Notas acerca del Régimen Jurídico de los Ficheros de Datos Personales de Titularidad Universitaria

GUILLERMO OROZCO PARDO

Profesor Titular del Departamento de Derecho Civil. Universidad de Granada

I.- PLANTEAMIENTO DEL TEMA.

I.1- Introducción y antecedentes:

Estas breves líneas pretenden iniciar al lector en el conocimiento de una temática nueva que ya está generando problemas en la gestión de los diversos órganos universitarios y que, en tiempos venideros, puede generar una diversidad de cuestiones de mayor enjundia. En efecto, el volumen de información que hoy se genera y procesa en los diversos ámbitos del quehacer universitario ha tenido como primera consecuencia la necesidad de aplicar los medios informáticos a la recogida, almacenamiento, proceso y transmisión de información y, dentro de esta, la más importante está referida a los datos personales de diverso orden que las universidades poseen relativos a sus trabajadores, alumnos y terceros que con ellas entran en relación.

Esta dinámica ha ido generando la aparición de ficheros automatizados que sirven para el tratamiento de esos datos personales y que han de estar necesariamente sometidos al régimen jurídico general establecido por el Ordenamiento jurídico para regular tales cuestiones. Dichas normas pretenden, como objetivo básico, asegurar que estos tratamientos y cesiones no vulneren en ningún caso los derechos y libertades de las personas concernidas. Los ficheros universitarios están encuadrados dentro de lo que las leyes denominan "ficheros de titularidad pública" merced a la naturaleza jurídica de sus titulares y los fines a que están afectos.

En consecuencia, como antes dijimos, estos ficheros se encuentran sometidos a un régimen jurídico que, "prima facie", puede parecer dispar pero

que, una vez aclarado, conforma un panorama nítido en su composición, aunque cambiante en un futuro próximo merced a la adaptación de una Directiva comunitaria y a una "previsible" sentencia de nuestro Tribunal Constitucional. Nuestra intención no es "agotar" el tema sino llamar la atención sobre esta temática y tratar de aventurar posibles soluciones a cuestiones ya suscitadas y promover posturas coordinadas en las distintas universidades españolas a la hora de abordar la problemática que, a buen seguro, se nos va a plantear.

I.2- Derecho e Informática:

El tema que abordamos se inserta en un contexto más amplio integrado por la multitud de consecuencias socio-jurídicas que las nuevas tecnologías están planteando al Derecho. La aplicación de los medios automatizados de recogida, tratamiento y transmisión de la información referida a las personas ha supuesto un "salto cualitativo" más importante que los que puedan suponer la imprenta o la televisión. La informática es la técnica de tratamiento y transmisión automatizada de información y supone la base de la llamada "sociedad de la información", y sus implicaciones socioeconómicas son de muy diverso orden: banca, gestión de empresa, correo, policía, seguridad, bolsa, son algunos de los sectores en los que este avance tecnológico se ha vuelto imprescindible. Incluso estamos ya ante la llamada "informática decisional" que muchas veces prepara, condiciona o adopta decisiones que afectan al ciudadano de forma relevante; además la informática sirve para obtener una información nueva, y más sensible, sobre la base de datos precedentes merced a su capacidad de relacionarlos entre sí, tal y como reconoce nuestro Legislador al afirmar que hoy las fronteras del tiempo y el espacio han "caído" por obra de la transmisión automatizada, y casi instantánea, de la información dentro de la "aldea global". A causa de lo anterior la informática permite acceder al conocimiento de una persona, de datos o perfiles concretos, en unos parámetros que ni él mismo puede sospechar, llegándose a un precipitado que podríamos denominar "personalidad informática".

Lógicamente, los medios informáticos se han vuelto hoy unos decisivos instrumentos de poder a los que el Derecho debe imponer unas normas de ética jurídica para impedir abusos: Es por ello que nuestra Constitución de 1978 habla en su artículo 18.4 de que la Ley "... limitará el uso de la informática..." en defensa de los derechos y libertades de los ciudadanos. Con ello pretende evitar que un avance decisivo y positivo pueda convertirse, por mor de un mal uso, en un instrumento de dominación al servicio de intereses antisociales.

I.3- La necesidad de una Ley general a desarrollar:

De todo lo anterior se deduce paladinamente que nuestro Legislador constituyente consideró necesario encauzar la aplicación de esta tecnología a través de unos parámetros de ética jurídica acorde con los principios y valores de un Estado democrático y social de Derecho. Como quiera que el artículo 18.4 CE se encuadra dentro del Capítulo 2º del Título I, relativo a los derechos fundamentales, no cabe la menor duda de la importancia que este precepto, y sus normas derivadas, posee dentro del contexto de nuestro Ordenamiento jurídico. Principios como la seguridad jurídica, la igualdad, el respeto a los derechos y libertades fundamentales, la responsabilidad o la interdicción de la arbitrariedad están consagrados en el artículo 9.3 CE y obligan de manera directa e inmediata a los ciudadanos y a los poderes públicos, dentro de los cuales se integran las Universidades. Todo ello se ha de proyectar en una Universidad que se integra en un marco del Estado, entendido como una "organización democrática de servicios", para proveer uno de los más esenciales: la enseñanza superior.

Por tanto, y como luego veremos, el precepto constitucional que sirve para dotar de una sólida base a todo el conjunto normativo aplicable a la materia es el 18.4 CE, que nos sirve además de criterio interpretativo y de instrumento integrador de las lagunas u obscuridades que pudieran surgir, tal y como ha afirmado nuestro Tribunal Constitucional. Con ello queremos desechar de salida visiones más o menos "administrativizadas" desde la perspectiva del artículo 105-b CE relativo al acceso a los archivos y registros administrativos, pues no hay una "vía paralela" sino que este mismo precepto ya se somete "per se" a los dictados antes citados cuando limita ese acceso mediante garantías en favor de la seguridad, la defensa, la averiguación de los delitos y "... la intimidad de las personas ...".

Por tanto, al margen de textos como el Convenio 108 de Consejo de Europa, el Acuerdo de Schenguen o la Directiva 95/46 cuya transposición obligará modificar la legislación española, podemos afirmar que en esta materia debemos partir de los dictados del artículo 18.4 CE y normas desarrolladoras.

I.4- Cuadro normativo:

Inicialmente, al aprobarse la Constitución de 1978, nuestro país no contaba con una norma legal "ad hoc" que regulara esta materia. Tan solo podíamos partir de los preceptos antes citados:

18.4 CE: "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 ".

105 CE: " La ley regulará:

b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".

El problema básico que es que no existía una norma de rango adecuado que desarrollara el artículo 18.4, verdadera piedra angular del sistema. No obstante, la Ley Orgánica 1/82 de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, establecía en su Disposición Transitoria 1ª que, en tanto no se promulgara la normativa prevista en el artículo 18.4 CE, las intromisiones contra tales derechos, provenientes de la utilización de la informática, se regularía por lo previsto en ella.

