

## ESTUDIOS

---

### LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN EL TRATAMIENTO DE DATOS: PRINCIPIOS Y DERECHOS. BREVE COMENTARIO DE LA TRANSPOSICIÓN DE LA DIRECTIVA 95/46/CE A LA LEY ORGÁNICA 15/1999

MARÍA DOLORES GARCÍA MESEGUER

*Secretaria del Juzgado de Paz de Aspe  
Doctorando en Derecho por la Universidad de Alicante*

RAFAEL MEDRÁN VIOQUE

*Experto en Comercio Internacional  
Doctorando en Derecho por la Universidad de Alicante*

#### NOTA PREVIA

Este trabajo responde a la doble intención de analizar como se ha transpuesto la Directiva 95/46/CE, de protección de Datos Personales a la Ley 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, y de realizar un seguimiento del desarrollo de los derechos que establece la Directiva, esto es, si simplemente se transcriben sus preceptos, lo que vaciaría de contenido a la transposición reduciendola a un mero trámite, o si por el contrario se aprovecha la transposición para aumentar el nivel de protección y garantía en cuanto al tratamiento de datos personales y su posible transferencia a países terceros.

*ÍNDICE: 1. Introducción. 2. Disposiciones Generales. 3. Protección de Datos: Principios Generales. 4. Derechos de las Personas. 5. Movimiento Internacional de Datos. 6. Conclusiones. 7. Bibliografía, Legislación y Jurisprudencia.*

## 1. Introducción

En la actualidad, a nadie se le escapa las posibilidades que la informática aporta a la solución de problemas y a la rapidez en la tramitación de cualquier expediente, tanto público como privado. Pero también debemos tener en cuenta los peligros que esta gigantesca capacidad y velocidad para el manejo de datos supone en la protección de los derechos fundamentales <sup>(1)</sup> principalmente los referidos a la intimidad al honor y la propia imagen. Sin embargo si bien con la informática se abre un nuevo actuar, no es menos nuevo que los países, junto con el descubrimiento del potencial económico que suponía la informática descubrieron los peligros que la misma entrañaba en cuanto a la intimidad, privacidad y ejercicio de sus derechos por parte de los ciudadanos, así, han sido numerosas las leyes que, desde prácticamente los años setenta se han ido dictando, como la Data Surveillance Bill de 1969, que fue una propuesta de ley británica que trataba de controlar el proceso de datos con la intención de impedir cualquier intromisión en la vida privada de los ciudadanos, o la «Daten-schutz», aprobada por el Parlamento de Hesse (Alemania) en 1970, o la Privacy Act de 1974 en Estados Unidos, o la Ley «La informática, los ficheros y las Libertades», promulgada en Francia el 06 de enero de 1978.

Ya en los años ochenta, en el seno del Consejo de Europa se firma el Convenio de Estrasburgo sobre Protección de Datos (Convenio 108 del Consejo de Europa) de 28 de enero de 1981, promulgándose con posterioridad la «Data Protection Act» que entró en vigor el 12 de Junio de 1984 en Gran Bretaña. En el ámbito de países pertenecientes a la comunidad, se firma en 1985 por Alemania, Francia, Bélgica, Holanda y Luxemburgo el primer Tratado de Schengen, y que tendrá su continuación en el segundo Tratado de Schengen de 1990, que obliga a los países firmantes a adoptar las medidas necesarias para dar cumplimiento a lo prescrito en el Convenio del Consejo de Europa de 1981, siendo este el antecedente más directo en el que bebe la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y que es la base sobre la que se ha de asentar nuestra Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD). En cuanto a la legislación española, podemos citar como antecedentes la Constitución de 1978, fundamentalmente en los apartados uno y cuatro del artículo 18; la Ley Orgánica 1/1982 de 5 de mayo de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, y la Ley Orgánica 5/1992 de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

## 2. Disposiciones Generales

La LOPD inicia su articulado delimitando lo que es el objeto de la misma. Así, en su primer artículo se hace eco del mandato Constitucional establecido por nuestro legislador en el artículo 18.4 CE <sup>(2)</sup>, para garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamen-

<sup>(1)</sup> Todo esto a su vez, alentado por las novelas de Orwell y su «big brother», así como Huxley y su «un mundo feliz».

<sup>(2)</sup> El artículo 18.4 de la C.E. establece: «La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.»

tales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, olvidando incluir, como dice la directiva, que esta protección no podrá restringir ni prohibir la libre circulación de datos personales entre los Estados miembros amparándose en la protección del derecho a la intimidad.

Se extrae del ámbito de aplicación de la ley determinados tipos de datos personales como son los ficheros mantenidos por particulares en el ámbito exclusivamente doméstico, las materias clasificadas<sup>(3)</sup>, así como los relativos a la investigación del terrorismo y formas graves de delincuencia organizada; rigiéndose por sus disposiciones específicas, y de forma supletoria por la LOPD aquellos datos relativos al régimen electoral, los que tengan fines exclusivamente estadísticos y amparados por la legislación estatal o autonómica sobre esta materia, los relativos al régimen del personal de las fuerzas armadas, los derivados del registro civil y el registro central de penados y rebeldes y los provenientes de imágenes y sonidos obtenidos mediante la utilización de vídeo-cámaras por las Fuerzas y Cuerpos de Seguridad del Estado de acuerdo con las leyes que los regulan.

En lo que respecta al derecho nacional aplicable la ley se sigue basando en un criterio territorial para establecer la competencia judicial internacional, cuando se está hablando de una materia, en la cual, dado que la accesibilidad es a nivel planetario, es irrelevante.

