales hace efectivo sus derechos como tal ante tribunales, sino que con ella se refiere a la totalidad del decurso procesal a través del cual el afectado hace ejercicio del derecho de acceso, desde el requerimiento de sus datos al responsable de la base de datos, pasando por la reclamación administrativa ante la denegatoria del primero, hasta la acción judicial misma. Ello explica el énfasis puesto en Europa por conferir facultades a las autoridades de control de los diversos Estados miembros para conocer de las reclamaciones formuladas contra los responsables de tratamiento, sin perjuicio de un ulterior recurso judicial.

Sin embargo, las limitaciones propias del objeto, la oportunidad, y el impulso de la acción contralora radicada en sede jurisdiccional le hace insuficiente para hacer frente a los riesgos que importa el tratamiento indebido de los datos personales, ya no sólo para los derechos fundamentales de los afectados, sino inclusive por lo tocante a la legitimidad misma de un sistema democrático; de ahí la pretensión de la Directiva comunitaria, y de todas las legislaciones nacionales que han implementado sus disposiciones en el derecho interno de los Estados miembros y candidatos de la Unión Europea, de incorporar otros mecanismos, los que enseguida revisaremos, y particularmente de elevar a la autoridad de control a la condición de un elemento esencial en la obtención de un nivel de protección adecuado en la materia.

---

[12] Pérez-Luño, Antonio Enrique, "Intimidad y Protección de Datos Personales: del Habeas Corpus al Habeas Data", en **Estudios sobre el Derecho a la Intimidad**, Editorial Tecnos, 1992, pp. 40 – 42.

Con todo, para aquilatar apropiadamente las ventajas del control jurisdiccional, debemos considerar que él se encuentra normalmente comprendido en un andamiaje mayor, en el cual se incluyen otros mecanismos de control, mediante los cuales se sortean sus deficiencias, sin perjuicio del rol que pueda desempeñar respecto de estos últimos.

3.- Los códigos deontológicos.

La Directiva y la generalidad de la legislación nacional de los Estados miembros de la Unión Europea ha evidenciado la necesidad de contar con disposiciones especiales aplicables al tratamiento de datos personales para fines determinados, así, v. gr., cuando ellos son empleados para efectos de evaluación crediticia, cuando lo son en el contexto de una relación laboral, o bien para fines de seguridad social. Tal inconveniente se ha resuelto mediante los expedientes de acudir a la elaboración de normativas específicas –tal como sucede con el tratamiento de datos con ocasión de las comunicaciones electrónicas–, a la elaboración de pautas orientadoras por las autoridades de control nacional y, punto sobre el cual nos detendremos, a la formulación de códigos deontológicos –también llamados códigos tipo, en España; códigos de buenas prácticas, en Reino Unido; y códigos de conducta, en la Directiva–, los que junto con constituir un medio de adecuación de la normativa general a la especificidad de determinados contextos de tratamiento de datos, permiten hacer frente a la obsolescencia normativa y aún dirigir procesos legislativos posteriores.

Los códigos deontológicos, al decir de Orti Vallejo, constituyen normas de conducta relativas al manejo del banco y tratamiento de datos adoptadas por determinados sectores empresariales, asociaciones gremiales o profesionales.[13] Por consiguiente, son una expresión de autorregulación, por la cual los propios agentes fijan normas para el desempeño de sus actividades, si bien ello no excluye la participación de la autoridad pública durante su proceso de elaboración, ya sea fomentando su adopción, verificando su legalidad o simplemente registrando su existencia.

La Directiva 95/46/CE destina su capítulo V a los códigos de conducta, imponiendo a los Estados miembros y la Comisión, dentro de sus respectivas competencias, la obligación de alentar la elaboración de tales códigos destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de la Directiva, así como de las disposiciones nacionales adoptadas por los Estados miembros en relación con la misma,[14] previendo la intervención de una autoridad de control nacional o comunitaria en tal proceso, según los casos.

---

13 Orti Vallejo, Antonio, **"Derecho a la intimidad e informática"**, Editorial Comares, España, 1994, p. 17.

14 La propia Directiva considera que los códigos de conducta pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado.

Tratándose de proyectos de códigos comunitarios, así como de modificaciones o prórrogas a códigos comunitarios existentes, podrán ser sometidos al dictamen del Grupo de protección de datos que crea la propia Directiva, el cual se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la misma Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes.[15] Posteriormente, la Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del Grupo.