Pero esta norma era a todas luces insuficiente para resolver la variada problemática que este tema estaba ya suscitando y ello no escapa a la percepción del legislador. Prueba de ello son las diversas iniciativas parlamentarias que se siguieron desde 1979 hasta 1992, año en que se aprobó una ley específica desarrolladora del precepto constitucional de referencia. Esta laguna de nuestro Ordenamiento fue parcialmente paliada, parece que como imposición para aplicar el Tratado de Schenguen, mediante la firma por España del Convenio 108 del Consejo de Europa, Convenio de Estrasburgo para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, cuyo instrumento de ratificación es de 27 de enero de 1984. (BOE 15/11/85) La aplicación directa, o siquiera como norma interpretativa, suscitó una interesante problemática resuelta por el Tribunal Constitucional en la sentencia del llamado "caso Olaverri" (STC 254/1993) que puso de manifiesto la insuficiencia de los instrumentos legales que había a la sazón en nuestro país para afrontar el problema, si bien sirvió para que nuestro Alto Tribunal sentara doctrina sobre otras cuestiones interesantes a efectos prácticos y científicos.

Partiendo de la base de que para desarrollar un precepto constitucional relativo a derechos fundamentales debe optarse por la vía de la ley Orgánica y que tal norma ha de colocarse en lugar preferente dentro de ese "edifico normativo",

podemos citar como normas específicas para la regulación de la materia, en lo que a nuestro propósito interesa:

- El Convenio 108 del Consejo de Europa, de 28 de enero de 1981.

- La Directiva 95/46 del Parlamento Europeo, de 24 de octubre de 1995, cuyo plazo para ser adaptada termina en 1998.

- El artículo 18.4 CE.

- La Ley Orgánica 5/92 de 29 de octubre de Regulación del Tratamiento Automatizado de los Datos de carácter personal.(v. gr. LORTAD)

- R.D. 1332/1994 de 20 de Junio, que desarrolla determinados preceptos de la anterior.

- L.O. 10/1995, de 23 de noviembre, del Código Penal.

- En desarrollo del artículo 105.b CE cabe destacar la Ley 30/92 de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común.

Obviamente existen otras normas complementarias pero a los efectos del presente estudio no poseen relevancia como para integrarlas en este cuadro.

Al margen de otras consideraciones relativas a las norma procedentes de Organismos supranacionales, debemos tener muy presente que las leyes se relacionan entre sí por los principios de jerarquía normativa y especialidad de materia. Es por ello que no cabe la menor duda de que la LORTAD se convierte en la pieza clave de este sistema y es a partir de ella como debemos aplicar el resto de los preceptos citados.

II.- CUESTIONES GENERALES.

II.1- Conceptos previos:

Vamos a recoger aquí aquellas definiciones legales referidas a los conceptos más esenciales que se manejan en esta temática, utilizando preferentemente los recogidos en el artículo 3 de la LORTAD y normas de desarrollo:

- Fichero automatizado: todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización o acceso.

- Tratamiento de datos: operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

- Cesión de datos: toda obtención de datos resultante de la consulta de un fichero, la publicación de los datos contenidos en el fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada.

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

- Transferencia de datos: el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

- Bloqueo de datos: la identificación y reserva de datos con el fin de impedir su tratamiento.

- Responsable del fichero: persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.

- Encargado del tratamiento: introducido por la Directiva es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Como puede observarse, la Ley no incluye entre sus definiciones al "Titular del fichero", y ello porque opta por hacer hincapié en la responsabilidad por la gestión del mismo, antes que por la relación de pertenencia o titularidad. Ello ha provocado cierta polémica doctrinal en cuanto vincula directamente al titular/responsable del fichero con las consecuencias que de un incumplimiento de las normas se pudieran deducir.[110] Para resolver la cuestión la Directiva incorpora al "Encargado de tratamiento" como figura intermedia e instrumental que realiza el tratamiento, por cuenta del anterior, y de cuya actuación responde el titular del fichero, según las normas comunes de responsabilidad civil.

II.2- Especial referencia a los datos personales:

Digamos de salida que la Ley no ampara a las personas jurídicas, aunque al Proyecto si se les aplicaban los beneficios de la misma, pues se circunscribe a las personas físicas. En consecuencia, todas la definiciones que se refieren a la persona concernida titular de los datos objeto de tratamiento se refieren a ámbitos de la vida de tales sujetos.

- Afectado: persona física titular de los datos que sean objeto del tratamiento.

- Consentimiento del interesado: toda manifestación de voluntad libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos que le conciernen.

- Identificación del afectado: cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada.

- Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

■ 110 No obstante la propia Ley habla de ficheros de titularidad pública o privada, con lo cual da a entender que acepta la distinción entre la persona, organismo o autoridad pública a cuyo nombre ha de figurar el fichero en el Registro y el responsable.

Esta información puede estar referida a las más diversas esferas de la vida de las personas físicas, razón por la cual la propia Ley considera que el concepto de intimidad no es suficiente para dotar de contenido a tan amplia definición, razón por la cual opta por más amplio de privacidad. Tal y como lo recoge el RD 1332/94 puede ser toda información "numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable".

La Directiva alude al interesado como titular de esos datos personales que permiten su identificación: números de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Por tanto, los más diversos ámbitos de la vida de las personas pueden ser objeto de protección de esta Ley en la medida en que no se circunscribe a ese "núcleo central" de su actividad personal que él mismo trata de preservar del conocimiento de los demás ("intimidad"), sino que se construye sobre el concepto de privacidad a la que la propia LORTAD entiende como "... un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado".

Cobra especial relevancia el hecho de que los datos puedan servir para identificar cualquiera de las facetas de personalidad del afectado, por lo que aquellos datos disociados que no pueden ponerse en conexión con los sujetos quedan fuera del ámbito de la Ley: por ejemplo datos estadísticos o de investigación. Ahora bien, tales elementos característicos de la personalidad del sujeto pueden ser más o menos "sensibles" según la esfera o faceta a que estén referidos. Es por lo que se establece un régimen legal más o menos estricto a la hora de autorizar el tratamiento de los datos según su naturaleza. Existen unos "datos especialmente protegidos" o "datos sensibles" sobre los que pesa una prohibición de tratamiento, salvo autorización legal o consentimiento del afectado: datos relativos a ideología, religión o creencias, vida sexual, origen racial o salud.

El régimen jurídico de tales datos especialmente protegidos se establece en el artículo 7 de la Ley a cuyo tenor podemos distinguir:

A - Datos sobre ideología, religión o creencias. Están tutelados por el artículo 16 CE y no se puede obligar a declarar sobre ello a ninguna persona y, por lo tanto, no cabe almacenarlos salvo que el afectado consienta expresamente por escrito, siendo revocable este consentimiento.

B - Datos sobre origen racial, salud o vida sexual. Sólo pueden recogerse cuando así lo dispone una ley, por razones de interés general, o lo consienta el afectado expresamente por escrito u otra forma susceptible de prueba.

Sólo se admiten la excepciones al consentimiento previstas para las Fuerzas de Seguridad. No se admiten ficheros cuya única finalidad sea almacenar datos especialmente protegidos.