En cuanto a las definiciones recogidas, vemos que tanto en la Directiva 95/46, como en la LOPD, aparece la definición de datos personales, si bien, la LOPD en su artículo 3, evita dar una definición de lo que se debe entender por identificable<sup>(4)</sup>, lo que no implica una laxitud en la protección de los derechos del interesado, por ejemplo, introduce el concepto de procedimiento de disociación consistente en que el resultado de un tratamiento de datos personales no pueda ser asociado a una persona identificada o identificable. Así, con respecto al término «consentimiento» la legislación nacional añade como requisito el que éste sea inequívoco<sup>(5)</sup>, estableciendo de esta forma un parámetro más amplio de protección. Nada dice expresamente nuestra Ley Orgánica con respecto al consentimiento tácito, lo que no implica un rechazo del mismo. Esta cuestión, que podría ser objeto de crítica por parte de la doctrina, viene recogida en el Real Decreto 1736/1998, de 31 de Julio que en su artículo 65.3 autoriza a los operadores de telecomunicaciones al tratamiento de los datos necesarios para la facturación y pago de las interconexiones (enumerados en el apartado 2) cuando tenga como finalidad la promoción comercial de sus propios servicios, recabando el consentimiento de forma tácita<sup>(6)</sup>. Se introducen, así mismo, conceptos nuevos como el de «cesión o comunicación de datos» y el de «fuente accesible al público». Sin embargo, la LOPD se olvida definir que debemos entender por «tercero» y por «desti-

<sup>(3)</sup> La Ley 48/78 de Secretos Oficiales de 7 de octubre, («BOE» núm. 243, de 11 de octubre de 1978), en su artículo 2 define que «a los efectos de esta Ley se consideran «materias clasificadas» los asuntos cuyo conocimiento por persona no autorizada, puedan dañar o poner en riesgo la seguridad o defensa del Estado».

<sup>(4)</sup> El apartado a) del artículo 2 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, establece «...se considerará identificable toda persona cuya identidad pueda 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».

<sup>(5)</sup> Compárese el apartado h) del artículo 3 de la LOPD 15/99, con el apartado h) del artículo 2 de la Directiva 95/46/CE.

<sup>(6)</sup> Vide Alonso Martínez, Carlos «El consentimiento del interesado en protección de datos»; Universidad Pontificia de Comillas, Madrid. XIV Encuentros sobre informática y Derecho 2000-2001. Edit. Aranzadi.

nario». Lo que sin lugar a dudas nos obliga a recurrir a la directiva, en cuanto derecho supranacional, para entender a que o quienes se refiere la LOPD cuando habla de los mismos <sup>(7)</sup>.

### 3. Protección de Datos: Principios Generales

En cuanto a la calidad de los datos, al relacionar el apartado 3 del artículo 4 de la LOPD con el apartado d) del artículo 6 de la Directiva 95/46/CE, nos damos cuenta que la ley española en lo relativo a la exactitud y actualización de los mismos, olvida el adjetivo «razonable» que es utilizado por la Directiva, lo cual, en principio, indica un mayor nivel de responsabilidad, compromiso y exigencia al responsable del tratamiento, toda vez que, al no delimitarse, se le puede exigir un esfuerzo desproporcionado en el mantenimiento exacto y actualizado de los datos.

Aunque tanto la Directiva en su artículo 6.1b), como la Ley en el artículo 4.1 definen de manera similar que características han de tener los datos recogidos para un determinado tratamiento, la Ley española en el artículo 4.7, añade una serie de conductas garantistas de cómo no deben ser obtenidos esos datos <sup>(8)</sup>, considerando infracción muy grave «la recogida de datos de forma engañosa y fraudulenta» <sup>(9)</sup>.

Con referencia a la calidad de los datos, se produce en la LOPD una trasposición prácticamente literal de las características que han de reunir los datos para poder mantener el criterio de calidad exigido en el Considerando 28 y artículo 6 de la Directiva 95/46/CE. Si bien, la Directiva al referirse a los principios relativos a la calidad de los datos, establece al responsable del tratamiento como garante de la calidad de los mismos, algo que la ley española no hace en dicho apartado ya que el régimen sancionador recogido en la Directiva da amplias facultades a los estados miembros para configurarlo <sup>(10)</sup>. Tanto en la directiva 95/46CE como en la LOPD, se observa la obligación de realizar la recogida de datos con un fin determinado, que deberá ser comunicado al interesado, debiendo ser cancelados los datos cuando no sirvan al propósito para el cual fueron recabados, no pudiendo modificarse el fin para el que fueron recogidos.

Con respecto al Derecho a la información al interesado por parte del responsable del tratamiento, tal y como recoge el Considerando 38 de la Directiva 95/46 CE, todo tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos, y contar con una información precisa y com-

<sup>(7)</sup> Artículo 2 de la Directiva 95/46/Ce, establece: «A efectos de la presente Directiva, se entenderá por: ... 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.

<sup>(8)</sup> Artículo 4.7 de la LOPD: «Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos».

<sup>(9)</sup> Ver artículo 44.4a) de la LOPD. Sin lugar a dudas la utilización por parte del legislador de la conjunción «y», en lugar de la disyuntiva «o», implica una mayor exigencia en cuanto a los requisitos necesarios para la consideración de la infracción como muy grave, con la consiguiente dificultad para aplicar la sanción.

