

ENSAYO JURÍDICO DE DERECHO INFORMATICO

LOS DATOS PERSONALES INFORMATIZADOS EN EL DERECHO PUBLICO FORANEO Y COLOMBIANO

LOS DATOS PERSONALES INFORMATIZADOS EN EL DERECHO PUBLICO FORANEO Y COLOMBIANO

Por:

Libardo Orlando Riascos Gómez

Doctor en Derecho

Lriascos@udena.edu.co

2008

ABSTRACT

Esta investigación de derecho informático, estudia el concepto de datos o informaciones de las personas físicas, previsto en las Constituciones y legislaciones Norteamericanas, Europeas, Australianas y colombianas. De igual forma, se analiza jurídicamente los datos de la persona procesados mediante medios electrónicos, telemáticos o informáticos. Los datos electrónicos de la persona en el ámbito personal (salud, raza o etnia, sexo, religión, pensamiento filosófico, político, sindical, conocidos como datos del núcleo esencial de la intimidad o vida privada), social, familiar, económico, laboral; entre otros, son objeto de regulación normativa amplia, restringida o prohibida por los Estados del mundo. Hacer el análisis de esa normatividad es el objeto principal de este ensayo jurídico.

Palabras Claves: Dato, Información, Constitución, Legislación, base de datos, procedimiento e intimidad

ABSTRACT

This investigation of computer right, studies the concept of data or physical people's informations, foreseen in the Constitutions and North American, European, Australian and Colombian legislations. Of equal it forms, the person's data processed by means of electronic, telematic or computer means is analyzed legally. The person's electronic data in the personal environment (health, race or ethnos, sex, religion, philosophical, political, union thought, well-known as data of the essential nucleus of the intimacy or private life), social, family, economic, labor; among other, they are object of wide, restricted normative regulation or prohibited by the States of the world. To make the analysis of that normatividad is the main object of this juridical rehearsal.

Key words: Date, Information, Constitution, Legislation, database, procedure and intimacy

CONTENIDO

PARTE TERCERA

EL PROCEDIMIENTO INFORMATICO, ELECTRONICO Y/O TELEMATICO DE LOS DATOS PERSONALES II.

3.1. Conceptualizaciones técnico-jurídicas devenidas de las nuevas tecnologías de la información y la comunicación (TIC) y la informática jurídica

3.2. Sistemas de tratamiento informatizado y el procedimiento informatizado de datos.

3.2.1. Fases del procedimiento informatizado de datos.

3.2.1.1 Fase inicial o Input: recolección, selección y organización específica de datos.

**3.2.1.2 Fase de tratamiento informatizado propiamente dicho o fase *in* de datos
En especial, el almacenamiento, el registro y la conservación de datos personales.**

TERCERA PARTE

3. EL PROCEDIMIENTO INFORMÁTICO, ELECTRÓNICO Y/O TELEMÁTICO DE LOS DATOS PERSONALES.

3.1. CONCEPTUALIZACIONES TÉCNICO-JURÍDICAS DEVENIDAS DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN (TIC) Y LA INFORMÁTICA JURÍDICA.

El rediseño de algunos conceptos jurídicos genéricos, como procedimiento, fases, principios y algunos otros específicos como procedimiento informático, electrónico o telemático; sistemas de tratamiento de entrada y salida (E/S) “automatizados de la información”, “procedimiento de disociación”, datos de carácter personal, “datos sensibles”, han sido producto de la incursión en las áreas jurídicas de las llamadas nuevas tecnologías de la información y la comunicación TIC, en unión plena con la informática jurídica.

En el presente aparte trataremos de conciliar ese rediseño conceptual, cuando menos, a los solos efectos de explicar el que llamamos procedimiento informático, electrónico o telemático, apoyándonos en el criterio de que los términos: procedimiento, fases, y principios. Estos términos, no son instituciones jurídicas procesales y/o sustantivas propias y excluyentes de una rama del derecho, sino que están al servicio de las ciencias sociales por pertenecer a la teoría general del derecho ^[65], y por tanto, su utilización es patrimonio *erga omnes* y no *inter alios* en las ciencias jurídicas.

3.2. SISTEMAS DE TRATAMIENTO INFORMATIZADO Y EL PROCEDIMIENTO INFORMÁTICO DE DATOS.

La LORTAD al precisar lo que debemos entender por “*tratamiento automatizado*” (o mejor tratamiento informatizado, como se ha sostenido), siguiendo las directrices previstas en el Convenio de Estrasburgo de 1981 ^[66] y más recientemente concretados por la Directiva 95/467CE ^[67], ha sostenido que tratamiento de datos (“automatizados” o no) está constituido por el conjunto de “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”.

De aquella conceptualización podemos deducir que el tratamiento por medios informáticos, electrónicos o telemáticos que permita una serie de funciones propias de los datos personales (recolección, grabación, etc.) endilgadas a conseguir unos fines o propósitos predeterminados por una persona privada o pública conforme a un ordenamiento jurídico vigente, podemos estructurar lo que ha de entenderse como procedimiento informático, electrónico o telemático de datos personales.

En efecto, entendemos por *procedimiento informático* de datos personales (género que incluye a la especie electrónico o telemático, en similar circunstancia a la conceptualización de datos personales informáticos, electrónicos o telemáticos, realizada al iniciar este aparte), aquél

estructurado por una serie concatenada de etapas, fases o ciclos aplicables a los datos de carácter personal, de conformidad con el ordenamiento jurídico y apto para construir un fichero o banco de datos informatizados, o sistema estructural e informático de datos que permite; entre otras atribuciones: el almacenamiento, consulta, difusión, cancelación, bloqueo o transferencia electrónica de datos.

Los *sistemas de tratamiento informatizado*, según el ius-informático López Muñiz Goñi^[68], son aquellos de “carácter informático utilizados para establecer los criterios de búsqueda de los documentos”, datos de cualquier tipo o informaciones, previamente a su recogida, selección, organización, estructuración, almacenamiento y registro, a través de medios informáticos, electrónicos o telemáticos. Estos sistemas apuntan a dos funciones que a la vez, constituyen una caracterización de uno y otro sistema. Estos son: Los sistemas de tratamiento informatizado de entrada y salida (E/S) de información. Estos apuntan al ingreso (*input. I/*) o la extracción o salida (*ouput./O*) de información o datos estructurados informáticamente, constituyen la técnica metodológica idónea para recoger, almacenar y transferir datos o informaciones y cumplen funciones informáticas exclusivas de los ficheros o bancos de datos informatizados.