Incluso se habla de datos "supersensibles" que son aquellos obtenidos de un tratamiento sobre datos previos de los que puede ser ignorante el propio afectado: resultado de un test, etc... No obstante, no debemos "obsesionarnos" con la sensibilidad del dato pues, como dice la teoría del "mosaico", un dato aparentemente irrelevante "ab initio" puede volverse enormemente significativo y revelador una vez puesto en relación con su contexto, al igual que la tesela que completa el mosaico o la pieza que completa u orienta al autor de un "puzzle".

De otro lado, existen otros datos que por su propia naturaleza o por la actuación del sujeto afectado, están a disposición del conocimiento de los demás son los llamados Datos accesibles al público definidos como "los que se encuentran a disposición del público en general, no impedida por cualquier norma imitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo" (Cfr. RD 1332/94 art. 1.3) Por tanto, son datos de esta naturaleza los repertorios telefónicos o las relaciones de cargos y unidades que las universidades publican; no lo son, sin embargo, las listas de calificaciones académicas del alumnado, toda vez que su publicación sustituye a la "papeleta" o carta de calificación de la nota, pero no es un instrumento de publicidad para terceros que les permita recoger y tratar esas calificaciones, que son datos personales protegidos por la Ley.

Teniendo presente el amplio y global concepto que la Ley contiene de lo que es un "dato personal" es ya indudable que nuestros ficheros universitarios están plagados de ellos y que estos afectan incluso a terceros como padres, cónyuges, hijos y demás personas relacionadas con los trabajadores, el alumnado y los servicios prestados por o a la Universidad.

III.- ANALISIS DE LA LORTAD.

III. 1- El régimen establecido por la LORTAD:

La LORTAD contiene unas disposiciones generales que se aplican a todo tipo de ficheros y luego unos preceptos específicos para los ficheros públicos y los privados. La estructura podría sintetizarse de la siguiente manera:

- Título 1º: Disposiciones generales, arts. 1 a 3.

- Título 2º: Principios de protección de datos, arts. 4 a 11

- Título 3º: Derechos de las personas, arts. 12 a 17.

- Título 4º: Disposiciones sectoriales, este título recoge preceptos específicos para los ficheros de titularidad pública o privada, si bien la Directiva parece imponer la necesidad de regularlos de forma unitaria. Se subdivide en:

  - Capítulo 1º: Ficheros de titularidad pública, arts 18 a 22, donde se contienen una serie de excepciones a los principios y derechos de la parte general que han sido muy criticadas e incluso fueron objeto de recurso de inconstitucionalidad.

  - Capítulo 2º: Ficheros de titularidad privada, arts 23 a 31, que regulan materias específicas de ficheros de personas, empresas o entidades privadas, pero que no se benefician de las excepciones antes comentadas.

  Lógicamente, los ficheros de los que son titulares las Universidades están regulados en el capítulo primero ántes comentado, aunque las excepciones más polémicas no se les aplican en ningún caso.

- Título 5º: Movimiento internacional de datos, arts. 32 y 33.

- Título 6º: Agencia de Protección de Datos: arts 34 a 41, donde se regula la estructura esencial de la llamada "Autoridad de control", y otras cuestiones como la competencia de las Comunidades Autónomas en esta materia. El Estatuto de la Agencia de Protección de Datos fue desarrollado por el RD 428/93 de 26 de Marzo. Este es el órgano que vela por el cumplimiento de la Ley, emite las autorizaciones precisas, dicta las instrucciones adecuadas, atiende las peticiones y reclamaciones, proporciona información sobre la materia, ordena el cese de los tratamientos y ejerce la potestad sancionadora prevista en la Ley.

- Título 7º: Infracciones y sanciones, arts 42 a 48, en ellos la Ley establece un catálogo de infracciones leves, graves o muy graves y las sanciones correspondientes. Este título debe se puesto en conexión con otros textos legales como el Código Penal y las normas que regulan el régimen disciplinario de las Administraciones Públicas y su responsabilidad.

En definitiva, la LORTAD se presenta como la "piedra angular" del sistema merced a su carácter de norma especial sobre la materia y su jerarquía orgánica, si bien debe ser puesta en conexión con otras normas del Ordenamiento que regulan cuestiones conectadas con sus preceptos. Así mismo, la Ley no entra a regular materias que son objeto de otras leyes especiales: régimen electoral, materias clasificadas, Registro civil, Registro de penados y rebeldes, personal militar o función estadística pública.

III.2- Excepciones a la aplicación de la LORTAD:

Esta norma pretende regular sólo aquellos ficheros que no están recogidos en otras leyes especiales en razón de su materia o dependencia orgánica. Se excluyen de la misma:

- Ficheros públicos cuyo objeto establecido por ley es almacenar datos para publicidad con carácter general: Registro Civil, Mercantil o de la Propiedad.

- Ficheros cuyo titular es persona física y tienen una finalidad exclusivamente personal.

- Ficheros de información técnica o comercial que reproducen datos accesibles al público aparecidos en boletines, repertorios, etc...

- Ficheros integrados por bases de datos de resoluciones jurídicas de carácter legal o jurisprudencial.

- Ficheros de datos de miembros, ex miembros de partidos, sindicatos, confesiones, iglesias, etc... No obstante, en estos ficheros se exige el consentimiento del afectado para la cesión de datos y se aplica la Ley a los datos especialmente protegidos.

III.3- Principios/deberes relativos a los datos:

Están referidos a los datos y los tratamientos de los que pueden ser objeto, funcionan como "condiciones para la licitud del tratamiento" al decir de la Directiva. Como tales principios constituyen mandatos que imponen deberes de conducta para los titulares y responsables de los ficheros y el tratamiento, quienes tienen que garantizar el cumplimiento de los mismos por todo el personal.

Podríamos sintetizarlos de la siguiente manera:

1- Se prohibe su recogida por medios fraudulentos, desleales o ilícitos. Por tanto, se han de recoger con fines determinados, explícitos y legítimos por lo que no se les puede tratar después de manera incompatible con aquellos fines, salvo que sean razones históricas, estadísticas o científicas.

2- Deben ser exactos y actualizados, de lo contrario han de cancelarse o rectificarse de oficio o a petición del interesado.

3- No pueden usarse para finalidades distintas a aquellas para las que se recogieron, con las precisiones antes comentadas.

4- Serán cancelados cuando dejen de ser necesarios, por lo que no deben ser conservados una vez que han dejado de ser útiles para la función prevista. De ello se exceptúa su mantenimiento por razones históricas, estadísticas o científicas o cuando existen normas legales que prevean otra cosa: fiscales, seguros, etc... En estos casos deben someterse al proceso de disociación cuando ello sea oportuno.

5- Se han de almacenar de forma que permitan el ejercicio del derecho de acceso a los afectados.

6- Han de ser adecuados, pertinentes y no excesivos en relación con los fines para los que se han recabado.

Otros deberes que han de observar los responsables de los ficheros son:

1- Inscribir debidamente los ficheros en el Registro a través de la Resolución correspondiente.

