

SABERES

Revista de estudios jurídicos, económicos y sociales

VOLUMEN 1 ~ AÑO 2003

Separata



TRIDIMENSIONALISMO JURÍDICO Y PROTECCIÓN DE DATOS PERSONALES FRENTE A SU TRATAMIENTO AUTOMATIZADO

María Antonia Rodríguez Pérez



UNIVERSIDAD ALFONSO X EL SABIO
Facultad de Estudios Sociales
Villanueva de la Cañada

© María Antonia Rodríguez Pérez

© Universidad Alfonso X el Sabio
Avda. de la Universidad,1
28691 Villanueva de la Cañada (Madrid, España)

Saberes, vol. 1, 2003

ISSN: 1695-6311

No está permitida la reproducción total o parcial de este artículo ni su almacenamiento o transmisión, ya sea electrónico, químico, mecánico, por fotocopia u otros métodos, sin permiso previo por escrito de los titulares de los derechos.

TRIDIMENSIONALISMO JURÍDICO Y PROTECCIÓN DE DATOS PERSONALES FRENTE A SU TRATAMIENTO AUTOMATIZADO*

María Antonia Rodríguez Pérez**

RESUMEN: Estudio del Derecho de la protección de datos personales desde una triple perspectiva. El Derecho de la protección de datos personales no escapa al Tridimensionalismo jurídico, pues es una materia más de las múltiples que encierran una dimensión fenomenológica (hecho), una dimensión axiológica (valor) y otra dimensión jurídica (norma). Bajo este planteamiento, se profundiza en cada una de las tres líneas de observación presentes en la cuestión abordada.

PALABRAS CLAVE: Tridimensionalismo, bases de datos, datos personales.

SUMARIO: 1. Tridimensionalismo jurídico y protección de datos personales.– 2. El hecho: la potencial agresividad de la informática en el tratamiento de los datos personales.– 3. El valor: la intimidad.– 4. La norma: derecho de la protección de datos personales.– 4.1. Derecho comunitario.– 4.2. Derecho español: la ley orgánica 5/1992 de regulación del tratamiento automatizado de datos de carácter personal.– 4.2.1. Título I.– Disposiciones Generales.– 4.2.2. Título II.– Principios de la protección.– 4.2.3. Título III.– Derechos de las personas.

1. Tridimensionalismo jurídico y protección de datos personales

La posibilidad de estudiar el Derecho contemplándolo desde tres puntos de vista quedó plasmada en la obra de autores como Icilio Vanni, Giorgio Del Vecchio, Miguel Reale, Recaséns Siches, Legaz Lacambra, Bobbio, Pátaro, etc.

Así, Giorgio Del Vecchio entendió que:

La Filosofía del Derecho comprende, pues, tres temas o investigaciones (lógica, fenomenológica y deontológica) y puede definirse como sigue: la Filosofía del Derecho es la disciplina que define el Derecho en su universalidad lógica, investiga los fundamentos y los caracteres generales de su desarrollo histórico y lo valora según el ideal de la justicia trazado por la pura razón¹.

* Publicado inicialmente en <http://www.uax.es/iurisuax> año 1999.

** Master en Informática y Derecho UCM. Profesora de de Informática Jurídica. Universidad Alfonso X el Sabio. Abogada especialista en Nuevas Tecnologías.

¹ Del Vecchio, G., *Filosofía del Derecho*. 2ª Ed., Bosch, Barcelona, 1935.

En la misma línea, Recaséns Siches afirma que el derecho:

[...] es una norma, con especiales características, elaborada por los hombres con el propósito de realizar unos valores. En esta concepción se observan las tres dimensiones de las que se ha venido hablando - valor - norma - hecho; pero indisolublemente unidas entre sí, en relaciones de esencial implicación. El Derecho no es un valor puro, ni es una mera norma con ciertas características especiales, ni es un simple hecho social con notas particulares. El Derecho es una obra humana social (hecho) de forma normativa, encaminada a la realización de los valores².