El Grupo de trabajo y algunas organizaciones encargadas de presentar los códigos aún están debatiendo la forma final de éstos. Así sucede con la Federación de Asociaciones Europeas de Venta Directa (FEDMA), que representa al sector de la venta directa a escala europea, la cual ha presentado un proyecto de código comunitario de prácticas para el uso de datos personales en la venta directa, que ha merecido sustanciales observaciones por el Grupo. Otro tanto acontece con un código de conducta sobre el tratamiento de datos personales presentado al Grupo por parte de las empresas de búsqueda de personal directivo (cazatalentos), presentado por la AESC; y el código de conducta sobre identificación paneuropea de la línea diamante, presentado por la ETP.

Distinta es la situación de la Asociación de Transporte Aéreo Internacional (IATA), que en 1997 presentó al Grupo de trabajo la práctica recomendada 1774 sobre la protección de la vida privada y los flujos transfronterizos de datos personales utilizados en el transporte aéreo internacional de pasajeros y cargamento (RP 1174), la que si bien no cumplía los requisitos de código de conducta con arreglo a la Directiva, recibió positivos comentarios del Grupo de Trabajo, siendo actualmente recomendada por IATA a sus miembros.[16]

En cambio, tratándose de códigos de conducta nacionales, la Directiva impone a los Estados miembros establecer 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, las que velarán, entre otras cosas, por la conformidad de tales proyectos con las disposiciones de derecho interno

---

15 El Grupo de Trabajo sobre Protección de Datos ha elaborado un documento de trabajo en el que establece el procedimiento y los elementos de examen de los códigos comunitarios, Cf. "Labor futura en relación con los códigos de conducta: documento de trabajo sobre el procedimiento de examen de los códigos de conducta comunitarios por el Grupo de Trabajo", aprobado el 10 de septiembre de 1998.

16 Grupo de Trabajo sobre Protección de Datos, Práctica recomendada IATA 1774 «Protección de la vida privada y los flujos transfronterizos de los datos personales utilizados en el transporte aéreo internacional de pasajeros y mercancías» Aprobado el 14 de septiembre de 2001.

adoptadas en aplicación de la propia Directiva. Además, se invita a la autoridad, si lo considera conveniente, a recoger las observaciones de los interesados o de sus representantes.

El progresivo reconocimiento obtenido por los códigos deontológicos ha supuesto superar ciertas desventajas inicialmente asociados a ellos y que dicen relación con la legitimidad en su proceso de elaboración, la fuerza obligatoria y la publicidad de los mismos.

El primer inconveniente relacionado con los códigos de conducta se vincula con la *representatividad* que debe implicar su elaboración, más aún cuando supone que la voluntaria aceptación de ellos por sus destinatarios es la que les confiere eficacia normativa. Peor aún, el problema cobra toda su fuerza cuando dos o más asociaciones profesionales u otras organizaciones gremiales pretenden atribuirse la representación del sector para imponer la adopción del código de conducta elaborado por sí a las demás. Además, de no exigirse cierta representatividad respecto de los códigos de conducta se corre el riesgo de una proliferación normativa sin límites, una pluralidad de regímenes jurídicos de concreción que socava toda pretensión de seguridad jurídica.

Siempre asociado a la legitimidad de su elaboración, un segundo inconveniente adjudicado a los códigos de conducta es el relativo a la *legalidad* de los mismos, esto importa juzgar la adecuación de sus normas con las previsiones que el ordenamiento jurídico interno del Estado a que se extiende su aplicación. El tema guarda estrecha relación con los propósitos perseguidos por asociaciones profesionales y las demás organizaciones que les adoptan, que en unos casos se limitan a satisfacer los intereses de sus destinatarios antes que fomentar el cumplimiento de sus disposiciones y las leyes relativas a la materia.

El tercer punto que merece reparos respecto de los códigos de conducta es el relativo a la *obligatoriedad* de los mismos, lo cual supone responder a cuán vinculantes resultan ellos para sus destinatarios, o bien, visto desde la perspectiva de las personas concernidas por los datos, cuál es la certeza que se les puede suministrar en cuanto a que serán cumplidas las disposiciones contempladas en ellos.[17] En general, la legislación carece de una respuesta sobre la exigibilidad de los códigos de conducta respecto de sus destinatarios. Por su parte, la doctrina estima que