2- Adoptar las medidas necesarias para garantizar la seguridad de los datos evitando su alteración, pérdida o el acceso no autorizado. A tal efecto, el Mº de Justicia debe elaborar un reglamento que establezca las condiciones técnicas de seguridad en relación con los centros de tratamiento, locales, equipos, sistemas y programas. No obstante, la ausencia de esta norma no empece que los responsables de los ficheros adopten las medidas necesarias para asegurar el cumplimiento de estos deberes, pues esta laguna legal no les exime de responsabilidad. A título indicativo el artículo 9 de la LORTAD le impone el deber de adoptar las medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos y eviten los perjuicios antes previstos, para lo cual han de tenerse en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

3- El deber de secreto que afecta a todas las personas relacionadas con el tratamiento y los ficheros, incluso con posterioridad a que concluya su relación con el titular o responsable del fichero.

Queda patente el elevado nivel de responsabilidad que se impone a los titulares y responsables de los ficheros que, en muchas ocasiones, no se corresponde con los medios técnicos de control de los que disponen para verificar el cumplimiento de lo establecido en la Ley. Es por ello muy necesario que las Secretarías Generales, que suelen figurar como responsables en la resoluciones del Rector, establezcan con toda claridad un esquema de competencias y responsabilidades que "impliquen" a los distintos sujetos que se encargan de los tratamientos y al personal que dirige los servicios a los que está adscrito el fichero en cuestión. Así mismo, es importante promover una Comisión técnica que se encargue de establecer esas medidas de seguridad que garantizan el cumplimiento de los deberes arriba reseñados.

III.4- <u>El consentimiento del afectado</u>:

Es el eje sobre el que gira todo el sistema, dado que esta materia parte de un nuevo derecho fundamental consagrado en el artículo 18.4 CE y reconocido por nuestro Tribunal Constitucional: el derecho a la llamada "autodeterminación informativa" frente a la informática o "libertad informática", que asegura a la persona un poder de decisión y control sobre el tratamiento de datos personales que le afectan.

Como principio general hemos de decir que todo tratamiento (que incluye la recogida de datos y su cesión) requiere el consentimiento del afectado. Dicho consentimiento ha de ser libre, informado y se puede prestar por cualquiera de las formas establecidas en Derecho, sea expreso, tácito o presunto, según proceda (debemos recordar los datos especialmente protegidos). Se exceptúan los casos en que una Ley permite un tratamiento sin consentimiento del afectado. Este consentimiento es revocable por causa justificada, pero sin que se le atribuyan efectos retroactivos.

A la hora de la recogida de los datos, el afectado debe ser informado de los siguientes extremos:

1- La existencia del fichero, de la identidad y dirección del responsable del fichero, su finalidad y los destinatarios de la información.

2- El carácter obligatorio o facultativo de las respuestas.

3- De las consecuencias de la obtención de los datos y de la negativa a suministrarlos.

4- De la posibilidad de ejercitar sus derechos legales: acceso, rectificación, cancelación, oposición y bloqueo.

Todos estos extremos deben figurar en los cuestionarios y demás documentos que se utilizan para la recogida de los datos: v.gr. impresos de matricula.

En cuanto a la cesión exige un consentimiento previo sobre la base de un cesionario determinado o determinable y que conste la finalidad de la cesión, pues de lo contrario el consentimiento es nulo. Ello implica que no se admiten previsiones de futuras cesiones al libre arbitrio del cedente de suerte que el

afectado no pueda determinar quienes serán esos futuros cesionarios: bastaría con prever, por ejemplo, otras universidades u organismos públicos dedicados a la educación superior.

No obstante, se establecen unas excepciones al consentimiento, algunas muy criticadas, de las que a nosotros interesan:

A-Que una "ley" disponga otra cosa.

- Que se recojan para el ejercicio de las funciones propias de las Administraciones Públicas.

B- Que se refieran a personas vinculadas por una relación negocial, laboral, administrativa o un contrato y sean necesarias para el mantenimiento de las relaciones o el cumplimiento del contrato.

C- Que la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces y Tribunales, en el ejercicio de sus funciones.

D- Los casos previstos en el artículo 19 de la LORTAD:

1º- Los datos recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones sólo se pueden ceder a otras Administraciones Públicas para el ejercicio de competencias diferentes o competencias que versen sobre materias distintas, cuando la cesión hubiera sido prevista en las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso.

2º- Pueden cederse en todo caso los datos que una Administración Pública elabore para otra.

Veda también la Ley la cesión de los datos de los ficheros públicos a ficheros privados (academias, etc...) salvo cuando sean datos recogidos de fuentes accesibles al público y lo consienta el interesado o una ley prevea otra cosa.[111]

E- Cuando sean datos relativos a la salud y la cesión sea precisa para solucionar una urgencia o para realizar los estudios epidemiológicos.(Cfr. art.8 de la Ley 14/1988 General de Sanidad)

Por supuesto, el cesionario se obliga igualmente a cumplir todas las disposiciones legales. Igualmente se puede proceder a la cesión cuando los datos han sido sometidos a un proceso de disociación.

IV- LOS DERECHOS DE LAS PERSONAS.

IV.1- Un nuevo derecho fundamental:

Ya hemos puesto de relieve anteriormente la dimensión constitucional de esta materia y la sede en que nuestra Carta Magna consagra las garantías que pretende instituir en favor de los ciudadanos: Título I, Capítulo 2º: de los derechos y libertades fundamentales. Ello ha llevado al Legislador, así como a la Doctrina más autorizada y a nuestro Tribunal Constitucional, a afirmar con rotundidad que el artículo 18.4 CE no sólo pretende promover una acción legislativa y funcional de los poderes públicos para limitar el uso de la informática (aspecto pasivo) sino que quiere garantizar al ciudadano una esfera de poder autónomo que le permita decidir acerca del tratamiento automatizado de los datos que le conciernen, no solo del nivel de conocimiento de su vida privada, sino el control de la información que le concierne y los usos que de ella se puedan realizar.

Como afirma el Ministerio Fiscal en el caso "Olaverri" la ya citada STC de 20 de julio de 1993) el Constitución consagra "una libertad positiva para ejercer un derecho de control sobre los datos referidos a la propia persona, que han salido ya de la esfera de la intimidad, para convertirse en elementos de un

■[111] Recordemos aquí que las calificaciones académicas no son datos accesibles al público, y las direcciones, cargos y demás datos de guías, agendas y repertorios sí lo son, pero están sometidos a las excepciones que la LORTAD establece.

archivo electrónico". No se trata por tanto de un derecho "semi-gaseoso", sino de un pleno derecho fundamental a una libertad positiva de control democrático que garantiza al ciudadano el libre ejercicio de sus derechos y libertades fundamentales y un digno desarrollo de su personalidad frente a los posibles abusos del uso de la información personal tratada en los ficheros públicos y privados.

Este derecho tiene sus propios instrumentos de tutela y puesta en práctica: el llamado "hábeas data" y los derechos instrumentales o garantías jurídicas subjetivas. Todo ello lo pone de manifiesto el Legislador en la Exposición de Motivos de la LORTAD y lo ha consagrado el Tribunal Constitucional.