Los iusinformáticos como López Muñiz-Goñi^[69], han clasificado a estos sistemas desde el punto de vista formal y funcional. Por lo primero, los sistemas de tratamiento informático son de entrada y salida de información. Por lo segundo, hacen referencia a las funciones que los sistemas pueden tener, según sea sistemas basados en acceso o recuperación de información. Las funciones de los sistemas se fundamentarán en el texto completo o “*full text*”, en los “descriptores” (palabras claves organizadas en un thesaurio) o en los resúmenes o “abstracts” de un texto. Todos estos sistemas tienen sus ventajas y desventajas que giran en torno al momento de elaboración (factor temporal), la subjetividad de los analistas o especialistas (más o menos acentuada, según el sistema escogido), la clase, calidad y cantidad de información o datos manejados y los costos sociales, económicos e intelectivos utilizados en la realización y puesta en funcionamiento de los sistemas de entrada/salida (E/S) de información.

Hoy en día, todos los sistemas de tratamiento informatizado de información emplean un sistema mixto tanto en el *input* como en el *output* de la información o los datos. En efecto, se utiliza sistemas de texto completo unido al de descriptores o sistemas de resúmenes unidos al de descriptores. Estos sistemas en su elaboración, diseño y estructuración tienen una previa parte manual o humana y otra exclusivamente informatizada^[70], si se trata de “*tratamientos automatizados*” de información o datos, y será exclusivamente humano si se trata de tratamientos no automatizados. Esta aclaración se hace, ya que la LORTAD, como las normas comunitarias europeas hacen referencia expresamente a estas dos clases de tratamientos de la información, y además, porque es nuestro propósito destacar que aún el sistema informático de tratamiento de datos tiene una parte inicial o *apriorística* de claro tinte intelectual o humano que es el que prepara, selecciona, estructura, organiza la información para meterla a un sistema informatizado. Trabajo humano previo que esta cargado de todas las ventajas y desventajas que esta clase de labores especializadas requiere, por ejemplo, para la elaboración de un sistema de tratamiento informatizado de información o datos jurídicos con documentación jurisprudencial, se requerirá de un grupo multidisciplinario conformado por lingüistas, ius-informáticos, ingenieros de sistemas, operadores, y sobre todo juristas, pues de lo contrario el sistema desde el punto de vista de la esencialidad de los contenidos estará muerto antes de nacer.

Ahora bien, el procedimiento informático de datos, siendo el género, *el procedimiento electrónico o telemático de datos* es una de las especies que se estructura por la utilización de medios y soportes informáticos electrónicos o telemáticos de software y hardware que se detallan más adelante--. Desde el punto de vista ius-informático las funciones que cumple este procedimiento especial son las que la LORTAD determina como las de “cesiones de datos que resultan de las comunicaciones, consultas, interconexiones y transferencias”, o en forma más

explícita por la Directiva 95/46/CE, cuando hace referencia a que los “procedimientos automatizados, y aplicados a los datos personales... (en la) comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión...” Como puede apreciarse el procedimiento electrónico o telemático de datos se utiliza básicamente en la transmisión (emisión/recepción) de datos, y como tal, genera documentos, informaciones o datos de carácter electrónico o telemático que antes hemos comentado. Sin embargo, tanto el procedimiento genérico como el específico, tienen una misma estructuración en cuanto a las fases, ciclos o etapas, lo que los diferencia son las funciones que cada uno desarrolla en sistema de tratamiento informatizado. Sobre esto nos ocuparemos seguidamente.

3.2.1. FASES DEL PROCEDIMIENTO INFORMATIZADO DE DATOS.

El profesor *Morales Prats* ^[71], siguiendo al ius-informático *Frosini*, expone que en el *ciclo operativo de un sistema informático* (basado en el que se sigue para el estudio del *habeas scriptum* o *habeas data*), se distinguen las siguientes fases: a) Fase de recogida de datos; b) Fase de tratamiento y programación de la información; c) Fase de conclusión del procesamiento de datos; y d) La transmisión de la información. Esta última aunque *a priori* no la ubica como una de las fases del procedimiento informatizado de datos, luego sostiene que esta es una modalidad de “fase conclusiva del ciclo operativo” que incluso se puede subdividir así: a) cuando la circulación de datos se hace a través de un *circuito interno* de emisión (por medio de terminales de ordenador); o por *circulación externa*, que permite la divulgación de la información.

El autor citado, al comentar esta última modalidad de fase conclusiva del procesamiento de datos, hace recaer su importancia en que “la puesta en circulación de los datos materializa la dispersión de las informaciones de un individuo reunidas con anterioridad en el banco de datos y memorizadas de acuerdo al *software*. Este es el momento --agrega enfáticamente-- en que, potencialmente, pueden perpetrarse mayores atentados a la *privacy* de las personas; la libertad informática se traduce ahora en una auténtica *facultad de control* de la información personal, despojada de su carácter preventivo” ^[72].

En nuestro criterio, siguiendo las pautas, metodología y criterios establecidos para los sistemas de tratamiento informatizados de entrada y salida (E/S) de información estudiados por el profesor *López Muñoz-Goñi*, referenciados anteriormente y las directrices normativas previstas en la LORTAD y las normas comunitarias: Convenio de Estrasburgo de 1981 y la Directiva 95/46/CE., hemos clasificado las etapas del procedimiento informatizado de datos así: a) Fase inicial o de *input*, constituida por la recolección y organización de datos. Fase que aún estando dentro del sistema informatizado es esencialmente producto de una actividad humana interdisciplinaria, según el área del saber humano que se maneje; b) Fase de tratamiento informatizado propiamente dicho o fase *in* de datos. En esta fase se inicia básica y esencialmente el procedimiento informatizado (llamado “automatizado” por la normativa española y europea) con toda su caracterización, funciones, elementos, soportes y medios informáticos, electrónicos o telemáticos; c) Fase de salida de datos o fase *output*, que a su vez, se subdivide en fase *output* general y fase *output* especial, según se utilicen medios informáticos, electrónicos o telemáticos *off line* u *on line*.