[17] El problema concerniente a la obligatoriedad de las disposiciones adoptadas por la entidad responsable de tratamiento de datos a través de los códigos de conducta era visualizado ya en el Lindop Report, el que proponía que una vez aprobados gozarán del valor de disposición reglamentaria, parecer que no fue hecho propio por el legislador británico. Cf. Heredero Higueras, Manuel, **"La Directiva Comunitaria de Protección de Datos de Carácter Personal"**, Editorial Aranzadi, Pamplona, 1997, p. 196. Para una revisión sobre las diversas opciones consideradas en el Lindop Report a efectos de que los códigos de conducta gozarán de obligatoriedad, cf. Losano, Mario. "Los orígenes del 'Data Protection Act' inglesa de 1984", en *Cuadernos y Debates*, Nº 21, Centro de Estudios Constitucionales, Madrid, 1989, pp. 9 – 60.

precisamente el carácter voluntario de los códigos no garantiza derechos legales a ninguna de las partes intervinientes, salvo que su texto haya sido incorporado contractualmente.[18] Aun cuando también se han dejado sentir voces que les atribuyen el carácter de *lex artis* y, como tales, tras ser registrados y generar cierto grado de confianza entre los afectados, susceptibles de significar responsabilidad por su infracción.[19] Hay también quienes estiman que los propios códigos debían de contemplar sanciones –de naturaleza reparadora y punitivo– que asegurasen su eficacia.[20] Finalmente, para algunos los códigos tienen el valor de recomendaciones y como tales la sanción que llevan aparejada es, como más, la expulsión o separación del infractor de la agrupación a que corresponden el código vulnerado.[21]

Un cuarto aspecto que merece ser resuelto, en aras de un conveniente régimen jurídico de los códigos de conducta, es el relativo a la *publicidad* de los mismos. Si alguna eficacia normativa tienen los códigos, morigerada siquiera, ella supone la adecuada difusión de sus disposiciones, tanto entre sus destinatarios, como entre las personas concernidas por los datos, que son quienes mayor preocupación habían de revelar por el cumplimiento de sus preceptos.

Para hacer frente a los reparos que se formulan respecto de los códigos deontológicos, la Directiva y la normativa interna de los Estados miembros prevé en ciertos casos la intervención de la autoridad de control; así ella es la encargada de promover la adopción de tales códigos, junto con velar por su representatividad y legalidad, e, igualmente, les brinda adecuados cauces de difusión en la comunidad jurídica.

4.- El agente de control interno

La proliferación de los sistemas de tratamiento y la propagación de los datos personales, particularmente por entidades del sector privado evidenció la necesidad de disponer de un mecanismo de control que no descansara exclusivamente en una fiscalización "virtual" -remota, si se prefiere-, sino que guardara más cercanía con las operaciones de tratamiento: un agente de control interno, esto es, una persona nombrada por el responsable de tratamiento, que, de manera independiente, asegure que el tratamiento de datos personales se realice de forma correcta y legal.

---

18 Estadella Yuste, Olga, **"La protección de la Intimidad frente a la Transmisión Internacional de Datos Personales"**, Editorial Tecnos, Madrid, 1995, p. 44.

19 Orti Vallejo, Antonio, op. cit., p. 93 – 94.

20 Herrán Ortiz, Ana Isabel, **"El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales"**, Dykinson, Madrid, 2002, p. 314.

21 Velázquez Bautista, Rafael, **"Protección Jurídica de Datos Personales Automatizados",** Edit. Colex. Madrid, 1993, p. 191.

La primera referencia normativa de la institución, aplicada al régimen jurídico del tratamiento de datos personales, la encontramos en la Ley Federal de Protección de Datos de la República Federal Alemana de 1977, en la cual cada departamento administrativo o empresa privada que procesaba datos nominativos debía designar un *comisario de protección de datos* dependiente de la entidad tratante, con formación profesional calificada, quien velaría por la observancia de la ley, sin quedar sujeto a instrucciones superiores para tal fin.[22]

La figura es posteriormente acogida por la Directiva 95/46/CE con el nombre de *encargado de tratamiento*, quien es nombrado por el responsable del tratamiento para cerciorarse de que las operaciones efectuadas no atentan contra los derechos y libertades de los interesados.[23]

El agente de control interno puede ser asociado al tratamiento de datos personales efectuados tanto en el sector público como en el privado. De hecho, la Directiva comunitaria e igualmente en las legislaciones de Inglaterra y Suecia, que establecen disposiciones comunes aplicables al procesamiento de datos prescindiendo de distingo en la naturaleza de la entidad tratante, admiten su empleo como mecanismo de control cualquiera sea ésta. En cambio, la legislación alemana, en la cual se establece un régimen jurídico diferenciado entre el tratamiento verificado por organismos públicos y personas o entidades privadas, circunscribe la aplicación del *comisario de protección de datos* a estas últimas.[24]

La principal ventaja atribuida al agente de control interno, en cuanto mecanismo de control, radica en la continuidad y proximidad de su cometido en relación con las operaciones de tratamiento efectuadas por la entidad responsable de la base de datos. Por consiguiente, más que constituir un ente que se limita a constatar la conformidad de la actividad en relación con las disposiciones legales o reglamentarias, el agente de control interno orienta y asiste a la empresa, así como a las personas empleadas en el procesamiento de datos, acerca del modo de proceder en la materia, mediatiza la relación entre las personas afectadas por el tratamiento de datos y la entidad a la cual controla, y vincula a ésta con la autoridad de control.