Luis Legaz Lacambra distingue en el Derecho una triple dimensión, como valor, como hecho y como norma. Dimensiones con las que se corresponden los tres aspectos de la validez jurídica que a su juicio merecen ser destacados: validez ética, validez sociológica o eficacia y validez jurídica o vigencia.

A partir de aquí mi estudio abordará las tres dimensiones que, según la Teoría Tridimensionalista, cabe apreciar en materia de protección de datos personales.

En primer lugar, la dimensión fenomenológica, esto es, el hecho desencadenante de la necesidad de protección jurídica: la aportación de datos personales, su combinación y las consecuencias fácticas que de ello se derivan.

A continuación, la perspectiva ética, axiológica, en suma, el valor. En nuestro caso la intimidad en tanto puede ser lesionada si el tratamiento de los datos personales se realiza mediante un uso abusivo de los medios informáticos. deben ser destacadas aquí tres cuestiones: el contenido del derecho a la autodeterminación informativa, el equilibrio entre los derechos que coexisten en esta disciplina y la distinción entre intimidad y privacidad.

Por último, la perspectiva jurídica, la norma, tanto los antecedentes comunitarios, como la normativa española, que hace especial hincapié en los principios inspiradores de su articulado y los derecho que reconoce.

2. El hecho: la potencial agresividad de la informática en el tratamiento de los datos personales

² Recasens Siches, L., Tratado General de Filosofía del Derecho, 7ª Ed., Porrúa, México, 1981.

En la sociedad actual, con frecuencia, nos encontramos con el requerimiento de instituciones, públicas y privadas, de proporcionar determinados datos sobre nuestra persona.

Esa solicitud suele fundarse en el bien común, el interés social o, sin más, para facilitar que se nos preste un servicio de manera más eficaz.

La vida misma exige continuas revelaciones de datos personales, pero revelaciones limitadas a personas concretas para fines predeterminados y en la creencia de que no serán objeto de conocimiento general.

De este modo se dispone de un conjunto de datos que, convenientemente tratados de forma automática, en relación con un fin determinado, proporcionan información sobre la persona.

La inteligencia artificial ofrece hoy la posibilidad de comparar, interrelacionar y analizar los datos de una persona, proporcionando un perfil de la misma. Pero, además, cabe que la comparación se establezca respecto de un modelo o perfil predeterminado, advirtiendo de los datos de la persona que se desvían del modelo y poniendo a disposición del responsable del fichero información sobre las conclusiones que se derivan de esa desviación.

Si a todo esto se añade la ayuda que proporcionan las comunicaciones y la transferencia de datos telemáticos, puesto que permiten el cruce de ficheros y registros informáticos, así como el correspondiente tratamiento de los mismos, nos encontramos con que la persona pierde el control sobre la utilización que se pueda hacer de sus datos personales y que la información parcial proporcionada en un principio, de por sí valiosa, se convierte en valiosísima, con lo que ello significa en el aumento de la cota de poder del responsable del fichero, esto es, la persona física o jurídica, pública o privada, que decide sobre la finalidad, contenido y uso del fichero y su tratamiento.

Y es que, como se apunta en Exposición de Motivos de la LORTAD, las modernas tecnologías de comunicación permiten salvar las defensas naturales de la intimidad: el tiempo y el espacio; el tiempo porque su transcurso daba lugar al olvido y el espacio porque impedía saber lo que había ocurrido en un lugar lejano, así como porque permitía escapar a la curiosidad ajena, mediante el traslado a otro lugar.

Pero la posibilidad actual de almacenar los datos del pasado y acceder a ellos en cuestión de segundos, con independencia del lugar o el momento, más o menos remoto, en que hayan sido almacenados, ha eliminado aquellas barreras naturales. (Pensemos en la INTERNET y la velocidad que podemos alcanzar para recuperar una información).

De ahí el temor a que el uso de la informática pueda violar el derecho a la intimidad y coartar el ejercicio pleno de los derechos de la persona.