En definitiva, se trata de un derecho implícitamente formulado en la Constitución que otorga el poder de conocer y decidir qué datos son recogidos y para qué finalidad. Parafraseando al Tribunal Constitucional podemos definirlo como "el derecho fundamental de la persona al libre control de las informaciones referidas a su privacidad, frente a las posibles agresiones a su dignidad y libertad producidas por un uso ilegítimo del tratamiento automatizado por medios informáticos de datos personales que le conciernen".

Este es un derecho que corresponde a toda persona física, con independencia de su estado civil o nacionalidad, que sea titular de los datos objeto del tratamiento y se puede ejercitar frente a todos aquellos que realicen tratamientos automatizados que le afecten: titulares, responsables de ficheros, encargados del tratamiento y personas vinculadas a ellos.[112]

Este derecho tiene un contenido positivo integrado por la facultad de control sobre los datos, básicamente el consentimiento, y los derechos instrumentales o garantías jurídicas subjetivas. De otro lado, tiene un contenido negativo integrado por los deberes que se imponen a los terceros: respeto a los principios de calidad de los datos, etc... Conlleva también unas cargas que obligan

■ 112 Menores, incapacitados y personas fallecidas están tuteladas por la Ley, si bien los mecanismos para ejercer este derecho son los establecidos para el caso: representes legales y legitimados "mortis causa".

al titular del derecho: facilitar los datos en ciertos casos, aceptar las excepciones legalmente previstas, aportar datos veraces, etc..

IV.2- LOS DERECHOS INSTRUMENTALES:

Son los "elementos nutrientes" del derecho fundamental antes citado, responden a las diversas facetas de su contenido positivo y sirven para su puesta en práctica y refuerzan su aplicación, razón por la cual se les denomina "garantías jurídicas subjetivas". Así mismo, son derechos personalísimos por lo que la Ley exige que sean ejercitados por el propio titular o su representante legal.

1°- Derecho de Impugnación:

Este derecho permite oponerse a los llamados "juicios informáticos" es decir, con su ejercicio el afectado impugna los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad. A tal efecto, se elevó una consulta a la A.P.D. acerca de la validez de las pruebas o exámenes realizados por computadora, y la Agencia se pronunció en favor de su validez, toda vez que no suponen una decisión basada en datos personales.(art. 12 LORTAD).

2°- Derecho de Información:

Este derecho implica que al momento de la recogida de datos debe ponerse en conocimiento del sujeto los siguientes extremos:

- De la existencia del fichero automatizado.

- De su finalidad.

- De los destinatarios de la información.

- Del carácter obligatorio o voluntario de la respuesta a las cuestiones planteadas.

- De las consecuencias de la obtención de los datos y de la negativa a suministrarlos.

- De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.

- De la identidad y dirección del responsable del fichero.

Esta información no es necesaria si su contenido se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Todo ello se debe reflejar en los cuestionarios de recogida de datos, así mismo se refleja en la Resolución que se publica en el B.O.E. y consta en el Registro General de Protección de Datos en la A.P.D., en el que se han de inscribir los ficheros, y que es de consulta pública y gratuita. De ello se deduce la importancia de cumplir con el deber de dictar la Resolución donde se recogen los ficheros y su estructura, así como cualquier modificación, supresión o creación de un nuevo fichero. (arts 5 y 13 LORTAD)

3°- El derecho de Acceso:

En virtud del mismo el afectado puede acceder al fichero para recabar información acerca de sus datos personales que son objeto de tratamiento en un fichero automatizado. Sus condiciones de ejercicio, criticables en algunos aspectos, están recogidas en la Ley y en el RD 1332/94 ya citado. Debe ejercitarse en intervalos no inferiores a 12 meses, salvo que se acredite un interés legítimo.

El afectado debe plantear su solicitud ante el responsable del fichero formulada por cualquier medio que garantice la identificación del afectado y en la que conste el fichero(s) a consultar. Para la consulta, el solicitante puede optar por uno o varios de los distintos sistemas que la Ley establece, siempre que la configuración e implantación del fichero:

- Visualización en pantalla.

- Escrito, copia o fotocopia remitida por correo.

- Telecopia.

- Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

Es importante adoptar un modelo de solicitud que se ponga a disposición de los afectados en el que consten todos los extremos exigidos por la Ley. Así mismo, cabe plantearse el sistema de consulta que se está poniendo a disposición de muchos alumnos para acceder a su expediente académico, mediante claves de seguridad e identificación y "tarjetas inteligentes", que no permiten modificarlos pero sí que facilitan el acceso. Hemos de recordar asimismo, que son derechos personalísimos que sólo puede ejercitar el afectado o su representante legal.

Sea cual sea el soporte elegido, la información ha de facilitarse en forma legible e inteligible y comprenderá los datos de base del interesado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

El responsable del fichero debe resolver la petición en el plazo máximo de 1 mes a contar desde la recepción de la solicitud. Si no se contesta en este período, se entiende denegada. La negativa al acceso, en el caso de los ficheros que nos ocupan, sólo puede basarse en las siguientes circunstancias:

- Razones de interés general.

- Intereses de terceros más dignos de protección.[113]

En tales casos, dado lo ambiguo de la causa, deberá necesariamente dictarse resolución motivada por parte del responsable del fichero. Ante esta decisión, el afectado puede acudir al Director de la Agencia de Protección de Datos, quien dará traslado de la reclamación al responsable del fichero para que formule las alegaciones pertinentes en el plazo de 15 días. Pasado este plazo, la Agencia, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia al afectado y al responsable del fichero, resolverá sobre la reclamación, dando traslado a los interesados. Contra esta resolución cabe interponer recurso contencioso-administrativo, aspecto este criticado por cuanto "desvía" a esa "vía lenta" una cuestión relativa a derechos fundamentales.

■[113] Obviamos aquí la cuestión de los ficheros de los Cuerpos Seguridad y Hacienda, que se "benefician" de unas excepciones criticables en algunos casos.

Es en este punto donde debemos hacer de nuevo referencia a la vía abierta por el artículo 105.b CE sobre el acceso a los archivos de las Administraciones Públicas. Como puede deducirse paladinamente, este es un supuesto que por la ubicación de dicha norma en la Carta Magna no debe interpretarse en ningún caso como de aplicación preferente, siquiera paralela, con lo establecido en el 18.4 CE referido a derechos fundamentales, pues esta es la norma a partir de la cual debe interpretarse lo dispuesto en dicho artículo 105.b CE, tal y como expresamente establece el artículo 35.h) de la Ley 30/92 de Régimen Jurídico y Procedimiento Administrativo Común, que reconoce el derecho de los ciudadanos "al acceso a los registros y archivos de las Administraciones Públicas en los términos previstos en la Constitución y en esta u otras Leyes ".

Así lo ha entendido el propio Legislador al desarrollarla en el Título IV, Capítulo primero de la citada Ley 30/92, pues consagra en su artículo 35 los "derechos de los ciudadanos" y regula en el artículo 37 el derecho de acceso a los Archivos y Registros. A tenor del párrafo 1° mismo los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud.