Pese a la utilidad que significa disponer de un mecanismo como el que se viene comentando, la institución del agente de control interno no ha estado exenta de críticas; éstas se han centrado

---

22 § 28 y 29 de la Ley Alemana Federal de Protección de Datos de 1977.

23 Sobre la incorporación de la figura por la Directiva 95/46/CE, Cf. Heredero Higueras, Manuel, **"La Directiva Comunitaria…"**, op. cit., pp. 169 – 170. Sobre la inspección administrativa mediante sujetos privados, en que el agente de control interno es denominado colaborador, Cf. Rivero Ortega, Ricardo. **"El Estado vigilante. Consideraciones jurídicas sobre la función inspectora de la administración"**. Ed. Tecnos. Madrid, 2000, pp. 149 y ss.

24 La Ley de Datos de 1990 establece un régimen único aplicable al tratamiento de datos por el sector privado, a diferencia de la Ley de 1977, que, junto con distinguir entre tratamiento por organismos públicos y privados, a su vez, tratándose de estos últimos formulaba un distingo entre aquellos verificados para fines comerciales y no.

en que su establecimiento menoscabaría la protección de los titulares de datos, al dejar la comprobación sobre la legalidad de su tratamiento entregada a un tercero empleado del propio responsable de la base de datos, con una independencia meramente formal que no satisface las exigencias de un control efectivo.

No obstante, nos parece que el reparo formulado contra el agente de control interno evidencia una insuficiente documentación en quienes le sostienen, ya que supone que el cometido fiscalizador se radica en forma exclusiva y excluyente en tal figura, cuando la experiencia europea demuestra que la institución conjuga su quehacer con el accionar de la autoridad de control nacional y no obsta al ejercicio de las facultades que la ley asigna a ésta, así como a los propios titulares de los datos personales.

5.- La Autoridad de Control.-

Ya a comienzos de los ’70 la Ley de Datos de Hesse preveía una instancia de control, con las limitaciones propias de toda incipiente legislación, calificada en doctrina como de *“Autoridad de Control”*, una entidad administrativa cuyo propósito era informar los derechos de los ciudadanos frente al tratamiento automatizado de datos que les conciernen, asesorar a los responsables de tratamiento, visar los códigos de conducta adoptados por entidades públicas o privadas, fiscalizar el cumplimiento de la legislación y, más aún, sancionar las infracciones cometidas respecto de ella o abogar porque así ocurra, si es del caso. En definitiva, la entidad llamada a velar porque sea cumplida la normativa interna sobre tratamiento de datos.

En lo sucesivo, la generalidad de las legislaciones nacionales han adoptado una autoridad de control respecto del tratamiento de datos personales: en Suecia la *Datainspektionen*; en la República Federal Alemana el Comisario Federal de Protección de Datos, junto a autoridades de tutela estatal; en Francia la *Commission Nationale de l’Informatique et des Libertés*.

Entretanto, a instancias del Consejo de Europa, el Convenio de Estrasburgo de 1981 obliga a los Estados partes a concederse mutuamente asistencia para el cumplimiento del mismo, para ello cada cual debía designar a una o más autoridades nacionales. Sin embargo, no exige que se trate de una autoridad especialmente dedicada a ello, admitiendo, por consiguiente, que la competencia de asistencia mutua a nivel internacional sea acumulada a la de otro organismo público preexistente.

En 1984 Inglaterra adopta la *Data Protection Act*, en la cual, a efectos de control, se contemplan dos entidades: el Registrador de Protección de Datos y el Tribunal Administrativo de Protección de Datos. Por su parte, España promulga la LORTAD, en la cual se crea la Agencia de Protección de Datos y, a su vez, admite la creación posterior de autoridades de control por las diversas comunidades autónomas del país.