3.2.1.1. FASE INICIAL O INPUT: RECOLECCIÓN, SELECCION Y ORGANIZACIÓN ESPECÍFICA DE DATOS.

Esta etapa en cualquier sistema informatizado se lleva a cabo con mecanismos, metodología e instrumentalizaciones de carácter humano, aunque no se descarta que parcialmente se realice con soportes y medios informáticos, electrónicos o telemáticos, una vez han sido recolectados los datos manualmente, tras la aplicación de encuestas, entrevistas, volantes, cumplimentación de formularios o impresos, etc. Es decir, que se recoge la información o datos con medios manuales para posteriormente seleccionar y organizarla con medios

informáticos, con programas de ordenador y hardware idóneos para la realización de dichas labores. Sin embargo, no se descarta que en algunas disciplinas del saber humano y en la formación de ciertos ficheros o bancos de datos (v.gr. con carácter estadístico, archivístico, histórico, científico e investigativo en sociología, economía, ingeniería e incluso en derecho), la recolección de información o datos se realice por completo con medios informáticos de software y hardware, por cuanto la información se halla almacenada en memoria central o periférica de un ordenador *off line* u *on line*. En este último se descarta la actividad de inmediatez humana directa y personal y se reemplaza por la realización humana indirecta a través de medios informáticos.

La parte de esta fase realizada con medios y recursos de carácter humano tiene como características principales la de ser una actividad humana, especializada, personal o por regla general de carácter colectivo y multidisciplinaria, según el tipo, cantidad y calidad de información o datos recogidos. Esta parte, con todas sus ventajas o desventajas constituye una parte de la fase inicial de carácter subjetivo, bien se haya realizado directa y personalmente o en forma indirecta con medios informáticos.

Como lo sostiene el profesor *Morales Prats* [73], durante este período se presentan los mayores problemas para el legislador; entre otros, los surgidos en torno a la fijación de los límites de la licitud de las recolecciones de datos. Como principio general debe propugnarse la *prohibición* de la recogida de los *datos sensibles*, cuyo procesamiento puede atentar la intimidad de las personas y en consecuencia posibilita prácticas discriminatorias; son informaciones que revisten esta calidad: los datos relativos a la raza, opciones religiosas, filiación política, actividades sindicales, hábitos sexuales, antecedentes judiciales, así como historiales sanitarios, entre otros. Esta prohibición debe estar por encima incluso de un eventual consentimiento del titular de la información o datos, y el cual sólo será permisible para la recolección de información de “carácter personal no sensible”, aunque el legislador deberá regular en forma “casuista”, cuales se consideran tal.

El Convenio de Estrasburgo de 1981, enfáticamente al categorizar las clases de datos personales sostuvo que los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente *a menos que* el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales (artículo6). Esta norma europea extiende este principio de prohibición de recolección de datos conocidos como del “*núcleo duro de la privacy*”, según el derecho anglosajón, como una regla general; pero establece una ventana de excepción a la prohibición, cuando sostiene que las legislaciones estatales podrán regular el tratamiento informatizado de aquellos datos si el ordenamiento jurídico previere específicamente medidas de protección y garantías apropiadas. Sin embargo, dicha excepción no se establece para los datos personales referidos a *condenas penales* (parte *in fine* del artículo citado).

La LORTAD (L.O. 5/1992, Oct. 29), en el marco del ordenamiento jurídico español al reglamentar el artículo 18.4 de la CE., toma como referente la ventana de excepción del Convenio Europeo, para establecer una categorización de datos personales según los niveles de protección referidos a cada una de estas. Así establece una clase de “datos especialmente protegidos” (artículo 7) y dentro de aquellos los subdivide así: a) Los datos relativos a la ideología, religión y creencias, según el artículo 16-2 CE, nadie está obligado a declarar en contra de aquellos, sólo podrán ser recolectados (o “recabados”), si existe consentimiento del titular, previa la admonición o derecho de información, de su “derecho a no prestarlo”; b) Los datos relativos a la ideología, religión y creencias, “podrán ser objeto de un tratamiento automatizado de datos de carácter personal”, con el consentimiento expreso y por escrito del titular de los mismos (“el afectado” dice indebidamente la norma). Aquí se permite no sólo la fase inicial del tratamiento informatizado, como en los datos personales del literal anterior, sino para todas las fases del procedimiento en esta categoría de datos; c) Los datos personales

referidos al origen racial, a la salud y a la vida sexual “sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo dispongan una ley o el afectado consienta expresamente” (artículo 7-3). Se permite el tratamiento informatizado en todas las fases del procedimiento, aunque hace énfasis en la etapa inicial y última del procedimiento, especialmente la referida a la trasmisión de datos por “cesión”; d) Los datos personales relacionados con la ideología, religión, creencias, origen racial o la vida sexual y hayan sido objeto de tratamiento informatizado en todas sus fases quedan “prohibidos” si su “finalidad exclusiva” radica en el “almacenar” estos datos (artículo 7-4). Aquí se prohíbe no la recolección de esta clase de datos con carácter informático, sino el almacenamiento en memoria central o periférica de los datos tratados informáticamente; y, e) Los datos de carácter personal relacionados con la “comisión de infracciones penales o administrativas”, sólo podrán ser tratados informáticamente, si el ordenamiento jurídico vigente sobre la materia lo permite. Esta dispensa legal para el tratamiento informático, excluye cualquiera otra. Sin embargo, la LORTAD en esta temática, utiliza indebidamente la terminología ius-informática, pues hace referencia a una posible “inclusión” en “ficheros automatizados de las Administraciones Públicas competentes” de datos relativos a la comisión de infracciones penales o administrativas, cuando lo que debe aclarar es si pueden ser o no objeto de tratamientos informatizados, a partir de qué fase o fases y hasta cuáles otras se extiende la prohibición o permisión, si fuere el caso.