<sup>(10)</sup> El artículo 24 de la Directiva 95/46/CE establece que: «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.»

pleta respecto a las circunstancias de dicha obtención. Siendo imprescindible para el ejercicio de los derechos que la Ley otorga a los interesados, el que estos dispongan de toda la información referente a los tratamientos que con sus datos se están realizando, toda vez que la falta de información haría inviable el legítimo ejercicio de sus derechos. Hemos de preguntarnos desde que momento tenemos derecho a la información, sin lugar a dudas, a nuestro entender, el momento ideal será aquel que se produzca con anterioridad a la recogida de datos del interesado y por supuesto antes de que el responsable realice cualquier cesión a terceros. Huelga decir, que toda información que se facilite al interesado, ha de ser transparente e inteligible por este, pues en caso contrario se debilitaría el ejercicio de los derechos que le asisten. La LOPD, en su artículo 5, recoge de forma amplia el derecho a la información transponiendo todos los preceptos recogidos en el articulado de la Directiva 95/46CE. Si bien, la legislación española salva de manera elegante la posibilidad que refleja la Directiva en su artículo 18.4 (posibilidad de eximir de notificación a la autoridad de control por parte de las asociaciones sin ánimo de lucro) con la obligación recogida el Título IV, capítulo II de la ley de notificar siempre a los asociados y miembros la cesión de sus datos. Nos encontramos ante un precepto —el artículo 5 de la LOPD— de elevada importancia, toda vez que como menciona el Tribunal Constitucional <sup>(11)</sup> en su Sentencia 292/00, «sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales...» «...es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales...»

El artículo 6 de la Ley establece la necesidad del consentimiento del afectado de forma inequívoca para cualquier tratamiento de datos de carácter personal, salvo que la ley disponga otra cosa, ahora bien, como establece nuestro Tribunal Constitucional <sup>(12)</sup>, «...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...»

En lo que respecta al derecho de oposición, la normativa española lo reconoce, en el artículo 6, cuando al hablar del consentimiento del afectado, en su apartado cuarto establece que, «en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal.», es decir, se establece un criterio amplio y genérico siempre que, como dice la Ley, exista un motivo fundado y legítimo a una concreta situación personal. A sensu contrario en el caso de que para el tratamiento se precise el consentimiento del interesado éste podrá ejercer su derecho de oposición en cualquier momento y sin mediar motivo alguno. De la lec-

<sup>(11)</sup> Vide Sentencia 292/2000 de 30 de Noviembre del Pleno del Tribunal Constitucional en Recurso de inconstitucionalidad 1463/2000, promovido por Defensor del Pueblo. «BOE» núm. 4 Suplemento, de 4 de Enero de 2001.

<sup>(12)</sup> Vide anotación 11.

tura del artículo 14 de la Directiva parece ser que el derecho de oposición recogido en esta es más limitado que el recogido en la ley española.

Cuando la ley española en su artículo 7 se refiere a los datos especialmente protegidos, se muestra más garantista que la Directiva europea, pues al referirse al almacenamiento de datos relativos al origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, la salud o a la sexualidad que pueden mantener las entidades sin ánimo de lucro, se exceptúan aquellos que la Directiva llama «personas que mantengan contactos regulares», ya que como dice Herrán Ortiz<sup>(13)</sup> se ha de evitar el abuso de conceptos jurídicos indeterminados.

Podemos decir que la Ley española, eleva el nivel de protección establecido en el marco de la Directiva en cuanto al tratamiento de datos especialmente protegidos, toda vez que al referirse a la forma de manifestar el consentimiento, no solo requiere que este sea explícito, tal y como establece la Directiva en el apartado 2 a) del artículo 8, sino que va más allá al definirlo, exigiendo que el mismo sea expreso y por escrito, cambiando un concepto genérico por dos requisitos específicos.

Siguiendo con el análisis de los datos especialmente protegidos, observamos que si bien la Directiva y la ley permiten, con el consentimiento interesado, el tratamiento de datos relativos al origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, la salud o a la sexualidad, la ley española da un paso más al recalcar la prohibición de crear o mantener ficheros cuyo único objetivo sea «almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual»<sup>(14)</sup>, lo que sin lugar a dudas supone un plus de garantía ante el protagonismo que las conductas intolerantes están adquiriendo en la sociedad occidental.

Con respecto al tratamiento de los datos relativos a la salud, la LOPD hace una trasposición prácticamente literal de la Directiva 95/46, remitiendonos a su vez, a la legislación autonómica y estatal sobre sanidad. La dispersión normativa existente sobre la materia ha sido detectada desde la Unión Europea que ya prepara las bases para acercar las posiciones de los quince respecto a este sector. No obstante, queremos incidir en el tema de que, cuando hablamos de datos relativos a la salud, el mero hecho de dirigirnos a un determinado facultativo médico puede suponer un consentimiento presunto para que éste acceda a todos nuestros datos concernientes a la salud, con las limitaciones que al respecto establezca la legislación nacional o autonómica sobre la materia. Aparece de esta forma el peligro potencial que puede suponer que los datos de un determinado paciente lleguen a manos de aseguradoras privadas, quienes, una vez analizado el historial médico, denieguen la posibilidad de asegurarse o impongan unas cuotas que hagan inviable la obtención de un seguro. Por otra parte, el mantenimiento de unos controles excesivamente estrictos, podrían llegar a dificultar el desarrollo de la ciencia y la medicina en particular.

En cuanto a la seguridad de los datos, la ley española en su artículo 9, no observa el coste económico como una variable a la hora de establecer el nivel de protec-

---

<sup>(13)</sup> HERRAN ORTIZ, Ana Isabel, «España: La protección de datos personales en el marco de la Unión Europea». Editado en Revista Electrónica de Derecho Informático, el 26 de octubre de 2001; vlex.com.