Desde comienzos de los noventa, la Comunidad Europea estaba abocada a la elaboración de una Directiva comunitaria en la materia, la que cristalizó en la Directiva 95/46/CE, la cual prevé, como un elemento esencial en el sistema de protección, que los Estados partes cuenten con una autoridad pública independiente abocada a ejercer funciones de promoción, fiscalización y coordinación respecto de la legislación sobre tratamiento de datos personales.[25]

A efectos de trasponer la normativa comunitaria en el derecho interno, diversos Estados europeos dictan nuevas leyes en la materia en las cuales se prevé una autoridad de control, así el Garante para la Protección de Datos Personales previsto por la legislación italiana, por la Ley 675 de 1996 sobre la tutela de las personas y otros sujetos respecto al tratamiento de datos personales; la *Data Protection Act de 1998*, que contempla el *Data Protection Commissioner* y el *Data Protection Tribunal*; la nueva Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD), mediante la cual España insiste en la existencia de la Agencia de Protección de Datos y otros organismos competente a nivel autonómico.

La Directiva confiere cierto margen de maniobra a los Estados miembros para la configuración de sus respectivas autoridades de control, lo cual ha permitido que ellas se adecuen a las realidades institucionales que les son propias. Con todo, el énfasis lo ha puesto la Directiva en la concesión de independencia a tal autoridad. En el entendido que ella es imprescindible para disponer de un óptimo cumplimiento de la normativa tanto por las entidades responsables de tratamiento del sector público como del privado. En este sentido se observa bastante celo en las legislaciones internas en lo tocante al nombramiento de quienes integran la autoridad de control, a las inhabilidades a que se ven afectos los mismos, a la inamovilidad de sus miembros, así como al otorgamiento de facultades reglamentarias y, quizá el punto que mayor esfuerzo demanda actualmente en la Unión Europea, la atribución de recursos materiales suficientes para el cabal desempeño de su cometido.

Por lo que respecta a sus funciones, una breve sistematización de las que suelen serle conferidas nos permite mencionar las siguientes:

1.- Difusión, Asistencia y Promoción. La autoridad de control es responsable de la difusión de las disposiciones legales y reglamentarias aplicables al tratamiento de datos personales, ya que las más de las veces la infracción a sus preceptos encuentra su explicación en una falta de conciencia de antijuricidad del comportamiento por

[25] Si bien inicialmente se exigía una independencia orgánica, hoy se estima suficiente que la autoridad competente goce de independencia funcional. Cf. Heredero Higueras, Manuel. **"La Directiva Comunitaria..."**, op. cit., pp. 201 – 210.

parte del responsable de registros o bases de datos. A tal tarea se suma la asistencia a los más diversos sectores de la comunidad: a los titulares de datos, acogiendo sus denuncias y dándoles curso a través de un procedimiento de resolución alternativa de las controversias suscitadas entre éstos y las entidades tratantes de datos; a los responsables de registros y bases de datos, asistiéndolos en la formulación de códigos deontológicos, en la adopción de políticas de seguridad, entre otras; a los organismos públicos, informando las decisiones que recaigan sobre materias de su competencia. Además, la autoridad de control realiza acciones de promoción en la materia, por ejemplo, mediante la el fomento en la aplicación de tecnologías de protección de la intimidad por las entidades que procesan datos y la adopción de códigos de conducta por los responsables de tratamiento.

2.- Registro. La autoridad de control es responsable de un registro público de las entidades que tratan datos personales, las cuales deben practicar notificación previa a la iniciación de las operaciones de tratamiento, si bien se admiten ciertas excepciones, por las cuales se releva o simplifica tal trámite, o bien se refuerza con exigencias adicionales, si es del caso. Además, en algunas legislaciones –es el caso de Francia y España– el registro se extiende a aquellos antecedentes que tienen relevancia general para una correcta aplicación e interpretación de la ley, tales como las resoluciones, informes o recomendaciones emitidas por la propia autoridad, así como los códigos de conducta que han merecido su aprobación.

3.- Inspección. La autoridad de control está dotada de facultades de inspección, las que incluyen el requerimiento de informes y antecedentes de los responsables de base o registros de datos, así como el ingreso y registro de los establecimientos y equipos en que se realizan las operaciones. Por su parte, los funcionarios de la autoridad de control quedan afectos a guardar confidencialidad con respecto a la información a que acceden con motivo del ejercicio de las facultades fiscalizadoras; y, en contrapartida, la obstrucción al desempeño fiscalizador –negativa a suministrar información, proporcionar información falsa y resistencia al acceso, entre otras– faculta a la autoridad para imponer sanciones de naturaleza administrativas a los responsables, o bien requerir su aplicación por tribunales.