Es por ello que se plantea la necesidad de que desde el ordenamiento jurídico se otorgue al ciudadano el amparo debido, frente a la potencial agresividad de la informática.

3. El valor: la intimidad

Dado que, técnicamente, es posible confeccionar una información que proporcione conclusiones sobre el comportamiento, ideología, aficiones, enfermedades, etcétera de la persona y que, identificándola con ella afecte a su entorno personal, social o profesional en los límites de su intimidad, en el constitucionalismo democrático contemporáneo ha adquirido creciente actualidad el derecho a la autodeterminación informativa.

Derecho al que la doctrina más autorizada da la consideración de fundamental, con base en el artículo 18.4 de la Constitución Española (Entre otros, Frosini, Losano, Pérez Luño, Davara).

Así, De Lucas³ afirma que se trata de un derecho fundamental con independencia de su carácter instrumental, pues, «en último extremo, todos lo son respecto de la dignidad humana. De modo que puede considerarse como un instrumento al servicio de la intimidad y la libertad personales». Afirma también que la existencia de este derecho «no es más que llegar a la conclusión latente en el precepto constitucional», que al remitir al legislador la limitación del uso de la informática, no está sino prohibiendo «la destrucción de la autodeterminación informativa a causa de un uso abusivo de la informática».

Qué se entiende por derecho a la autodeterminación informativa. La construcción del concepto se debe a la doctrina y jurisprudencia alemanas, que lo definen, en palabras de Pérez Luño, como «la libertad para determinar quién, qué y con qué ocasión pueden conocer informaciones que conciernen a cada sujeto»⁴.

En este sentido fue decisiva la sentencia del Tribunal Constitucional Federal Alemán de 15 de diciembre de 1983 sobre la Ley del censo de población, que reconocía este derecho y consagraba las facultades y

³ De Lucas Murillo De La Cueva, P., El derecho a la autodeterminación informativa, Tecnos, 1990.

⁴ Pérez Luño, A. E., Manual de Informática y Derecho, Ariel, Barcelona, 1996.

garantías básicas de los ciudadanos en orden a la información, el acceso y control de sus datos personales.

Ahora bien, como señala el Profesor de Lucas, la salvaguarda del derecho a la autodeterminación informativa ha de estar en equilibrio con el respeto a otros derechos, especialmente el reconocido en el artículo 20.1.d) de la Constitución Española, esto es, el derecho fundamental a comunicar y recibir libremente información veraz por cualquier medio de difusión.

De modo que el régimen jurídico de la protección de datos debe tener la menor incidencia posible en los derechos que colisionan con la autodeterminación informativa. Y a la inversa, ya que ese derecho a comunicar y recibir libremente informaciones está limitado constitucionalmente, en virtud del artículo 20.4 de la Constitución Española, por el respeto a los derechos fundamentales y especialmente al derecho al honor, la intimidad, la protección de la juventud y la infancia, y a la propia imagen.

En nuestro Derecho, la protección de la intimidad estaba regulada ya, de modo general, en la Ley Orgánica 1/82 de 5 de mayo, de protección civil del derecho al honor, la intimidad personal y familiar, y la propia imagen. Alcanzando dicha protección a la esfera en la que se desarrollan las facetas más singularmente reservadas de la vida de la persona. Porque en el domicilio se realiza la vida cotidiana y a través de las comunicaciones la persona expresa sentimientos.

Pero el Derecho a la Protección de Datos va más allá. Tiene como fin proteger la intimidad frente a su violación mediante el tratamiento automatizado de los datos personales o uso abusivo de la informática. Y por eso introduce un nuevo concepto: privacidad (término que resulta de la castellanización del vocablo anglosajón *privacy*) que añade un plus al concepto de intimidad. Es el:

Conjunto, más amplio, más global, de facetas de la persona que, aisladamente consideradas, pueden carecer de significación intrínseca, pero que, coherentemente enlazadas entre sí arrojan un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado (Exposición de Motivos de la LORTAD- LO 5/92).