Esta norma general viene limitada por los párrafos 2° y 3° que salvaguardan la protección de los datos personales de terceras personas incluidas en tales documentos:

2."El acceso a los documentos que contengan datos referentes a la intimidad de las personas estará reservado a éstas, que, en el supuesto de observar que tales datos figuran incompletos o inexactos, podrán exigir que sean rectificados o completados, salvo que figuren en expedientes caducados por el transcurso del tiempo, conforme a los plazos máximos que determinen los diferentes procedimientos, de los que no pueda derivarse efecto sustantivo alguno".

Como puede apreciarse esta norma veda el acceso de terceros a los datos personales de otros sujetos, a tal efecto el concepto de intimidad debe interpretarse como referido a la privacidad, en el sentido establecido por la Exposición de Motivos de la LORTAD que hace referencia al mismo en los siguientes términos:

"El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquella es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo- la privacidad constituye un conjunto más amplio, más global de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que lo desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo".

Por tanto, la legislación especial aquí aplicable está integrada, básicamente, por la LORTAD como norma específica para ficheros automatizados y, por extensión, a los mecanizados.

El artículo 37.3 L.P.A. permite el acceso de los terceros que acredite un interés legítimo y directo, pero sólo en determinadas circunstancias:

"El acceso a los documentos de carácter nominativo que sin incluir otros datos pertenecientes a la intimidad de las personas, figuren en los procedimientos de aplicación del derecho, salvo los de carácter sancionador o disciplinario, y que, en consideración a su contenido, puedan hacerse valer para el ejercicio de los derechos de los ciudadanos, podrá ser ejercido, además de por sus titulares, por terceros que acrediten un interés legítimo y directo".

Por tanto, el margen de actuación del tercero en el acceso a los datos personales ajenos es muy estrecho y, en todo caso debemos tener muy presente lo establecido en el artículo 11 del RD 1332/94 que desarrolla una materia relativa a garantías subjetivas integradas en un derecho fundamental, tal y como hemos afirmado. A su tenor:

"Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el

afectado frente al responsable del fichero, sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el presente Real Decreto.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos". A tal efecto, en los ficheros de titularidad privada, la única razón para denegar el acceso es que la solicitud sea formulada por persona distinta del afectado, según el artículo 14.2 del Real Decreto citado.[114]

Por tanto, el acceso a los datos de los trabajadores y del alumnado de la Universidad obrantes en sus ficheros sólo se puede permitir al propio afectado o a su representante legal. No obstante, pueden ser objeto de cesión siempre que se cumpla el principio general del artículo 11 de la LORTAD, o se acojan a una de las excepciones legalmente previstas. Como norma general, los datos sólo pueden ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

No obstante, caben algunas excepciones al consentimiento, entre las cuales destacamos:

A)- Cuando una Ley prevea otra cosa.

Esta excepción ha sido muy criticada porque no concreta cuál ha de ser el rango de esa "Ley" por lo que puede permitir que un Reglamento o Resolución limite un derecho fundamental.

B)- Cuando se trate de datos recogidos de fuentes accesibles al público. En este punto conviene recordar que el artículo 19.3 no permite ceder datos de esta

■[114] El artículo 32 L.P.A. regula la representación de los interesados admitiendo éste cuando ambos, representante y representado, posean plena capacidad de obrar y siempre que se haga constar de forma fidedigna por un medio válido en Derecho, salvo para los actos "de mero trámite" en los que se presume la representación. No obstante, tan "generoso" criterio no puede aplicarse al ejercicio de estos derechos, pues el RD 1332/94 lo veda expresamente al circunscribirse a la representación legal de menores e incapacitados.

naturaleza recogidos en ficheros de titularidad pública a los ficheros privados, sino con el consentimiento del afectado o cuando una Ley prevea otra cosa.

C)- Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.

Esta es una de las excepciones que más juego pueden dar en los ficheros universitarios toda vez que la actividad de las universidades cada vez provoca una mayor necesidad de interconexión.

D)- Cuando la cesión es a órganos tales como el Defensor del Pueblo, Ministerio Fiscal, Jueces y Tribunales en el ejercicio de sus funciones.

E)- Cuando se produzca entre Administraciones Públicas en los supuestos del artículo 19 LORTAD, ya comentado.

Debemos recordar en este punto las cautelas antes reseñadas al hablar del consentimiento del afectado en la cesión de datos y la conveniencia de preverlo en los formularios de recogida de datos.[115]

4°- <u>Los derechos de Rectificación y Cancelación</u>:

Son consecuencia del anterior y permiten al afectado instar al responsable del fichero para que, en cumplimiento de sus deberes deducidos de los principios

■[115] Reiteramos la necesidad de que el cesionario sea determinado o determinable y que el consentimiento es revocable. Es por ello importante que las Universidades prevean un sistema coordinado de cesiones entre ellas bajo el amparo de las excepciones previstas en la Ley y, cuando sea preciso, un consentimiento previo recabado al afectado. Así mismo, la acción social desempeñada por muchas Universidades les ha llevado a tratar datos "sensibles" que afectan al sujeto que facilita el dato y a terceros, cónyuge, hijos, padres, convivientes, etc... que pueden ser relativos a la salud, rendimientos económicos, sanciones y demás cuyo tratamiento está muy restringido por el artículo 7 y 8, por lo que no deben ser objeto de cesión y en esos ficheros deben extremarse las medidas de seguridad previstas en el artículo 9 y 10, cuya supervisión corresponde, en última instancia, al responsable del fichero.

de calidad y licitud de los tratamientos, mantenga la exactitud, veracidad y oportunidad de los datos obrantes en el fichero rectificando o cancelando los datos incompletos, inexactos, inadecuados, excesivos o no pertinentes. No obstante, los datos que reflejan hechos constados en un procedimiento administrativo se considerarán exactos si coinciden unos y otros.

La solicitud debe dirigirse al responsable del fichero, con las precisiones de identidad antes enunciadas, y haciendo constar los datos que se han de rectificar o cancelar y el fichero(s) en que se encuentran.

El responsable del fichero debe hacer efectiva la rectificación o cancelación procedente en el plazo de 5 días siguientes a la recepción de la solicitud. Si los datos rectificados o cancelados hubiesen sido cedidos previamente, el responsable del fichero debe comunicarlo al cesionario dentro del mismo plazo.

La petición puede ser desestimada de dos maneras:

A - Por transcurso del plazo de 5 días sin contestación expresa.

B - Por resolución motivada en la que se comunica la decisión de acceder a la solicitud. Las razones en que ello puede fundarse son:

- Que la legislación aplicable al caso imponga un plazo determinado de conservación de los datos en cuestión.

- Cuando su cancelación pueda causar un perjuicio al propio afectado o a un tercero.

- Cuando concurran razones de interés general.

- Cuando concurran intereses de terceros más dignos de protección.

Ante la denegación el afectado puede iniciar el procedimiento de tutela de sus derechos ante la Agencia de Protección de Datos, descrito anteriormente y que se regula en los artículos 17.1 LORTAD y 17 del RD 1332/94

5°- Otros derechos instrumentales:

Nos referimos en concreto a dos facultades que se encuentran implícitas en el contenido del derecho a libre autodeterminación informativa. El primero de ellos el derecho de bloqueo, recogido en el artículo 16 del RD 1332/94 y que permite exigir que, cuando sea procedente la cancelación de datos personales y no sea posible su extinción física, tanto por razones técnicas, como por causa del procedimiento o soporte utilizado, el responsable del fichero proceda al bloqueo de los datos con la finalidad de impedir su ulterior proceso o utilización. Tal extremo habrá de ser comunicado igualmente a los posibles cesionarios de los datos objeto de bloqueo.