4.- Facultades sancionadoras. La autoridad de control suele estar facultada para imponer sanciones administrativas –tales como multas y restricciones temporales para el tratamiento de datos– cada vez que se cerciora de la ocurrencia de actos u omisiones que importen una infracción a las disposiciones legales y reglamentarias vigentes, sin perjuicio de su reclamación judicial; si bien también existen algunas legislaciones que exigen un requerimiento judicial para tales efectos, como acontece en Suecia y

Reino Unido. En cambio, tratándose de ilícitos de naturaleza penal asociados al tratamiento de datos, la autoridad de control sólo dispone de facultades procesales suficientes para seguir las acciones criminales del caso y obtener la sanción del infractor precisamente por los tribunales de justicia.

5.- Facultades cautelares. La autoridad de control por lo general dispone de facultades excepcionales para adoptar medidas cautelares –tales como decretar el cese temporal de las operaciones de tratamiento, el congelamiento de una base de datos, o el bloqueo de determinados datos– en casos graves en que exista un riesgo real o inminente para los derechos del titular de los datos personales.

6.- Facultades normativas. La autoridad de control dispone habitualmente de facultades normativas, ya sea de orden general, que se concreta en disposiciones reglamentarias, o bien particular, mediante la emisión dictámenes u pronunciamientos específicos. Mediante tal expediente se concretan las previsiones generales de la ley, se orienta y conduce las operaciones de tratamiento de conformidad los principios inspiradores de la ley, se salvan sus omisiones y hace frente a la obsolescencia normativa resultante de las permanentes innovaciones introducidas en el sector.

7.- Cooperación Internacional. La autoridad de control cuenta con facultades y atribuciones suficientes para practicar acciones de cooperación internacional en materia de tratamiento de datos, sea que ellas se dirijan hacia titulares de datos personales y entidades tratantes de datos con residencia en el extranjero, o bien hacia organismos internacionales o autoridades de control de otros países. Asimismo, tratándose de flujo transfronterizo de datos personales, la autoridad de control certifica que el nivel de protección brindado en otros países sea similar al brindado en nuestra legislación, y, de no ser así, autoriza en casos de excepción la transmisión de datos a tales países de destino.

Con todo, nos parece del caso puntualizar que en Europa la institución de una autoridad de control en materia de tratamiento de datos personales es parte integrante de un sistema, en el cual deben concurrir tanto los agentes sociales pertinentes –esto es, titulares de datos personales y entidades responsables del tratamiento de los mismos– como el Estado, a través de la acción de la mentada autoridad, así como de sus tribunales de justicia.

Ahora bien, el adecuado funcionamiento de tal sistema de control supone como elemento esencial, aun cuando no el único, según cuanto hemos apreciado a lo largo de este artículo, la existencia de la autoridad de control, la cual coadyuva al funcionamiento de los restantes mecanismos de control.

6.- Otros mecanismos de control.

Los precedentemente examinados son los elementos centrales sobre los cuales se diseña el sistema de control europeo en la materia, aunque están lejos de ser los únicos, ya que las legislaciones de los Estados miembros de la Unión también acuden a otros, tales como las tecnologías de protección de la intimidad, los contratos-acuerdo y al propio Defensor del Pueblo.

a) Las tecnologías de protección de la intimidad

Se trata de mecanismos de control sobre el tratamiento que recae respecto de los datos personales que coadyuvan a aquellos otros previstos en el ordenamiento; tienen por propósito instaurar sistemas y tecnologías de información y comunicación, que minimizan la recolección y el empleo de datos personales, y dificultan las posibilidades de tratamiento ilícito.

La Comisión de las Comunidades Europeas ha distinguido tres tipos de productos según la tecnología empleada en su elaboración: aquellos que respetan la intimidad, los que son diseñados cumpliendo cabalmente con las disposiciones legales vigentes; aquellos que facilitan la protección de la intimidad, los cuales introducen además determinados elementos que facilitan el acceso de los usuarios a aspectos relacionados con la misma, tales como proporcionar al usuario medios simples para hacer ejercicio de sus derechos; y, los productos que fomentan la protección de la intimidad, esto es, aquellos creados con el fin de hacer un uso lo más amplio posible de datos verdaderamente anónimos, para lo cual recurre a procedimientos de disociación de los datos.[26]

Aplicaciones que responden a las características enunciadas son actualmente alentadas en la Unión Europea, particularmente en relación con el tratamiento de datos personales que supone el funcionamiento de la administración pública electrónica. Sin embargo, las mismas presentan un serio percance, cual es la dificultad para reconocer aquellos productos que responden a los estándares normativos de protección de la intimidad, más aún, desde que se ha constatado que algunas aplicaciones que se presentan como tales no satisfacen los requisitos.