Esta distinción entre intimidad y privacidad es contemplada por nuestro legislador en la Exposición de Motivos de la LORTAD –LO5/92, entendiéndose que la intimidad queda protegida por las previsiones de los artículos 18.1, 2 y 3 CE, mientras que la privacidad puede resultar menoscabada por la utilización torticera de la informática. Con lo que su

amparo constitucional reside en el artículo 18.4 CE y constituye el bien jurídico que se trata de proteger con el derecho a la autodeterminación informativa, o lo que es lo mismo, la libertad para decidir quién, qué y cómo puede conocer informaciones concernientes a la persona que ésta tiene derecho a mantener reservadas.

4. La norma: derecho de la protección de los datos personales

4.1. Derecho comunitario

Esta problemática de la protección de la privacidad frente a la potencial agresividad de las tecnologías de la información y comunicación ha sido objeto de regulación por los Ordenamientos de nuestro entorno y por del Derecho Comunitario.

El estudio, en el marco de la Unión Europea, de lo que se ha venido a llamar "Derecho de la Protección de Datos" se inició a finales de los años sesenta con una serie de Resoluciones y Recomendaciones.

La protección de datos se entiende como el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad.

En 1981 el Convenio 108 del Consejo de Europa para "la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", hecho en Estrasburgo y ratificado por España en 1984, obligaba a los signatarios a incorporar las normas de aplicación que permitieran realizar los principios allí consagrados, de manera eficaz.

El segundo paso estuvo protagonizado por la firma del Acuerdo de Schengen en 1985. Tal acuerdo pretendía la eliminación paulatina de fronteras entre los países signatarios, inicialmente Alemania, Francia y los países del Benelux, y más tarde otros de la Unión Europea, incluido España.

Tal objetivo necesitaba de una fluida transmisión de información que, bajo el imperio de la legislación francesa, se hizo depender de la colaboración policial y de la existencia en los Estados firmantes de las normas de aplicación del Convenio 108 antes señalado.

La Unión Europea también aprobó la Directiva 95/46 CE "sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de éstos". Esta Directiva pretende

armonizar la fluidez de la transmisión de datos en el seno de la Unión Europea para mayor eficacia de los poderes públicos y desarrollo del sector privado con la defensa de los datos personales. También prevé la existencia en cada Estado miembro de una autoridad independiente para garantizar la tutela de los datos personales y velar por la correcta aplicación de la Directiva. (En España esa autoridad es la Agencia de Protección de Datos). Así mismo, contempla la existencia de una autoridad comunitaria para la interpretación homogénea de las normas nacionales e informar a la Comisión de los conflictos entre normas y prácticas de los Estados.

4.2. Derecho español: La Ley Orgánica 5/1992 de regulación del tratamiento automatizado de los datos de carácter personal

Los compromisos derivados del Convenio 108, del Acuerdo de Schengen y la inminente aprobación que se avecinaba de la Directiva de Protección de Datos 95/46, determinaron, junto al mandato constitucional recogido en el artículo 18.4, la promulgación, aunque tarde, de la Ley Orgánica 5/92, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE nº 262, de 31 de octubre de 1992).

Ley, que, tras una larga exposición de motivos, se estructura del siguiente modo:

Una primera parte, general o dogmática, proclama los derechos derivados de la autodeterminación informativa, en cuyo Título I formula las disposiciones generales referidas a su objeto, ámbito y definiciones. En el Título II recoge los principios de la protección de datos y en el Título III se refiere a los derechos que garantizan el reconocimiento de la autodeterminación informativa.

La segunda parte, especial u orgánica, versa sobre los mecanismos a que deben acomodarse las bases de datos personales. El Título IV regula los ficheros de titularidad pública y privada. El Título V disciplina el movimiento internacional de datos. El Título VI regula la naturaleza y régimen jurídico de la Agencia de Protección de Datos. Y, por último, el Título VII tipifica las infracciones y sanciones.