No obstante, cuando tales datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos y ello se demuestre, la cancelación de los mismos comporta siempre la destrucción del soporte en que figuren.

Como quiera que el bloqueo supone una decisión del responsable que podemos considerar subsidiaria de la cancelación, el afectado puede recurrirla ante la Agencia de Protección de Datos.

El llamado derecho de Oposición esta formulado en el artículo 14 de la Directiva 95/46 y está conectado con las excepciones al consentimiento en la recogida y tratamiento de datos. Como se ha dicho, el tratamiento o cesión de datos personales en los ficheros de titularidad pública puede llevarse a cabo sin consentimiento del afectado cuando sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o al cesionario. Igualmente, se admite esta excepción cuando sea necesario para la satisfacción de un interés legítimo perseguido por el responsable del tratamiento o por el cesionario, siempre que frente a ello no deban prevalecer el interés o los derechos y libertades fundamentales del interesado que deban ser protegidos.

En tales casos, el afectado puede oponerse, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos sean objeto de tratamiento, salvo que la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse a esos datos.

Este derecho es también ejercitable, previa petición y sin gastos, al tratamiento de los datos personales respecto de los cuales el responsable prevea un tratamiento destinado a la prospección. Debe ser informado previamente en caso de cesión para el mismo destino, a la cual podrá oponerse, sin que ello le ocasione gasto alguno.

V.- TUTELA DE LOS DERECHOS

Los mecanismos de tutela de estos derechos poseen varias vías de aplicación. Además de la autotutela del interesado que diligentemente debe ejercitar sus derechos en tiempo y forma, podemos citar tres posibles actuaciones.

V.1- La reclamación administrativa:

Los actos que supongan infracción de los deberes establecidos en la Ley o la lesión de un derecho del afectado pueden ser objeto de reclamación ante la Agencia de Protección de Datos. Para ello se arbitran dos procedimientos:

A)- Reclamación ante la Agencia de Protección de Datos:

Los artículos 17 de la LORTAD y del RD 1332/94 establecen y regulan un procedimiento que se aplica frente a la negativa por parte del responsable del fichero al ejercicio de los derechos de acceso, rectificación y cancelación. Para ello el afectado debe comunicar a la Agencia los hechos alegados y los preceptos legales que se entienden infringidos. De la reclamación se da traslado al responsable del fichero para que, en el plazo de 15 días, formule las alegaciones oportunas. Transcurrido este plazo, la Agencia resolverá la cuestión planteada, previos los informes, pruebas y otros actos que considere oportunas, incluida la audiencia a las partes. Debemos entender que este mismo procedimiento debe aplicarse en el caso de que el responsable opte por el bloqueo de los datos.

B)- Recurso ante los Tribunales:

Contra esta decisión de la Agencia cabe plantear recurso contencioso administrativo, cuestión que como se ha dicho ha sido criticada por un sector doctrinal, que hubiera preferido un procedimiento judicial más rápido y menos costoso.

C)- El procedimiento sancionador:

Viene recogido en el artículo 47 de la LORTAD y se regula en los artículos 18 y 19 del RD 1332/94. A tal efecto la Ley hace una precisión muy importante en su artículo 42: los responsables de los ficheros están sujetos al régimen sancionador establecido en la misma. Incluso el artículo 45.2 establece para los ficheros de las Administraciones Públicas la posibilidad de que el Director de la Agencia de Protección de Datos proponga la iniciación de actuaciones disciplinarias por la vía establecida en la legislación sobre régimen disciplinario de las Administraciones Públicas.[116]

A tal efecto, la LORTAD establece en su artículo 43 un catálogo de infracciones leves, graves y muy graves, que se completa con los tipos recogidos en el Código Penal. De entre todas ellas podemos citar las siguientes:

A) Leves:

- No proceder a la rectificación o cancelación de errores, lagunas o inexactitudes de carácter formal de los ficheros, bien sea de oficio o a petición de persona o institución capacitada para ello.

- No cumplir las instrucciones del Director de la Agencia, o no suministrar la información requerida.

- No conservar los datos actualizados en los ficheros.

- Cualquier otra que afecte a cuestiones formales o documentales y que no constituya una infracción más grave.

B) Graves:

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos para los mismos sin cumplir las formalidades legales previstas.

■ 116 Cfr. arts 127 y siguientes de la Ley 39/92 de Procedimiento Administrativo y RD 1398/93 de 4 de agosto por el que se aprueba el Reglamento para el ejercicio de la potestad sancionadora.

- Recoger datos sin el consentimiento preceptivo o sin dar la información legalmente requerida.

- Realizar el tratamiento sin cumplir los principios de calidad y licitud o infringiendo los deberes establecidos en la Ley y demás disposiciones.

- Impedir u obstaculizar el ejercicio del derecho de acceso o negar la información solicitada.

- Mantener los datos inexactos o no proceder a rectificarlos o cancelarlos cuando ello proceda y resulten afectados los derechos de las personas.

- La vulneración del deber de secreto, cuando no sea infracción grave.

- No observar las medidas de seguridad técnicas y organizativas que reglamentariamente se determinen en los locales, programas y equipos.

- No remitir a la Agencia las notificaciones previstas en la Ley o en sus disposiciones de desarrollo o no proporcionarle cuantos documentos e informaciones deba recibir.

- Obstruir el ejercicio de la labor inspectora.

C) Muy Graves:

- La recogida de datos en forma engañosa o fraudulenta.

- Comunicar o ceder datos fuera de los casos permitidos.

- Recabar y tratar datos sensibles del artículo 7.2 sin consentimiento del afectado o los del artículo 7.3 sin consentimiento o cuando no lo permita una Ley.

- Crear ficheros cuya única finalidad sea tratar datos relativos a ideología, creencias, religión, origen racial o vida sexual.

- No cesar en el uso ilícito de los tratamientos cuando sea requerido por la Agencia.

- Transferir datos personales a países que no proporcionen un nivel adecuado de protección.[117]

- Realizar un tratamiento de los datos personales de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, si con ello se impide o atenta contra el ejercicio de los derechos fundamentales.

- La vulneración del deber de secreto con respecto a los datos especialmente protegidos.

La iniciación del procedimiento sancionador corresponde de oficio al Director de la Agencia por propia iniciativa o mediante denuncia del afectado. En el acuerdo del Director se designará al instructor y, en su caso, el secretario, así mismo se identificará al presunto responsable y se concretan los hechos imputados, con expresión de las infracciones cometidas, de las medidas provisionales a adoptar y las sanciones que pudieran imponerse.[118]

Dicho acuerdo de incoación de expediente se notifica al responsable y se le informa de su derecho a formular alegaciones y de utilizar los medios de defensa procedentes, citando expresamente los preceptos que son de aplicación. Dentro de los 15 días siguientes a la notificación, el instructor ordenará la práctica de cuantas pruebas y actos de instrucción sean procedentes para esclarecer los hechos y determinar las responsabilidades. En el mismo plazo, el presunto responsable puede hacer sus alegaciones y proponer las pruebas que estime convenientes.