<sup>(14)</sup> Vide artículo 7.4 de la LOPD.

ción del que deben gozar los datos en función de su naturaleza, al contrario de lo establecido por la Directiva, tanto en sus Considerandos <sup>(15)</sup>, como en su articulado <sup>(16)</sup>. Si bien, puesto que estos requisitos en la Ley española, quedan supeditados al desarrollo reglamentario pudiera ser que en este se disminuyera el nivel de protección. A este respecto, el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, establece tres niveles de protección en función del carácter de los datos tratados, y que califica como nivel de seguridad básico, medio y alto.

Por su parte, el *Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal* establece, que el nivel de protección de los datos se realizará en función de la sensibilidad de los mismos. De tal manera que, el nivel básico se aplicará a todos aquellos ficheros que contengan datos de carácter personal, como por ejemplo, nombre, dirección tanto electrónica como postal, teléfono, etc; el nivel medio de seguridad se aplicará a los ficheros que contengan datos referentes de infracciones administrativas o penales, hacienda pública, servicios financieros, etc; por último el nivel alto de protección se aplicará a los ficheros que contengan datos acerca de la ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas <sup>(17)</sup>. A este respecto, el Real Decreto 195/2000 de 11 de febrero por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el reglamento aprobado por el Real Decreto 994/1999 de 11 de junio, establece en su artículo único que las medidas de seguridad previstas para el nivel básico, deberán ser operativas antes del 26 de marzo de 2000.

El artículo 10 de la LOPD, se hace eco del deber de secreto, a diferencia de la Directiva 95/46/CE <sup>(18)</sup>, la cual únicamente hace referencia al secreto en relación con los datos referidos a la salud e historiales clínicos y a los miembros y agentes de las autoridades de control, obligación esta que, a criterio del legislador español, afecta tanto al responsable del fichero como a todos aquellos que intervengan en cualquier fase del tratamiento, y es más, dicha obligación, subsistirá aun después de finalizar sus relaciones con el titular del fichero o responsable del tratamiento. El incumplimiento de esta obligación, viene tipificada como infracción en el artículo 44 de la LOPD, pudiendo calificarse esta de leve, grave o muy grave en función de la mayor o menor sensibilidad de los datos tratados.

La comunicación de datos precisa del previo consentimiento del interesado para que esta se produzca. Las excepciones recogidas por la Directiva, que evitarían la necesidad de obtener el consentimiento por parte del interesado para la comunicación de sus datos personales, vienen adaptadas y refundidas por el legislador en el artícu-

---

<sup>(15)</sup> La Directiva 95/46/CE, en su Considerando (46) establece «...corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse;»

<sup>(16)</sup> Vide apartado 1 in fine del artículo 17 de la Directiva 95/46/CE.

<sup>(17)</sup> Vide artículo 4 y artículos 8 y ss. del Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, para observar en qué consiste cada uno de los niveles de seguridad.

<sup>(18)</sup> Vide Considerando 33 y artículos 8 y 28 de la Directiva 95/46/CE.

lo 11 de la LOPD para garantizar un nivel de protección suficiente en el interior de nuestras fronteras en cuanto a la comunicación de datos, si bien, no halla reflejo exacto en la Directiva, toda vez que esta únicamente establece un marco de mínimos para la transferencia de datos entre Estados, al que han de sujetarse los estados miembros tanto en sus relaciones entre si, como con sus nacionales y con terceros Estados, por ello, si la comunicación se efectúa previo procedimiento de disociación <sup>(19)</sup>, no será aplicable lo establecido en el artículo 11 al que nos referimos <sup>(20)</sup>, toda vez que, al no ser posible la identificación del interesado, no existe riesgo alguno y desaparece la necesidad de proteger su intimidad a través de la protección de sus datos.

En el artículo 12 de la ley podemos observar las consecuencias y requisitos del encargo a un tercero del tratamiento de datos por parte del responsable del tratamiento. Siendo lo novedoso y no recogido en la Directiva el que el encargado del tratamiento, pasa a ser responsable del mismo en el caso de que incumpla las estipulaciones previstas en el contrato que ha de firmar. Esta transformación es importante en tanto en cuanto le hará responsable directo de la infracción cometida, debiendo hacerse cargo de los perjuicios sufridos por los interesados como consecuencia de su ilícito comportamiento.

#### 4. Derechos de las Personas

El artículo 13 de la ley, primero dentro del Título III relativo a los Derechos de las personas, resulta ser una copia prácticamente literal, en su apartado primero, del correlativo en el artículo 15 de la Directiva, en cuanto al derecho que le asiste a toda persona a no verse sometida a una decisión con efectos jurídicos, sobre ella, o que le afecte de manera significativa, y que esté basada únicamente en un tratamiento de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad, conducta, etc. En este sentido, la Ley española concede al interesado la potestad de impugnar aquellos actos administrativos o decisiones privadas que vulneren lo preceptuado en el apartado primero, así como el derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizado para adoptar la decisión. Nos encontramos ante un peligro potencial que la Ley trata de neutralizar. Evidentemente, nadie quiere quedar atrapado en unos pocos datos, o como bien dice Ramos Méndez <sup>(21)</sup> «es una llamada de atención contra el peligro de creer que, porque se tiene algún dato, ya se tienen todos los elementos de juicio; contra la tentación de que puede juzgarse a las personas por sus «generales características» y no por sus «particulares actos» probados y pertinentes para el juicio de que se trate; contra la comodidad del miedo reverencial al «infalible» ordenador, como antes existió la comodidad del miedo reverencial a la «infalible» prensa, o a la «infalible» televisión.» Si bien, la legislación española es más restrictiva en cuanto a las decisiones individuales automatizadas que la Directiva comunitaria, ya que en ésta, se permite la realización de este tipo de tratamientos en el ámbito de la autonomía de la voluntad, es decir, como consecuencia de la firma de un contrato. Sin

<sup>(19)</sup> Comparar artículo 3 LOPD, con artículo 2 Directiva 95/46/CE. Nótese que el concepto «procedimiento de disociación» no aparece.