Para hacer frente a la falta de transparencia con que algunos productos se presentan en el mercado, incrementar la confianza de los usuarios y garantizar una competencia leal entre las empresas que ofertan tales aplicaciones, la Comisión de las Comunidades Europeas ha considerado recientemente necesario implementar prácticas de certificación y verificación independientes de los productos.

---

[26] Cf., Comisión de las Comunidades Europeas, "Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)", Bruselas, 15 de mayo de 2003, pp. 17 – 18.

b) Los Contratos – Acuerdo

La falta de uniformidad legislativa entre los diversos países, en cuanto al régimen jurídico aplicable al tratamiento de datos personales, conduce a la ausencia de un estándar equivalente en la protección que se brinda a los derechos de las personas concernidas, lo cual constituye un obstáculo para la transferencia internacional de datos.

Esta situación ha sido especialmente sensible para los Estados miembros de la Unión Europea, los que tras las deficiencias evidenciadas por el Convenio de Estrasburgo, han acudido a la dictación de un Directiva comunitaria en la materia, a fin de garantizar un estándar suficiente de protección, necesario para la libre circulación de los datos entre los Estados miembros. Sin embargo, la Directiva 95/46/CE surte sus efectos obligacionales sólo respecto de los Estados partes de la Unión, con lo cual subsiste el problema con relación a terceros países, especialmente en atención a la frecuencia con que las empresas europeas acuden a servicios de tratamiento fuera de la Unión, ya sea para concentrar medios tecnológicos, reducir costos, u obtener operaciones ininterrumpidas.

Para hacer frente a los riesgos aparejados a la transmisión de datos a terceros países se ha recurrido al expediente de soluciones contractuales, esto es, a la suscripción de contratos-acuerdos con los Estados interesados en promover la transmisión de datos, mediante los cuales se garantiza un nivel adecuado de protección.

Los contratos-acuerdos, junto con ofrecer una solución para la transferencia transnacional de datos, tienen la ventaja de revestir la fuerza obligatoria necesaria para hacerles exigibles y, en caso de incumplimiento, requerir indemnización por los perjuicios que su infracción irrogare. Sin embargo, presentan el inconveniente de que tal derecho se confiere a los Estados partes, no así a los titulares de los datos personales, quienes no concurren a la celebración del contrato, salvo se incluyan cláusulas que les atribuyan la calidad de terceros beneficiarios, práctica que viene recomendando el Grupo de trabajo en protección de datos personales creado por la Directiva.

La Directiva admite que las negociaciones que conduzcan a la celebración de contratos-acuerdos se produzcan a nivel comunitario o nacional, siendo numerosos los Estados miembros que han acudido a tales mecanismos para reglamentar el flujo transfronteras de datos personales.[27] Así, por ejemplo, la legislación de Suecia faculta al Gobierno para dictar normativas sobre tales transferencias a países terceros, siempre y cuando ella se regule por un contrato que proporcione las garantías adecuadas para proteger los derechos de los interesados.

[27] Sobre el particular, cf. Estadella Yuste, Olga, op. cit., pp. 49 – 50.

Prescindiendo de las ventajas de los contratos-acuerdos, lo cierto es que ellos no constituyen propiamente mecanismos de control en materia de tratamiento de datos personales, sino que, a lo sumo, entre sus diversas previsiones se contienen fórmulas de control. Sin embargo, nos ha parecido pertinente incluirlos en éste acápite, en cuanto a través de ellos se puede alentar el cumplimiento de las normas relativas al tratamiento de datos personales, aún cuando su ámbito de aplicación quede circunscrito a las trasferencias internacionales de éstos.

c) El Defensor del Pueblo

Al ser discutida en España la necesidad de disponer de un medio de control estatal para salvaguardar el cumplimiento sobre la normativa que reglamentaría el tratamiento de los datos personales, se suscitó controversia en torno a sí era menester crear una nueva entidad a la cual encomendar tal labor, o bien adjudicar ella a alguna ya existente que velase por los derechos ciudadanos involucrados.