4.2.1. Título I.- Disposiciones Generales.

En desarrollo del artículo 18.4 CE limita el uso de la informática y de las técnicas y medios de tratamiento automatizado de los datos de carácter

personal, con el fin de garantizar el honor, la intimidad personal y familiar de las personas físicas y el ejercicio pleno de sus derechos.

Es de aplicación a datos de carácter personal registrados en soporte físico, esto es, ficheros, ya públicos, ya privados, susceptibles de tratamiento automatizado y su uso posterior automatizado o no.

Se excluyen del ámbito de aplicación de la LORTAD: los ficheros públicos cuyo objeto, legalmente establecido, sea publicar los datos con carácter general; los ficheros de personas físicas, para fines personales; los ficheros de información tecnológica y comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales; los ficheros de informática jurídica que reproducen resoluciones judiciales publicadas en periódicos o repertorios oficiales (accesibles al público); los ficheros de los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas (si bien, estos tienen un tratamiento especial en la propia LORTAD), de datos que se refieran a sus miembros o a sus ex - miembros.

Por su parte, tienen regulación específica los ficheros siguientes: los regulados por la legislación de régimen electoral (LO 5/85); los sometidos a normativa sobre protección de materias clasificadas (L9/68 de secretos oficiales, modificada por L 48/78); los derivados del Registro Civil (LRC de 8 de junio de 1957) y del Registro Central de Penados y Rebeldes; los que sirven a fines exclusivamente estadísticos (L 12/89 de la función estadística pública), cuya recogida, control, secreto estadístico, condiciones de seguridad, potestad sancionadora e inicio de actuaciones disciplinarias corresponde a la Agencia de Protección de Datos; y los ficheros de datos de los informes personales regulados en el artículo 68 de la L 17/89, reguladora del régimen del personal militar profesional.

El artículo 3 de la LORTAD recoge las definiciones de los conceptos siguientes:

- Datos de carácter personal: informaciones concernientes a las personas físicas identificadas o identificables.
- Fichero automatizado: conjunto organizado de datos personales que sean objeto de tratamiento automatizado, cualquiera que fuese la forma de su creación, almacenamiento, organización y acceso.
- Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo o cancelación y cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- Responsable del fichero: persona física o jurídica, pública o privada, u órgano administrativo que decida sobre la finalidad, contenido o uso del tratamiento.
- Afectado: persona física titular de los datos.

- Procedimiento de disociación: tratamiento de datos personales, de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable.

4.2.2. Título II.- Principios de la protección.

Coincido con Davara⁵ en que el criterio clasificador de estos principios debe ser temporal. Debe atender al momento en que entra en juego cada uno de ellos.

a) Relativos a la toma o recopilación de los datos:

- Principio de pertinencia: en virtud del cual sólo se puede recoger los datos que sean adecuados, pertinentes y no excesivos al fin legítimo que se persigue con la creación del fichero. Cuando dejen de ser pertinentes o necesarios deben ser cancelados.
- Principio de lealtad: - siguiendo la denominación de Del Peso⁶ - prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos. Lo contrario se califica como infracción muy grave, correspondiendo una sanción de multa de 50 a 100 millones de pesetas.
- Principio de información: se debe informar al interesado al que se solicitan los datos de modo expreso, preciso e inequívoco de: la existencia del fichero automatizado, la finalidad con que se recogen los datos y los destinatarios de la información; si debe responder obligatoriamente; las consecuencias de que los proporcionen o se nieguen a suministrarlos; los derechos que tienen de acceso, rectificación y cancelación; así como la identidad del responsable del fichero y su dirección. Estas advertencias deben constar en los cuestionarios de recogida de datos, cuando se toman por este medio, salvo que se deduzcan claramente de la naturaleza de los datos que se piden y las circunstancias en que se recaban.

⁵ Davara Rodríguez, M. A., Manual de derecho informático, Aranzadi, Pamplona, 1997.