<sup>(20)</sup> Vide apartado 6 del artículo 11 de la LOPD.

<sup>(21)</sup> Eduardo Ramos Méndez y otros, «informática jurídica», página 216 y ss; UNED 1994.



embargo, el apartado 4 del artículo 13 de la LOPD establece que dicha valoración basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

El artículo 14 de la LOPD, nos proporciona la posibilidad, pública y gratuita, de conocer, recabando la información oportuna del Registro General de Protección de Datos, la existencia de aquellos tratamientos que sobre nuestros datos se estén realizando y de los cuales tengan conocimiento. Cuestión esta, sin lugar a dudas, importante para ejercer más fácilmente y con mayor posibilidad de éxito, el derecho de acceso recogido en el artículo 15. En el mismo sentido se expresa el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos <sup>(22)</sup>.

El artículo 15 de la ley garantiza el derecho de acceso del interesado al tratamiento de datos que sobre ellos se están realizando. La ley española otorga mayores derechos al interesado que la legislación comunitaria, pues establece entre otras, la gratuidad de la consulta, que la Directiva fija en «sin gastos excesivos», estableciendo así mismo el concepto genérico de «periodicidad razonable», para acceder por parte del interesado al tratamiento que sobre sus datos se están realizando. Por su parte, la ley española entiende que esta «periodicidad razonable» lo es, siempre y cuando, el derecho de acceso por parte del interesado, a solicitar y obtener información gratuita de sus datos de carácter personal sometidos a tratamiento, lo sea a intervalos no inferiores a doce meses, eso sí, se exceptúan aquellos casos en los que el interesado acredite un interés legítimo al efecto, en cuyo caso, podrá ejercitarlo con antelación.

Las excepciones y limitaciones al derecho de acceso vienen recogidas en los artículos 23 y 24 de la LOPD, dentro de las disposiciones sectoriales, referidas a los ficheros de titularidad pública, artículo este último que, junto con el artículo 21 de la LOPD, han sido objeto de declaración de inconstitucionalidad parcial por el Tribunal Constitucional en Sentencia 292/2000 <sup>(23)</sup>. Estas excepciones y limitaciones vienen a hacerse eco de lo establecido en el artículo 13 de la Directiva 95/46/CE, ajustándose, como dice Herran Ortiz <sup>(24)</sup>, a unas concretas condiciones que delimita la propia Directiva, como el hecho de que la limitación se establezca en una disposición legal y que no concurra riesgo de atentado contra el interesado, lo que no excluye que deban adoptarse las garantías legales apropiadas y que los datos sean tratados únicamente con fines estadísticos o de investigación científica.

No creemos que resulte muy apropiada la sistemática utilizada por la propia Ley al referirse a las excepciones del derecho de acceso, rectificación y cancelación, toda vez que, si bien dedica el Título III a hablar de los derechos de las personas, es en este lugar en el que, al final de todo el listado de derechos y por una cuestión de sistemática, deberían de recogerse las excepciones y limitaciones a los mismos, y no dentro del capítulo I «ficheros de Titularidad pública» del Título IV relativo a Disposiciones

<sup>(22)</sup> Vide apartado 2.º del artículo 4, artículo 7 y artículo 23 del Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. («BOE» núm. 106, de 4 de mayo de 1993).

<sup>(23)</sup> Vide Sentencia 292/2000 de 30 de noviembre del Pleno del Tribunal Constitucional en Recurso de inconstitucionalidad 1463/2000, promovido por Defensor del Pueblo. «BOE» núm. 4 Suplemento, de 4 de Enero de 2001.

<sup>(24)</sup> Vide anotación 13.

Sectoriales, haciendo una traslación literal de la sistemática de la LORTAD <sup>(25)</sup>, dejando escapar la oportunidad que se le ofrece al legislador para subsanar una sistemática que consideramos no del todo apropiada.

El artículo 16 de la LOPD amplía a diez días <sup>(26)</sup> el plazo para proceder a la rectificación o cancelación de los datos del interesado, lo que implica una previa actuación por parte del interesado. Igualmente, parece deducirse que el responsable del tratamiento deberá proceder de oficio a la rectificación de los datos inexactos o incompletos, o a la cancelación cuando éstos no se ajusten a lo dispuesto la ley, lo que implica un deber de velar por la veracidad de los datos por parte del responsable del tratamiento. La ley a su vez también establece mecanismos para la cancelación o rectificación de los datos contenidos en determinados registros públicos y prevé que las leyes impongan plazos a partir de los cuales los datos caducarán y deberán ser eliminados, así como una comunicación en cascada a los cesionarios para que procedan a su rectificación o cancelación, todo ello sin perjuicio de que los datos bloqueados puedan conservarse a disposición de las Administraciones públicas, Jueces y Tribunales para la atención de posibles responsabilidades.

El artículo 17 de la ley nos habla del procedimiento a seguir para el ejercicio de los derechos de oposición, acceso, rectificación o cancelación y dispone que estos serán «establecidos reglamentariamente». A este respecto, ya se pronunció Ramos Méndez <sup>(27)</sup>, cuando al hablar de la LORTAD, consideraba razonable el reenvío al Reglamento, pues «no es necesario ni prudente que la Ley ( más general y duradera, de más difícil modificación que su reglamento) se comprometa con detalles que pueden regularse más precisamente después». Solo añadir que la LOPD expresamente recoge la gratuidad de los citados procedimientos.