Por su parte, la Directiva Comunitaria 95/46/CE, establece una regla general y amplia gama de excepciones sobre la prohibición para todo el tratamiento informatizado de categorías especiales de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad (artículo 8). La Directiva no hace distinción ni en el nivel ni en los requisitos exigidos para la protección de las diversas categorías de datos personales, como sí lo hace la LORTAD. Sin embargo, establece una serie de excepciones a la regla general, como es usual en la normativa comunitaria, que en nuestro criterio hace casi nulatoria la regla.

A título enunciativo veamos algunas de las excepciones. Estas son: a) Cuando haya dado su consentimiento explícito a dicho tratamiento, salvo que la legislación de los Estados miembros de la CE., disponga que la prohibición no puede levantarse aún con el consentimiento del titular de los datos; b) El tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho Laboral en la medida en que esté autorizado por la legislación y éste prevea garantías adecuadas; c) El tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento; d) El tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados; e) El tratamiento se refiere a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial (artículo 8-2, literales (a), a (e),) .

Se establece también en la norma comunitaria, unas excepciones de carácter especial, según se trate de datos personales de carácter médico; por motivos de interés público; o bien, se refieran a datos relativos a infracciones, condenas penales o medidas de seguridad, sanciones administrativas o procesos civiles (artículo 8-3 a 5). En estos casos previo el lleno de unos requisitos de forma y de fondo, tales como: a) para el caso de datos personales médicos, se requiere que el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al *secreto profesional* sea en virtud de la legislación nacional, o de las normas

establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto; b) En el caso de datos personales, por “motivos de interés público importantes”, podrán ser sujetos de tratamiento, con las excepciones previstas en los literales (a), a (e) del artículo 8-2 de la Directiva 95/46/CE, o las que establezca el derecho interno de los Estados miembros, o bien por una autoridad de control de los poderes públicos (jurisdiccional o administrativa); y, c) En el caso de los datos personales relativos a infracciones, condenas penales, medidas de seguridad, sanciones administrativas o procesos civiles, podrán ser objeto de tratamiento cuando se realicen “bajo el control de la autoridad pública” o si el derecho interno de los Estados miembros prevén garantías apropiadas y específicas. Sin embargo, para el caso de las condenas penales, podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. En los casos anteriormente previstos en los literales b) y c), los Estados miembros de la CE, “notificarán a la Comisión” creada al efecto por la Directiva.

Una especial consideración de la Directiva, le dedica al tratamiento de datos personales y la “libertad de expresión”, cuando permite dicho tratamiento, siempre y cuando sea con fines exclusivamente periodísticos o de expresión artística o literaria, llamando la atención a los Estados miembros para que establezcan “exenciones y excepciones” en la medida que resulten necesarias para “conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión” (artículo 9).

Una directriz general que establece la Directiva Comunitaria aplicable no sólo a la fase inicial del tratamiento informatizado sino durante toda la existencia de éste es como sigue: los datos recogidos con “fines determinados, explícitos y legítimos”, no serán “tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas” (artículo 6-b.).

Ahora bien, sea que se permita el tratamiento informatizado de datos personales y dentro de estos los denominados “sensibles” (caso LORTAD), o bien se permita el tratamiento de datos personales por vía de excepción (caso de las normas comunitarias: Convenio y Directiva), o más aún se permita dicho tratamiento, porque así está previsto en el ordenamiento jurídico vigente comunitario o nacional (caso de España), el titular de los datos personales sometidos a tratamiento tendrá una enriquecida serie de derechos, pero también deberes que cumplir.

En efecto, estos derechos y deberes surgen *ipso jure* con el sometimiento de un dato personal a un procedimiento informatizado.

No pretendemos agotar en este aparte el tema, que por demás ha sido objeto de estudio concienzudo y amplio en el derecho privado español v.gr. *Orti Vallejo* [\[74\]](#) y *López Díaz* [\[75\]](#), sino destacar esos aspectos importantes de la visión ius-informática de la intimidad, en armonía con los principios de protección de los datos personales cuyo tratamiento ha sido mediante medios informáticos, electrónicos o telemáticos.

En efecto, en el Título II de la LORTAD, bajo el nomen de “Principios de la protección de datos”, se recogen principios propiamente dichos, derechos (como el de *habeas data* en toda su extensión: acceso, actualización, rectificación, cancelación o borrado de datos y el *derecho a la información*, y que son objeto específico del Título III, LORTAD) y obligaciones de los sujetos intervinientes (v.gr. El ejercicio de las acciones pertinentes en caso de fallecimiento del interesado; las del responsable del fichero; la gestión del fichero por un tercero por cuenta del responsable del fichero, etc) en el tratamiento de datos por medios informáticos, electrónicos y telemáticos, con lo cual el contenido no se compadece con la rúbrica; más aún, constituye una rémora que arrastra la LORTAD del Convenio del Consejo de Europa, posteriormente reiterada por la Directiva 95/46/CE, e incluso contiene una avalancha de excepciones a los principios de protección de datos que en momentos los hacen nugatorios, o cuando menos, los dejan tan endeblés que parece no existieran en la ley como candados de protección, pues cualquier llave

o algo que se le parezca los abre. De ahí que se hayan presentado diversas demandas de inconstitucionalidad ante el Tribunal Constitucional Español que desde 1994, hasta la actualidad esperan resolución.

Entre muchas otras clasificaciones, destaquemos la del profesor Davara ^[76], el cual los clasifica, así: a) Pertinencia de los datos, b) El derecho de información de los afectados de modo expreso, preciso e inequívoco, c) El consentimiento, salvo que la Ley disponga otra cosa, d) La Cesión de los datos. Por su parte, Souvirón ^[77], agrupa a los principios, así: a) De congruencia y racionalidad, b) Transparencia, c) Calidad y veracidad de los datos almacenados, d) El consentimiento o de autodeterminación del “afectado”, diferente si son datos personales de carácter general o se trata de datos denominados “sensibles”, e) Seguridad de los datos; y, f) El Principio del Secreto.