Tal dilema decantó en la posibilidad de servirse del Defensor del Pueblo, organismo que contaba con una basta experiencia velando por los derechos fundamentales de las personas frente al accionar de entidades públicas. No obstante, tal definición importaba enfrentar una nueva disyuntiva, cual era: limitar las facultades de la autoridad al control sobre el tratamiento de datos por organismos públicos, a fin de no desnaturalizar el instituto, aunque con el consiguiente menoscabo para una protección integral en la materia; o bien, admitir la necesidad de disponer de un organismo paralelo que hiciera las veces en relación a las entidades privadas que procesasen datos personales, con el serio percance de que tal definición importaría fragmentar el sistema de protección y exponer a la comunidad a criterios disímiles entre los organismos competentes en el sector público y privado.[28]

A la postre, se impuso la opción por la creación de un organismo ex - novo, que hiciese las veces de autoridad de control en el derecho interno, sin perjuicio de admitir la creación de agencias de control autonómicas, en el marco del transvase de competencias hacia las Comunidades Autónomas, si bien con las restricciones y prevenciones del caso.[29]

Una situación similar a la española tuvo lugar, con motivo de la institución de la autoridad de control en materia de tratamiento de datos, en Suecia y en Reino Unido, países en los cuales

[28] Acusando la limitación de las competencias del Defensor del Pueblo para asumir las competencias pertinentes tratándose de la protección de las personas frente al tratamiento de datos personales, Cf. Romeo Casabona, Carlos María, **"Poder informático y seguridad jurídica"**. FUNDESCO. Madrid, 1988, p. 33 infra. 37.

[29] Lucas Murillo de la Cueva, Pablo, "Informática y Protección de Datos Personales", en *Cuadernos y Debates*, Nº43, Centro de Estudios Constitucionales. Madrid, 1993, pp. 121 – 122.

también se optó por la creación de una nueva autoridad: la Inspección de Datos y el Comisionado de Protección de Datos, respectivamente, si bien ambas entidades presentan el sello innegable de la institución del Ombudsman, particularmente por la importancia que se atribuye a la función preventiva que les competen en la materia.

Sin embargo, tal definición no importa la privación al Defensor del Pueblo de facultades para obrar en defensa de los derechos de los ciudadanos amagados por el tratamiento de datos, especialmente cuando él es efectuado por organismos públicos; de hecho, la propia LORTAD ya preveía instancias de comunicación entre la Agencia de Protección de Datos y el Defensor del Pueblo con miras a la corrección en el accionar de las entidades del sector público responsables del tratamiento de datos. Más aún, en el caso de España, el Defensor del Pueblo formuló requerimientos de constitucionalidad ante el Tribunal Constitucional por algunas disposiciones de la antigua ley de datos que en ciertos extremos juzgaba contrarios a la Carta Fundamental.

Por consiguiente, ni aún el establecimiento de una autoridad de control específica en materia de tratamiento de datos, excluye la intervención del Defensor del Pueblo cuando se dan las hipótesis que hacen concurrente su competencia en la materia.

III. CONCLUSIONES

Tras estimar agotado nuestro afán, en orden a revisar la normativa europea en relación con el régimen jurídico del tratamiento de datos personales, parece oportuno precisar algunas breves conclusiones.

En primer término, el panorama europeo permite sostener que, tratándose del régimen jurídico aplicable al tratamiento de datos personales, se ha logrado la construcción de ciertos consensos mínimos, sobre la base de y por los cuales se ha verificado cierta *aproximación normativa* en la materia: un marco conceptual común, una definición relativamente uniforme del ámbito de aplicación, unos mismos principios rectores del procesamiento de datos y una notable similitud en los derechos conferidos a aquél a quien los datos conciernen, son, entre otros, elementos indiciarios de ello.

En segundo lugar, se aprecia en Europa que el reconocimiento y promoción de mecanismos de autocontrol no garantizan la obtención de un nivel de protección adecuado en la materia, ya que las reservas y omisiones que su funcionamiento merece evidencian la necesidad –esto es, en cuanto condición imprescindible– de disponer de una autoridad de control, un organismo público encargado de promover e informar a la comunidad sobre la legislación aplicable al tratamiento de datos personales, fiscalizar el cumplimiento de la normativa y sancionar su infracción, o bien instar por la sanción del infractor, en su caso.

Los reparos en cuanto a la certificación de las tecnologías de protección de la intimidad, a la independencia del agente de control interno, a la representatividad y legalidad de los códigos deontológicos, por mencionar algunos, encuentran oportuna respuesta en la institución de una autoridad de control y, más aún, ella no sólo salva tales cuestionamientos, sino que emprende cometidos que ninguno de tales mecanismos satisface: difusión, publicidad, asistencia, fiscalización y sanción. Vale decir, la implementación de una política pública coherente con un Estado democrático que promueve las condiciones que garantizan el pleno desarrollo de las personas.