Al igual que la Directiva 95/46/CE en su artículo 22, la Ley española en su artículo 18 establece que la tutela de derechos enumerados en esta ley podrá llevarse a cabo por vía judicial con posterioridad al recurso administrativo interpuesto ante la autoridad de control, que en el caso español será la Agencia de Protección de Datos o institución autonómica equivalente. Así mismo la ley nos indica el plazo máximo para la resolución expresa de tutela, estableciéndolo en seis meses. Contra las resoluciones de la autoridad de control, procederá interponer el correspondiente recurso contencioso-administrativo. Como dice Vizcaíno Caldera <sup>(28)</sup>, no solo son reclamables los derechos recogidos en el artículo 18, sino que, también «...podrían ser objeto de reclamación la recogida de datos de los afectados sin proporcionarles la comunicación a que se refiere el artículo 5; la recogida de datos en forma engañosa o fraudulenta; el incumplimiento del deber de secreto respecto de los datos del reclamante; la cesión o comunicación de datos sin consentimiento del afectado en los casos en que dicho consentimiento no esté exceptuado; la falta de información al afectado cuando los datos no hayan sido recabados del interesado en los supuestos del artículo 5.4 de la Ley; la

---

<sup>(25)</sup> Vide a este respecto la derogada Ley Orgánica 5/1992, de 29 de octubre de regulación de Tratamiento Automatizado de los Datos de carácter personal, «BOE» 262 de 31 de octubre.

<sup>(26)</sup> Obsérvese la norma cuarta de la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, que establece el plazo en cinco días.

<sup>(27)</sup> RAMOS MÉNDEZ, Eduardo y otros, «informática jurídica», p. 219 y ss; UNED 1994.

<sup>(28)</sup> Ver VIZCAÍNO CALDERA, Miguel «Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal», p. 215 y ss; Editorial Civitas 2001.

recogida de datos especialmente protegidos, sin consentimiento expreso o por escrito; el tratamiento de datos sin consentimiento del afectado cuando este consentimiento sea necesario; la continuidad en el tratamiento pese a la revocación en el consentimiento notificada fehacientemente al responsable del fichero...»

El artículo 19 de la Ley española se hace eco de lo establecido en el artículo 23 de la Directiva en cuanto a responsabilidad por perjuicios a las personas derivados del incumplimiento de las disposiciones establecidas en la misma <sup>(29)</sup>, al regular la posibilidad de indemnización por daños sufridos «como consecuencia del incumplimiento de lo dispuesto en la Ley Orgánica 15/1999 de protección de datos y que deberán ser satisfechos por el responsable o encargado del tratamiento. Si bien, distingue entre ficheros de titularidad pública, exigiéndose la responsabilidad conforme a la legislación reguladora del régimen de responsabilidad de las Administraciones públicas, y ficheros de titularidad privada ejercitándose la acción, en estos casos, ante la jurisdicción ordinaria.

De la conjunción de estos dos artículos, se puede concluir que, si un individuo reclama la cancelación de los datos de un determinado fichero de titularidad privada que le está produciendo un perjuicio, la correspondiente autoridad de control le notifica después de seis meses que no ha lugar a tal reclamación, se inicia entonces la vía contencioso-administrativa que después de varios años de pleito le otorga su derecho. Con esta resolución, y si no se produce apelación por parte del responsable o el encargado del tratamiento, se inicia la vía ordinaria para obtener la indemnización por la lesión de sus derechos. Si se dice que la justicia que no es rápida no es justicia, nos hallamos ante un procedimiento poco justo e ineficaz, puesto que las trabas que se imponen al actor son suficientes como para que esté desista de la pretensión.

## 5. Movimiento Internacional de Datos

La Ley Orgánica 15/1999 dedica el Título V, como venía haciendo la derogada LORTAD, al movimiento internacional de datos de carácter personal, siendo este, tal y como establece la Instrucción 1/2000 de la Agencia de Protección de Datos, una de las cuestiones que ha suscitado un mayor número de dudas por parte de los responsables de los ficheros y de la sociedad en general. Se trata pues de conciliar la protección de los datos de carácter personal, con el libre flujo de los mismos, optándose por exigir que el país de destino cuente en su ordenamiento con un sistema que garantice un nivel de protección «adecuado» <sup>(30)</sup>. Así, el artículo 33,1 de la ley establece, como norma general, los mismos requisitos para la transferencia internacional de datos que la Directiva 95/46/CE en su artículo 25.1, si bien, la Ley le otorga al Director de la Agencia de Protección de Datos, en virtud de lo establecido en la Directiva, la potes-

---

<sup>(29)</sup> El artículo 23, apartado 1.º de la Directiva 95/46/CE, establece: «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».

<sup>(30)</sup> En este sentido se expresa la Directiva 95/46/CE cuando en el apartado primero de su artículo 25 establece como criterio a valorar a la hora de transferir datos personales a países terceros, el que «el país tercero de que se trate, garantice un nivel de protección adecuado».

tad, como la persona responsable, de dar la autorización a la transferencia internacional si se obtienen las garantías adecuadas.

En el artículo 33.2 de la LOPD encontramos los criterios para considerar cuando un país proporciona un nivel de protección adecuado (la Directiva usa el término «nivel de protección adecuado», en el artículo 33.2 de la Ley se utiliza el término «carácter adecuado del nivel de protección», sin embargo, el artículo 33.1 de la misma, al ser copia literal y calcada del artículo 32 de la LORTAD<sup>(31)</sup> utiliza el término de «protección equiparable», lo cual, no hace sino añadir confusión al texto, pues un término similar, «nivel de protección equivalente» es el utilizado por el Convenio 108 del Consejo de Europa cuando en la letra a) del apartado 3 de su artículo 12 al hablar de las excepciones, claramente establece «...a menos que la reglamentación de la otra Parte establezca una protección equivalente...»<sup>(32)</sup> tal y como dice Herran Ortiz), al igual que hace la Directiva en el artículo 25.2.