Ahora bien, teniendo en cuenta que los principios no son meras declaraciones pragmáticas establecidas por el legislador, sino contenidos axiológicos que sirven a unos fines u objetivos de la materia objeto de la misma ley y que por esto son de la esencia en la interpretación o hermenéutica jurídica de los asuntos relacionados. En otros términos, son contenidos de esencia, presencia y decisión de un continente o materia específica. En nuestro caso, los principios de protección de los datos personales deben revelar esos contenidos de esencia, presencia y decisión en las fases del procedimiento de tratamiento por medios informáticos, electrónicos o telemáticos de los datos, pues es hacia ahí donde están orientados rectamente estos principios, no hacia los derechos y deberes de los sujetos intervinientes en el procedimiento, pues estos tienen su estructura propia delimitada por la misma LORTAD, aunque obvia y finalmente los implique, tal y como veremos más adelante.

En tal virtud, en la *fase inicial de recolección, selección y organización de los datos personales*, deben imperar una serie de principios que involucran a la licitud, calidad, cantidad, oportunidad, proporcionalidad, compatibilidad con los fines de los datos mismos y de información. En este sentido, la LORTAD, establece que los datos deben ser adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que se haya obtenido (artículo4.1). Estas finalidades que deben perdurar hasta las fases de almacenamiento, conservación y utilización de los datos (Exposición de Motivos --en adelante: E.de M.-- y artículo4.2. LORTAD).

En la E. de M. de la LORTAD, ha quedado patentizado estos argumentos cardinales, así:

Los principios generales, por su parte, definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados cuanto la congruencia y la racionalidad de la utilización de los datos. Este principio, verdaderamente cardinal, de la congruencia y la racionalidad, garantiza que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados; su observancia es, por ello, capital para evitar la difusión incontrolada de la información que, siguiendo el mandato constitucional, se pretende limitar.

Igualmente, atendiendo al consentimiento de forma inequívoca dado por el interesado en el momento de la recogida de datos y por las subsiguientes fases del procedimiento y cuya “base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recogida de datos sea lícita” (E de M., LORTAD) ^[78], el interesado deberá ser previamente informado de modo expreso, preciso e inequívoco de una serie de actividades, facultades y derechos (constitucionales --artículo 16.2 CE-- o, legales --artículo5 a 8-- LORTAD) que le conciernen como sujeto titular, identificado o identificables (*cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de una persona*) de los datos, mismos que se abordan al final de esta parte del trabajo.

Actividades previas y derechos tales como: a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos, d) De la posibilidad de ejercitar el *habeas data* y, e) De la identidad y dirección del responsable del fichero. De igual manera, a exigir que los cuestionarios u otros impresos utilizados para la recogida, sean claros, precisos y con las advertencias pertinentes al caso (artículo 5.1 y 5.2 LORTAD).

En el Convenio Europeo de 1981, en iguales términos determina la mencionada serie de principios para esta fase inicial del procedimiento, bajo el intitulado de “Calidad de los datos” (artículo 5) y “Categorías particulares de datos” (artículo 6), haciendo énfasis en que los datos se obtendrán y tratarán leal y legítimamente, serán exactos y si fuere necesario puestos al día y queda prohibido la recolección como cualquier tratamiento “automatizado” de datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos relativos a la salud, a la vida sexual o los referentes a las condenas penales.

En la Directiva 95/46/CE, divide estos principios de la fase inicial del procedimiento en los principios relativos a la “calidad de los datos” y los principios relativos a la “legitimación del tratamiento de datos”. Entre los primeros destaca que los datos personales objeto y sujetos a tratamiento informatizado por parte de los Estados miembros, al menos en la fase inicial del procedimiento se tendrá en cuenta que estos datos serán tratados así: a) de manera leal y lícita, b) recogidos con fines determinados, explícitos y legítimos, c) ser adecuados, pertinentes y no excesivos a los fines para los cuales se recogen (“recaban”), d) ser exactos, y cuando sea necesario, actualizados, e) recogidos y conservados en una forma que permita la identificación de los interesados.

En los principios relativos a la legitimación del tratamiento de datos, establece unos derechos-deberes para los titulares de los datos, así como una serie de garantías para los Estados miembros que deben implementar cuando un dato personal se someta a procedimiento informatizado. El titular de los datos o “interesado” como le llama la Directiva, permitirá el tratamiento informatizado de datos personales, siempre que: a) haya dado su consentimiento de forma inequívoca; b) sea necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas pre-contractuales adoptadas a petición del interesado; c) sea necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento; d) sea necesario para proteger el interés vital del interesado; e) sea necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos; y, f) sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieren protección, en particular el derecho a la intimidad (artículo 7 en conc. artículo 1-1, Directiva).

En la *Privacy and data Protection Bill 1994 (NSW) Australiana* [\[79 \]](#), establece una serie de principios aplicables a las diferentes fases del procedimiento informatizado que hemos planteado. En efecto, el artículo 21, consagra como primer principio el de “La manera y propósitos de la recolección de la información”, en éste se establece que la información personal no debe ser coleccionada por una personal natural o jurídica (institución, entidad o corporación) privada o pública, para la inclusión en un registro informático (fichero o banco de datos) o en una publicación generalmente disponible a menos que : a) la información sea reunida para propósitos legales directamente relacionados con una función o actividad del propias del recolector de la información o coleccionista; y , b) la recolección de la información sea necesaria para cumplir con los propósitos señalados. En todo caso, la información o datos personales no deben ser recogidos por medios ilegales o injustos.

3.2.1.2. **FASE DE TRATAMIENTO INFORMÁTICO PROPIAMENTE DICHO O FASE *IN* DE DATOS. EN ESPECIAL, EL ALMACENAMIENTO, EL REGISTRO Y LA CONSERVACIÓN DE DATOS PERSONALES.**

Si bien el tratamiento informático comienza con la recolección, selección y organización de la información, la fase propiamente informática inicia, por regla general, en la presente fase, la cual hemos denominado *fase in de datos*; o una vez, que se disponga de un software y hardware apropiados para el tratamiento informatizado de los datos personales, la fase es *in tótum Informática de datos*.