Transcurrido aquél plazo el instructor acordará la practica de las pruebas pertinentes, a cuyo efecto concederá un plazo de 30 días, transcurrido el cual el expediente se pondrá de manifiesto al responsable para que en el plazo de 15 días formule sus alegaciones y aporte los documentos que estime de interés.

■ [117] Cfr. Orden del Ministerio de Justicia de 2 de Febrero de 1995.

■ [118] Cuando las infracciones son cometidas en ficheros de las Administraciones Públicas, el Director de la Agencia debe dictar una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notifica al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

Cumplidos los trámites se dicta la propuesta motivada de resolución que se notifica al presunto responsable para que formule las alegaciones oportunas, en el plazo de 15 días. Concluido éste, el instructor elevará el expediente al Director de la Agencia, quien puede ordenar la práctica de nuevas actuaciones.

La resolución ha de contener necesariamente los hechos imputados, la infracción cometida, el precepto que la tipifica, el responsable de la misma y la sanción impuesta; igualmente puede contener la declaración de no existencia de responsabilidad. Contra la resolución cabe interponer recurso contencioso-administrativo y ha de ser notificada también al denunciante, si lo hubiera.

Las sanciones pueden ser desde una multa de 100.000 pts hasta los 100 millones para las infracciones muy graves, si bien su cuantía se gradúa en función de los derechos afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad y a la reincidencia.

El artículo 197.2 del Código Penal impone las penas de prisión de 1 a 4 años y multa de 12 a 24 meses "al que sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos o a quien los altere o utilice en perjuicio del titular de los datos o de un tercero".

Si tales datos se revelan, difunden o ceden a terceros se impone la pena de prisión de 2 a 5 años. Se impone la pena de prisión de 1 a 3 años y multa de 12 a 24 meses al que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realice la conducta antes descrita.

Si los hechos antes descritos se realizan por los encargados o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impone la pena de 3 a 5 años de prisión y se difunden, ceden o revelan, se impone en su mitad superior.

Si tales actos están referidos a los datos especialmente protegidos o la víctima sea un menor o un incapaz, se impondrán las penas previstas en su mitad

superior. Ello se agrava si existe ánimo de lucro, pues la pena puede llegar hasta la prisión de 4 a 7 años.

El artículo 198 agrava la pena, e impone la inhabilitación absoluta por tiempo de 6 a 12 años, cuando el autor de las conductas descritas sea una autoridad o funcionario público que actúa prevaliéndose de su cargo.[119]

Para proceder contra estas conductas se precisa denuncia del agraviado o de su representante legal; no obstante, no se exige denuncia en los casos del artículo 198, ni cuando el delito afecte a los intereses generales o a una pluralidad de personas. Tal sería el caso de que la responsabilidad penal se derivase de hechos probados en una resolución sancionadora de la Agencia de Protección de Datos.

V.2- Derecho de Indemnización:

Las lesiones que se produzcan por incumplimiento de la Ley a los afectados en sus bienes o derechos, originan el deber de indemnizar. La reclamación en el caso de los ficheros de titularidad pública se substanciará según lo previsto en el artículo 139 y siguientes de la Ley 30/92 y legislación concordante. Para calcular la indemnización se atenderá al resultado dañoso, la existencia de intencionalidad, la responsabilidad profesional del personal al servicio de las Administraciones Públicas y su relación con la producción del resultado dañoso.

Las autoridades y personal al servicio de las Administraciones públicas responden de acuerdo a lo establecido en los artículos 145 y siguientes de la Ley 30/92, de suerte que la reclamación del particular se plantea directamente a la Administración, quien debe indemnizar al particular y luego actuar contra la autoridad o funcionario causante de la lesión, siguiendo el procedimiento reglamentario, sin perjuicio de pasar el tanto de culpa a los Tribunales competentes.

■ [119] Es también digno de mención que el artículo 200 del Código Penal extiende su protección a los datos reservados de las personas jurídicas.

Esta llamada a la "responsabilidad profesional" del personal nos induce a realizar una última reflexión: la mayoría de las Universidades han establecido como responsable del fichero al Secretario General, posiblemente por esa competencia de custodia de archivos y registros que posee todo secretario de órgano colegiado, pero ello no ha corrido paralelo con la capacidad de control sobre tratamientos que posee dicho responsable.[120] A menudo en estas cuestiones se exigen unos conocimientos técnicos y jurídicos que no concurren en algunas personas, por lo que se presume una preparación que no se posee y por cuya ausencia se debe responder.

De otro lado, los ficheros automatizados suelen estar adscritos a órganos o dependencias muy concretas: personal, alumnos, acción social, etc... cuyos jefes o responsables actúan con una elevada dosis de autonomía, por lo que el responsable "ex lege" no suele estar en contacto con su gestión diaria. Frente a todo ello, la L.P.A. establece que la responsabilidad civil por estas infracciones se mide según los criterios de la legislación civil, donde prima la responsabilidad objetiva por culpa "in vigilando" o "in eligendo" que hace responder por hechos ajenos.

Por todo ello consideramos necesario formar en la materia a todo el personal relacionado con los ficheros, establecer un adecuado marco normativo que consagre un claro esquema de competencias y responsabilidades y crear un órgano de control y seguimiento de los tratamientos y seguridad de los ficheros.

Con esto damos fin a estas breves y apretadas líneas en las que hemos querido llamar la atención acerca de un problema de cuya magnitud, tal vez, no seamos plenamente conscientes y, que sin embargo, por la gravedad de las consecuencias que pueden derivarse, precisa una mayor atención de las Universidades para evitar que un instrumento positivo como es la informática,

■ 120 No obstante, y a título de ejemplo, algunas Universidades han instituido como responsable al Gerente, caso de Valladolid o Baleares; otras al Director o Jefe del órgano al que está adscrito el fichero, caso de Zaragoza. Granada ha establecido la competencia del Secretario General, bajo la autoridad del Rector, "sin perjuicio de la responsabilidad directa que en la gestión y custodia de los ficheros corresponde al jefe de cada uno de los servicios o unidades".

pueda ser objeto de utilización para fines incompatibles con los servicios que presta la Universidad.

BREVE RESEÑA BIBLIOGRAFICA:

- A.A.V.V. " Jornadas sobre el derecho Español de la Protección de Datos Personales ". Madrid, 1996

- A.A. V.V.:" Banche dati e diritti della persona ". Milano, 1988

- Agencia de Protección de Datos: Memorias de los años 1994, 1995 y 1996

- Davara Rodríguez, M.A.:" Derecho Informático ". Pamplona, 1993

- Frossini, V.:" Informática y derecho ". Bogotá, 1988

- Pérez Luño, A.E.:" Manual de informática y derecho". Barcelona, 1996

- Revista "Informática y Derecho" de la UNED, números 1 al 11, Aranzadi, Pamplona.