El artículo 34 de la Ley 15/1999, establece el régimen de excepciones a la autorización para la transferencia de datos, debiendo tenerse en cuenta, a este respecto, tal y como establece la Instrucción número 1/2000 de la Agencia de Protección de Datos, «... las Decisiones de la Comisión de las Comunidades Europeas, números 2000/518/CE, 2000/519/CE, 2000/520/CE, de 26 de Julio, que consideraron adecuado, entre otros, el nivel de protección de datos personales en Suiza, Hungría...» Así mismo, el Director de la Agencia de Protección de Datos, previa audiencia del transmitente, podrá acordar la suspensión temporal de la transferencia de datos a un tercer estado, cuando, aún teniendo un nivel adecuado de protección, las Autoridades de Protección de datos de ese estado, resuelvan que el destinatario ha vulnerado las normas de protección de datos de su derecho interno, o que existan indicios racionales de que se estén vulnerando las normas de protección de datos por el destinatario de la transferencia<sup>(33)</sup>.

A mayor abundamiento, la Directiva añade en su artículo 25.3 la obligación entre los países y la Comisión de informarse acerca de aquellos países que no «garantizan un nivel de protección adecuado», de forma, que si esta información es fluida, en poco tiempo se conseguirá una lista a nivel mundial de cuáles son los países a los que se puede realizar una transferencia de datos y a cuáles no.

En el artículo 25.4 de la Directiva nos encontramos con una prescripción dirigida a los países por la cual mediante ratificación de la Comisión acerca del nivel de protección que hallamos en un país determinado, los Estados miembros deberán tomar las medidas necesarias tendentes a evitar las transferencias de datos a dicho país.

El artículo 25 apartados 5 y 6 nos dice que la Comisión podrá iniciar negociaciones y emitir un informe al final de estas, en el cual se recoja si un país tercero «a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones a efectos de protección de la vida privada o de las li-

---

<sup>(31)</sup> Ver a este respecto la derogada Ley Orgánica 5/92, de 29 de octubre de regulación de Tratamiento Automatizado de los Datos de carácter personal, «BOE» 262 de 31 de octubre.

<sup>(32)</sup> Ver Convenio 108 del Consejo de Europa, de 28 de enero de 1981, sobre Garantías Individuales. Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. «BOE» 15 noviembre 1985 (núm. 274).

<sup>(33)</sup> Obsérvese la norma cuarta de la Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.

bertades o de los derechos fundamentales de las personas», garantiza o no un nivel de protección adecuado. Obligando a los Estados miembros a adoptar las medidas necesarias para el cumplimiento de los acuerdos alcanzados en esas negociaciones.

En lo que respecta a las excepciones a las transferencias de datos a países terceros, la LOPD establece una serie de requisitos similares a los que también se hallan recogidos en la Directiva. Así, la ley española recoge en los apartados *e)*, *f)* y *g)* del artículo 34 de forma idéntica lo establecido en los apartados *a)*, *b)* y *c)* del artículo 26 la Directiva. El resto de apartados del artículo 34 de la LOPD excepto el apartado *k)* son una extensión o una muestra con más detalle de aquello que la Directiva llama «interés público importante», «ejercicio o defensa de un derecho en un procedimiento judicial», «salvaguardia de interés vital del interesado» o «transferencia... en virtud de disposiciones legales o reglamentarios». El apartado *k)* de la LOPD, obviamente no tiene reflejo en las excepciones previstas en el artículo 26 de la Directiva 95/46CE, ya que, si uno de los fines de esta es la libre circulación de datos dentro de la Comunidad, sería redundante el que un apartado de su articulado recogiera esta obligación que forma parte del espíritu informador de la misma.

Por otro lado, la Directiva establece un mecanismo mediante el cual los responsables del tratamiento a través de acuerdos contractuales puedan garantizar un nivel adecuado de protección, haciendo de esta manera inútil todas las precauciones recogidas en el articulado de la misma, ya que incluyendo «cláusulas contractuales apropiadas»(sic), se pueden burlar las precauciones que toma la Directiva para evitar que los datos lleguen a países con un nivel de protección no adecuado. Sin embargo, trata de salvarlo incluyendo un procedimiento de control mediante el cual los Estados miembros tendrán que informar a la Comisión y a los demás países miembros de los acuerdos que realicen para la transferencia de datos a países terceros que no proporcionen un nivel de protección adecuado y si se opusiere un país, o la propia Comisión, esta emitirá un dictamen que obligará a los países miembros a tomar las medidas necesarias para su cumplimiento. Sin embargo, dicha garantía queda en papel mojado, toda vez que la transferencia ya habrá sido realizada en el momento en el que obtenga la autorización por parte de la autoridad de control nacional. Así, la Instrucción 1/2000 de la Agencia de Protección de Datos, recoge este mismo procedimiento, si bien, para evitar la posible indefensión de los perjudicados ante la posibilidad de sentencias judiciales o resoluciones administrativas que no sean reconocidas en el país al que se realizó la transferencia de datos, establece un régimen de solidaridad en la responsabilidad entre el transmitente y el destinatario <sup>(34)</sup>.

## 6. Conclusiones

No es nuestra intención hacer un memorándum a modo de conclusiones que aburra al lector, toda vez que nuestra opinión y crítica ha sido vertida a lo largo de la exposición del presente trabajo de investigación al que en todo momento nos remitimos, sin pretensión de agotar el potencial crítico que toda ley tiene, más aun cuando esta es el resultado de una transposición con la que podemos estar o no de acuerdo.