Esta fase se subdivide, a su vez, en otras subetapas necesarias para el pleno desarrollo del tratamiento informático de los datos personales. Estas son: almacenamiento en memoria central o periférica de ordenador (storage), el Registro Informático (visión ius-informática y iusadministrativa), y la conservación de datos (jurídica y tecnológicamente) que implica no sólo el mantenimiento sino la administración de los datos, según su origen y fines para los que fueron recolectados, almacenados y registrados por los responsables (públicos o privados) de los mismos.

La aclaración del inicio propiamente informático obedece a la advertencia hecha en la anterior fase sobre la actividad esencialmente humana del procedimiento, salvo que se realice con datos personales con fines exclusivamente estadísticos, históricos, científicos, investigativos, archivísticos o de cualquier otro género parecidos que se hallen almacenados en memoria central o periférica de un ordenador o sea producto de transmisión o teletransmisión (emisión/recepción) de datos, con similares fines. En consecuencia, la fase inicial del tratamiento puede ser exclusivamente humana o tecnológica o informática o mixta. En cambio, esta fase es exclusivamente tecnológica o informática, pues los datos ya recogidos, seleccionados y organizados son objeto directo de tratamiento por software o hardware idóneos con soportes y medios informáticos, electrónicos o telemáticos.

Ciertamente, como afirma el profesor *Morales Prats* ^[80], los requisitos para un tratamiento de los datos, controlado y con garantías, se centran, por un lado, en la adopción de medidas de seguridad técnicas que preserven los datos adquiridos de accesos ilícitos y de fugas de información y, por otro lado, en el mantenimiento de la transparencia durante el proceso hasta la obtención de los resultados de programación (software). Sin embargo, también debe implementarse medidas no sólo que aseguren los datos personales *per se* sino que también garanticen los derechos y deberes de los titulares de los mismos, a la vez, que potencien las garantías sustantivas y procesales por parte de los Estados en sus respectivos ordenamientos jurídicos. A fin de analizar estos aspectos en su conjunto pasamos a analizar las subetapas de esta fase.

3.2.1.2.1. **EL ALMACENAMIENTO ELECTROMAGNETICO DE DATOS PERSONALES.**

Almacenar datos personales, al menos a los fines de este trabajo, consiste en guardar electromagnéticamente datos digitales (texto, sonido e imágenes) con y en soportes y medios informáticos, electrónicos o telemáticos de software o hardware (en forma provisional o definitiva), datos considerados personales por el ordenamiento jurídico, aptos de ser objeto y sujetos de tratamiento informatizado, a fin de que cumplan los propósitos legales y legítimos previstos desde del inicio del tratamiento informatizado conforme lo autoriza el ordenamiento jurídico o autoridad competente.

El almacenamiento de datos personales constituye por tanto, una actividad tecnológica de carácter informática con soportes y medios igualmente informáticos configurada por esta parte eminentemente tecnológica (software y hardware idóneos); y otra, de índole jurídica. Tecnología y derecho interactúan de forma plena en un marco de almacenamiento lícito, legítimo y ajustado a los requerimientos tecnológicos. Aquí haremos énfasis en aspecto jurídico.

El almacenamiento electrónico de datos, en soportes y medios de hardware, sea en forma provisional (en memoria central del ordenador) o sea en forma definitiva (en el *hard disk del ordenador*, discos flexibles, discos compactos, o unidades de “backup” --copias de seguridad--), se realiza en formatos, velocidades y lógica de ordenación de datos o información con carácter electromagnético, por ser una de las principales funciones de todo sistema, equipo o dispositivo de computador. El almacenamiento de datos en el *hard disk*, como uno de los dispositivos más importantes de entrada y salida (E/S) de información, lo es, porque en términos de Norton ^[81], es una especie de “*biblioteca de referencia del ordenador, centro de clasificación y caja de herramientas, todo en uno*”.

El almacenamiento de datos, en soportes y medios de software o programas de computador tecnológicamente siguen los mismos pasos de E/S de información que para los soportes y medios de hardware, tanto en forma provisional como definitiva, con la diferencia de que en éstos el almacenamiento es de carácter lógico o intangible y en aquellos de carácter material o físico ^[82].

Almacenar electromagnéticamente datos de cualquier índole, descarta la simple acción de almacenamiento indiscriminado, ilegítimo e ilegal, sin parámetros de la lógica electrónica (que incluye potencialidades y funcionamiento electrónicos posteriores para un usuario de un fichero o banco de datos), tal como si fuese un gran armario donde se guardan cosas, elementos, papeles o documentos continentales de datos y a los cuales puede acceder cualquier persona en el momento que les plazca. Es decir, se descarta aquellos armarios o “ficheros o banco de datos” que en concepto de *Fairen Guillén* ^[83], son simples “*almacenes de datos*”, en donde la “menor indiscreción --perdónese la palabra, aquí no demasiado adecuada-- puede producir la ruina del honor, de la familia, de la intimidad del ciudadano”, puesto que no es una visión ius-informática del término almacenar la que se vierte y entiende con aquél concepto, sino una visión gramatical aplicada por deducción al *storage electrónico*.

Para entender el *storage electrónico*, debemos partir de la lógica del mundo escriturario o de la impresión y luego adentrarnos en la lógica electrónica (según el profesor *Ethain*), pues almacenar datos electrónicamente no sólo es apilar, guardar o compilar información o datos como papeles o documentos en un armario, sino que almacenar (como fenómeno electromagnético) incluye además actividades; tales como: la organización en memoria del ordenador (sea por fecha de creación, por extensión del archivo o *file*, en orden alfabético, en orden ascendente o descendente, etc); seleccionar, estructurar (según entrada de archivos, programas base o aplicativos, por jerarquía en el árbol de directorios, subdirectorios, --*The Tree*-- , etc); enlistar o encaminar (seguir un *path*) y proporcionar *a posteriori*, en el acceso a aquellos datos, una información en formatos y velocidades igualmente electrónicas. Quizá por esta versatilidad en las posibilidades y funciones de los datos almacenados electromagnéticamente, es por lo que no puede seguirse pensando en el término almacenar como sinónimo de arrumar o apilar sino que debemos sintonizar el término con el fenómeno iusinformático y lo que ello engendra, cuando menos, en el mundo del derecho.