⁶ Del Peso Navarro, Manual de dictámenes y peritajes informáticos, Díaz de Santos, Madrid, 1995.

b) Relativos al tratamiento de los datos:

- Licitud de los criterios de clasificación: su clasificación sólo puede seguir criterios que no se presten a prácticas ilícitas.
- Principio de exactitud: deber que tiene el responsable del fichero de poner los medios para comprobar la exactitud y puesta al día de los datos, de forma que resulten veraces, es decir, verdaderos sobre la situación real del afectado. Da lugar a los derechos de rectificación y cancelación.
- Principio del consentimiento: en general se requiere el consentimiento para tratar los datos de forma automatizada, salvo que los datos se tomen de fuentes accesibles al público, se recojan para el ejercicio de las funciones propias de las administraciones públicas, se refieran a personas vinculadas por una relación negocial, laboral, administrativa o contractual, y sean necesarios para el normal desenvolvimiento de esas relaciones. Ese consentimiento es revocable cuando exista causa justificada y no se le atribuya efectos retroactivos.
- Principio de seguridad: el responsable del fichero debe adoptar las medidas técnicas y organizativas y de personal que garanticen la no alteración, pérdida y tratamiento o acceso no autorizado.
- Principio del deber de secreto profesional: obliga al responsable del fichero y a quienes intervengan en cualquier fase del tratamiento a guardar secreto profesional sobre los datos del fichero. Los contrario constituye infracción muy grave que lleva aparejada multa de 50 a 100 millones de pesetas si se trata de datos referentes a la religión, ideología, creencias, origen racial, salud o vida sexual; y grave, castigada con multa de 10 a 50 millones de pesetas, si se trata de los demás datos personales.
- Principio de defensa de los datos especialmente protegidos: tienen esta consideración los relativos a: Ideología, religión o creencias, que sólo se pueden recabar con el consentimiento del interesado, al que no se puede obligar en virtud del artículo 16.2 CE, y advirtiéndolo del derecho a no prestar tal consentimiento. Excepto por razones de interés general, previo reconocimiento legal y en los casos que veremos a continuación. Se refuerza ese consentimiento a la hora de su tratamiento automatizado, dado

que tendrá que ser expreso y escrito. Origen racial, salud y vida sexual, que sólo pueden ser recabados, tratados automáticamente y cedidos con el consentimiento del interesado o sin él cuando se fundamente en razones de interés general si así se dispone legalmente. Es el caso del artículo 20.2 y 3 de la LORTAD, que contempla su recogida y tratamiento, sin consentimiento, sólo de los datos necesarios para la prevención de un peligro real para la seguridad pública, la represión de infracciones penales y los fines de una investigación concreta. Datos que serán cancelados cuando ya no sean necesarios para los fines que motivaron su almacenamiento (art. 20.4 LORTAD). Con respecto a los datos relativos a la salud, la propia LORTAD, dispone en su artículo 8 que es posible su tratamiento automatizado de acuerdo con la legislación sanitaria (Ley 14/86 General Sanitaria, Ley 25/90 del medicamento y Ley Orgánica 3/86 de medidas especiales en materia de salud pública) por las instituciones y centros sanitarios, públicos y privados, y por los profesionales correspondientes. En su artículo 11.2 f) establece que cabe la cesión de dichos datos sin previo consentimiento, cuando la misma sea necesaria para atender una urgencia o para realizar los estudios epidemiológicos en los términos del artículo 8 de la LGS 14/86.

c) Relativos a la utilización de los resultados:

- Principio de utilización abusiva: - expresión que utiliza Del Peso - los datos objeto de tratamiento no se pueden usar para fines distintos de aquellos para los que fueron recogidos.
- Principio de publicidad: la LORTAD crea el Registro General de Protección de Datos como órgano integrado en la Agencia de Protección de Datos. En él se inscribirán los ficheros automatizados de las administraciones públicas, los ficheros automatizados de titularidad privada, las autoridades a las que se refiere esta Ley, los códigos tipo (códigos deontológicos en los que los responsables de ficheros privados establecen las condiciones de organización, funcionamiento, obligaciones de los implicados en el uso y tratamiento, etc.) y los datos de los

ficheros necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación.