<sup>(34)</sup> Vide norma quinta de la Instrucción 1/2000, .... vide anotación 32.

Huelga decir que la LOPD garantiza lo que constituye el núcleo básico de protección de los derechos fundamentales mediante la articulación de un haz de derechos como son el derecho de información, acceso, oposición al tratamiento, rectificación, cancelación y bloqueo de datos, articulando unos métodos en cuanto a la recogida de datos y su tratamiento que hacen que los referidos derechos no se hayan de ejercitar de forma masiva.

En otro orden de cosas, podemos considerar hasta cierto punto comprensible que la Directiva goce de una cierta permisividad a la hora de utilizar conceptos jurídicos indeterminados que permitan realizar una transposición que aproxime las distintas legislaciones de los estados miembros y que no obligue a los mismos a reproducir literalmente los preceptos obrantes en la directiva —en cuyo caso hablaríamos de un Reglamento encubierto—. Por su parte, la ley española no acaba de eliminar la excesiva cantidad de conceptos jurídicos indeterminados que la directiva maneja, asunto este poco deseable, máxime cuando hablamos de derechos fundamentales, pues estos habrán de ser delimitados posteriormente por vía jurisprudencial.

No quisiéramos terminar este trabajo sin hacer una breve mención a la carencia, por parte de la LOPD, de una exposición de motivos, a diferencia de la anterior Ley que regulaba la materia —LORTAD—, como de la propia Directiva 95/46/CE, que posee un amplio número de Considerandos previos al articulado y por medio de los cuales el legislador europeo deja entrever las claves para interpretar su intencionalidad a la hora de establecer un amplio marco que sea punto de inicio para aproximar las legislaciones existentes y a su vez referente mínimo en la protección de datos personales a nivel Comunitario.

Si bien, un sector doctrinal defiende que el espíritu de las leyes se puede obtener de las intervenciones realizadas por los parlamentarios durante las sesiones de debate en las Cortes, dudamos que estas puedan ser utilizadas como verdadera fuente del derecho que nos permita no solo suplir las dificultades interpretativas que toda ley conlleva, sino facilitar el acercamiento de los ciudadanos a un texto normativo que contiene las claves para la protección de sus datos de carácter personal, y cuyo último fin es garantizar y proteger las libertades públicas y los derechos fundamentales.

Por último, solo referirnos al hecho de que cuando hablamos de las garantías mínimas que establece la comunidad con respecto al tratamiento de datos, no debemos creer que lo hace únicamente con la buena intención de elevar la protección de los derechos fundamentales de la persona, sino que lo hace con la intención más pragmática de evitar que se pongan trabas a la transferencia internacional de datos, lo cual, supondría importantes pérdidas económicas y un retraso en el desarrollo del comercio, tanto intra como extracomunitario, puesto que la regulación respecto de la protección de datos de carácter personal, y por consiguiente del derecho a la intimidad, que realiza nuestro principal adversario comercial -Estados Unidos-, se halla muy por debajo de la protección de estos derechos.

## 7. Bibliografía, Legislación y Jurisprudencia

ALONSO MARTÍNEZ, Carlos, *El consentimiento del interesado en protección de datos*; Universidad Pontificia de Comillas, Madrid. XIV, Encuentros sobre Informática y Derecho 2000-2001, editorial Aranzadi.

- GARRIDO FALLA, Fernando y otros: *Comentarios a la Constitución Española*, 3.ª Edición. 2001, editorial Civitas.
- HERRAN ORTIZ, Ana Isabel: *España: La protección de datos personales en el marco de la Unión Europea*. 2001, editado en Revista Electrónica de Derecho Informático; vlex.com.
- RAMOS MÉNDEZ, Eduardo y otros: *Informática Jurídica*, 1994. UNED
- VIZCAÍNO CALDERA, Miguel: *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, 2001, Editorial Civitas.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. («BOE» núm. 298, de 14 de diciembre).
- Convenio 108 del Consejo de Europa, de 28 de enero de 1981, ratificado por Instrumento 27 enero 1984 (Jefatura del Estado). Garantías Individuales. Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. («BOE» núm. 274, de 15 noviembre 1985).
- Ley Orgánica 5/1992, de 29 de octubre de Regulación de Tratamiento Automatizado de los Datos de carácter personal («BOE» núm. 262, de 31 de octubre).
- Ley 48/1978 de Secretos Oficiales de 7 de octubre, («BOE» núm. 243, de 11 de octubre de 1978).
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. («BOE» núm. 106, de 4 de mayo de 1993).
- Real Decreto 1736/1998, de 31 de julio, por el que se aprueba el Reglamento por el que se desarrolla el título III de la Ley General de Telecomunicaciones, en lo relativo al servicio universal de telecomunicaciones, a las demás obligaciones de servicio público y a las obligaciones de carácter público en la prestación de los servicios y en la explotación de las redes de telecomunicaciones. («BOE» núm. 213, de 5 de septiembre).
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal. («BOE» núm. 151, de 25 de junio).
- Real Decreto 195/2000 de 11 de febrero por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el reglamento aprobado por el Real Decreto 994/1999 de 11 de Junio. («BOE» núm. 49, de 26 de febrero de 2000).
- Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. («BOE» núm. 25, de 29 de enero).

Instrucción 1/2000, de 01 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.

Sentencia 292/2000 de 30 de Noviembre del Pleno del Tribunal Constitucional en Recurso de inconstitucionalidad 1463/2000, promovido por Defensor del Pueblo. «BOE» núm. 4 Suplemento, de 4 de enero de 2001.