El *storage electrónico* en memoria central y periférica de un ordenador de los datos personales, sea cual fuere el *programa o software-base* ^[84] que se utilice, junto a los *programas-aplicativos* ^[85], deben reunir los requisitos técnicos preestablecidos por la autoridad, institución, entidad u organismo encargado de aplicarlos, a fin de cumplir con los propósitos legales, lícitos, legítimos y justos *a priori* perseguidos con el mentado tratamiento. Estos requisitos están previstos en el ordenamiento jurídico para homologar, estandarizar; y en fin, generalizar la aplicación y utilización de estos medios tecnológicos conforme a derecho. En la legislación española, por ejemplo, se ha iniciado con la regulación de la utilización de soportes, medios y aplicaciones informáticas, electrónicas y telemáticas en el sector público ^[86], lo cual no obsta para extender su aplicabilidad al sector privado, pues la LORTAD, proporciona facultades de control técnico-jurídico a instituciones con un régimen y representatividad jurídicas *sui generis* (puestos en evidencia por inconstitucionalidad, ante el Tribunal Constitucional Español), conocido como la Agencia de protección de Datos.

La LORTAD, las normas comunitarias, y en general, las normas sobre datos personales sometidos a tratamiento informático, electrónico o telemático, han puesto mucho énfasis en esta sub-fase de la etapa input de datos, pues como lo sostiene la LORTAD en la E. de M., “*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*”. Amenaza que unida al avance de las tecnologías de la información y de la comunicación (TIC), que “*permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos*, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos. Los más diversos --datos sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado “dinero plástico”, sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner sólo algunos ejemplos--, relativos a las personas podrían ser, así, compilados y obtenidos sin dificultar” [\[87 \]](#).

Como fundamento primigenio de protección y garantía de los derechos y libertades públicas de los titulares de datos personales, almacenados en ficheros o bancos de datos, ha instituido, “el principio de consentimiento, o de autodeterminación”, por medio del cual el titular es consciente de sus actos, hechos u omisiones referentes a los datos personales que ha entregado, y a la vez, esta informado plenamente de aquellos que han sido recolectados [\[88 \]](#) y almacenados por su propio querer de conformidad con el ordenamiento jurídico y/o autoridad competente. Por ello, en la E.de M., de la LORTAD se afirma que la protección de los datos personales “ se refuerzan singularmente en los denominados “datos sensibles”, como pueden ser, de una parte, la ideología o creencias religiosas --cuya privacidad está expresamente garantizada por la Constitución en su artículo 16.2-- y, de otra parte, la raza, la salud y la vida sexual” [\[89 \]](#).

Con base en estas previsiones de claro tinte proteccionista, así como las sostenidas por el Convenio Europeo de 1981, sobre la materia, y también las contenidas en la CE (artículo 10), la LORTAD, pone más énfasis en algunos de los datos personales considerados parte del *núcleo duro de la privacy*, cuando sostiene: “quedan prohibidos los ficheros creados con la finalidad exclusiva de *almacenar datos de carácter personal* que revelen la ideología, religión, creencias, origen racial o vida sexual”. (artículo 7-4), aunque los otros no es que se excluyan por deducción, como pudiera pensar *apriorísticamente*, pues estos quedan tácitamente incluidos dentro de la prohibición mentada cuando hace referencia al tratamiento informatizado de los datos, pues el almacenamiento, como hemos sostenido hace parte de ese tratamiento.

Por su parte la Directiva 95/46/CE, establece un cuadro de protección genérica del procedimiento informatizado de datos dentro del cual se incluye la sub-fase de almacenamiento. En efecto, la norma sostiene: “ los principios de protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad en lo que se refiere al tratamiento de los datos personales objeto de la presente Directiva podrán completarse o precisarse, sobre todo en determinados sectores, mediante normas específicas conformes a estos principios” (Considerando 68); es decir, a los principios relativos a la calidad de los datos (artículo6) y a los principios referidos a la legitimación del tratamiento de datos (artículo 7), que hacen referencia a la licitud y legitimidad de los tratamientos de datos personales, antes enunciados según los parámetros de la LORTAD.

Sin embargo, cabe resaltar el Derecho a la información que tiene el titular de los datos cuando estos sean recabados del propio interesado, o incluso cuando no han sido recolectados de éste, no sólo en el momento de la recolección de los mismos, como viene siendo estudiados y exaltados, por la doctrina [\[90 \]](#) sino, y por sobre todo en el momento del almacenamiento de los mismos, pues es aquí donde se genera como surtidor, tanto el cuadro proteccionista o garantista de los derechos o libertades públicas por los Estados, como los posibles y gamados métodos de desconocimiento y vulneración de aquellos, y por tanto, conviene enfatizar unos y otros en esta sub-etapa del proceso informático, máxime cuando la recogida de datos ha sido

eminentemente informática, puesto que diferente es el caso si la recolección de datos es total o parcialmente humana, como antes hemos visto.

En efecto, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar al titular de los datos personales que le conciernan, lo siguiente: a) la identidad del responsable del tratamiento, o de su representante, según fuere el caso; b) los fines del tratamiento de que van a ser objeto los datos; c) la información sobre los destinatarios o las categorías de destinatarios de los datos; d) el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder; e) la existencia de derechos de acceso y rectificación de los datos que la conciernen, si fuere del caso (artículo 10 Directiva.)

El Derecho de información cuando los datos no han sido recolectados del propio interesado, se hace efectivo así: Los Estados miembros dispondrán que el responsable o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información siguiente, a menos que ya hubiese sido informado (Esto no se aplicará en el caso del tratamiento de datos con fines estadísticos o de investigación histórica o científica ^[91]). Estos son:

a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que va a ser objeto los datos; y en fin, los mismos otros derechos que tiene el titular de los datos cuando han sido recogidos del propio interesado (Artículo 11).