4.2.3. *Título III.- Derechos de las personas.*

Para hacer efectivo el derecho a la autodeterminación informativa, la LORTAD reconoce los siguientes derechos:

- a) Derecho de información: cualquier persona puede conocer, a través del Registro General de Protección de Datos, la existencia de ficheros automatizados de datos personales, sus finalidades y el responsable del fichero.
- b) Derecho de acceso: el afectado puede solicitar y tener información de sus datos personales incluidos en los ficheros. Información que comprende: los datos de su persona; los datos resultantes de su elaboración automatizada; el origen de los datos; los cesionarios de los mismos; los usos concretos; y las finalidades de su almacenamiento.
- c) Derecho de rectificación y cancelación: cuando el acceso revele que los datos son inexactos, incompletos, inadecuados o excesivos, el afectado puede solicitar su rectificación o cancelación, en su caso. Corresponde al responsable del fichero elegir entre rectificar o cancelar los datos, pero debe hacerlo efectivo en el plazo de los cinco días siguientes a la recepción de la solicitud.
- d) Derecho de impugnación: el afectado puede impugnar los actos administrativos y las decisiones privadas que impliquen una valoración de su comportamiento, cuyo fundamento sea un tratamiento que ofrezca una definición de sus características o personalidad.

En cuanto a las responsabilidades derivadas de la protección de datos personales, la Ley Orgánica 5/92 reguladora del tratamiento automatizado de datos de carácter personal regula imperativamente una realidad social, tipifica una serie de infracciones, adjudica las correspondientes sanciones y estructura un órgano administrativo encargado de velar por su cumplimiento.

El incumplimiento de las normas sobre archivo, tratamiento y uso de los datos personales origina infracciones administrativas clasificadas en leves,

graves y muy graves con la eventual y subsiguiente intervención revisora de los Tribunales Contencioso Administrativos.

Las sanciones correspondientes ascienden a multas de entre 100.000 y 10 millones de pesetas para las infracciones leves; entre 10 y 50 millones de pesetas para las infracciones graves; y entre 50 y 100 millones de pesetas para las infracciones muy graves.

Tales infracciones prescriben al cabo de 1, 2 ó 3 años de que se hubieran cometido, dependiendo de su naturaleza leve, grave o muy grave, respectivamente.

Ello no excluye la posibilidad de responsabilidad penal si la conducta hubiera incurrido en un tipo penal.

Además, si lesionan el derecho al honor o a la intimidad, el infractor incurrirá en responsabilidad civil extracontractual.

En cuanto al órgano administrativo encargado de su cumplimiento, la LORTAD crea la Agencia de Protección de Datos, ente de derecho público con personalidad jurídica propia y plena capacidad, que actúa con plena independencia de las administraciones públicas, en el ejercicio de sus competencias.

Entre sus funciones se cuentan:

- Velar por el cumplimiento de la legalidad introducida por la LORTAD.
- Asegurar el respeto de sus principio inspiradores.
- Informar a las personas sobre los derechos que se les reconocen.
- Atender las reclamaciones de las personas afectadas.
- Sancionar las infracciones.
- Ordenar la cesación del tratamiento y la cancelación de los ficheros cuando no se ajusten a las disposiciones de dicha Ley.
- Dictar instrucciones para adecuar los tratamientos a los principios de la misma. (La última es la Instrucción 1/98, de 19 de enero, sobre ejercicio de los derechos de acceso, rectificación y cancelación).
- Informar, preceptivamente, los proyectos de disposiciones generales que desarrollen dicha Ley.
- Recabar ayuda e información de los responsables de los ficheros.
- Publicar periódicamente una relación de los ficheros automatizados de datos personales.
- Controlar y autorizar los movimientos internacionales de datos.
- Desempeñar las funciones de cooperación internacional.

- Velar por el cumplimiento de la Ley de Función Estadística Pública respecto de la recogida de datos, secreto estadístico y condiciones de seguridad de los ficheros.