En la *Privacy and data Protection Bill 1994 (NSW) Australiana* ^[92], establece una serie de principios aplicables a las diferentes fases del procedimiento informatizado. El principio de "Storage and security of information", aplicable a esta fase del procedimiento informatizado estudiado está previsto en la ley especial australiana referenciada que establece, lo siguiente: El responsable (persona natural o jurídica, pública o privada) de la posesión o administración de datos o informaciones (registros desde el punto de vista iusinformático) esta obligada a: a) guardarlos de conformidad con los propósitos o fines explícitos, legales y con los usos determinados para aquéllos; b) almacenar los datos o informaciones en forma adecuada y pertinente, sin exceder los propósitos para los cuales fue almacenado (es decir, que exista proporcionalidad de los fines en la recolección y almacenamiento de los datos); c) confirmar que el procedimiento informático hasta esta etapa se ha realizado en forma justa y legal; d) Almacenar los datos por un lapso de tiempo necesario de conformidad con los fines perseguidos con dicha actividad; e) Proteger los datos almacenados aplicando medidas idóneas de seguridad contra la posible pérdida, acceso desautorizado, modificación, descubrimiento y/o divulgación no autorizados; y en general, contra el uso indebido de los mismos; y f) Suministrar la información concerniente a una persona y en poder del responsable de la misma, siempre que con esta actividad se prevenga un uso desautorizado o un descubrimiento de información no autorizada (Artículo 21).

3.2.1.2.2. REGISTRO Y CONSERVACION ELECTROMAGNETICA DE LOS DATOS .

¿Qué se entiende por registro de datos desde el punto de vista iusinformático?. Es la gran pregunta que debemos hacernos en éste punto, pues tanto la LORTAD, como las normas comunitarias; y en general, las normas que regulan el tratamiento informatizado de datos de carácter personal, se refieren todas a la actividad iusadministrativa de "inscripción en el Registro" de un fichero o banco de datos personales de índole informatizada, pero en manera alguna al registro iusinformático de los mismos, con la salvedad de la LORTAD, que hace referencia tácita a éste como veremos. En efecto, los cuerpos normativos sobre tratamiento informatizado de datos personales (LORTAD: LO 5/1992, 29 Oct.; Convenio Europeo de 1981; Directiva 95/46/CE; Privacy and data Australiana 1994, etc) hacen referencia a la inscripción en el registro de un fichero o banco de datos informatizados que contiene una cantidad de datos

considerados personales por el ordenamiento jurídico vigente, y como tales permitida su recolección y posterior almacenamiento electromagnético. Esta actividad es realizada, por regla general, por un organismo autónomo y colegiado creado al efecto, de régimen jurídico administrativo o *sui generis* como en el caso español ^[93] que cumple funciones de registro, vigilancia, control, administración e incluso sancionatorias y correctivas.

El Registro de datos desde el punto iusinformático o *registro informático* ^[94], abarca no sólo la actividad iusadministrativista de la inscripción informática ante una autoridad competente de un fichero o banco de datos contentivo de información catalogada como personal, sino también la previa e ineludible actividad electromagnética de la grabación (*save*) y confirmación del *storage electrónico de datos* digitales (texto, sonido o imágenes) en y con soportes y medios informáticos, electrónicos y telemáticos. Es decir, que el registro iusinformático contiene una etapa *a priori* y de carácter interna y otra, *a posteriori* de carácter externa. La primera se verifica por y ante la misma persona natural o jurídica, pública o privada titular del fichero o banco de datos; y la segunda, se lleva a cabo ante la autoridad competente para crear, llevar, gestionar y cumplir los fines y funciones del Registro General de los ficheros o bancos de datos de carácter personal de conformidad con el ordenamiento jurídico vigente.

La distinción de estas dos etapas en el registro de datos interesa determinarla a los siguientes efectos: a) confirmar que los datos de carácter personal son informaciones concernientes a las personas. En particular, toda información alfanumérica, gráfica, fotográfica, acústica, o de cualquier otro tipo susceptible de ser recolectada, *registrada*, tratada o transferida concerniente a una persona física identificada o identificable, por soportes y medios informáticos; b) Verificar y confirmar que los datos personales son susceptibles de almacenamiento y registro electromagnético. Se descartan los datos no susceptibles de procedimiento informático, es decir, los sujetos a tratamiento no informatizado; y ,c) En el caso de la legislación especial de tratamiento informatizado de datos española (LORTAD), la determinación, el momento y oportunidad jurídico-legal de iniciación del “*procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos*”, que regulará por el Ministerio de Justicia, por vía reglamentaria, aún no desarrollado (artículo 38-3)

Muy a pesar de ello, se ha dado más relevancia a la actividad *a posteriori* o externa del registro informático, más que a la previa por considerarla una fase enteramente tecnológica y casi sin incidencia jurídica. El Real Decreto No. 263 de Febrero 16 de 1996, que reguló la utilización de técnicas electrónicas, informáticas y telemáticas, vino a llenar en parte ese vacío legislativo, por lo menos en el ámbito del sector público, en el caso español. En una y otra etapas del registro informático se abren y cierran amplios portales de riesgo, vulneración o consolidación de derechos y deberes para los titulares de datos personales, de ficheros o bancos de datos e incluso de terceros que son dignos de estudiarse desde la óptica de los principios de protección y seguridad de los datos. Ciertamente, en el ámbito de la legislación de tratamiento informatizado de datos español, en forma expresa y con base en el principio de seguridad de los datos, se hace referencia a las dos etapas del registro informático cuando se prohíbe el registro de los datos de carácter personal contenidos en ficheros o bancos de datos informatizados que no reúnan las condiciones que se determinen por vía reglamentaria (por el Ministerio de Justicia) con respecto a su integridad y seguridad y a los centros de tratamiento, locales, equipos, sistemas y programas (Artículo 9 LORTAD).

Pese a todo, a nivel de la legislación española, se enfatiza en el registro informático en su fase externa, el cual se adelanta ante un órgano integrado en la “Agencia de Protección de datos” (artículo 38, LORTAD), denominado *Registro General de Protección de Datos*, reglamentado por el Real Decreto No. 428 de Marzo 16 de 1993, al que corresponde velar por la publicidad de la existencia de los ficheros o banco de datos informatizados de carácter personal, con miras a viabilizar el pleno ejercicio de los derechos de información, acceso, rectificación y cancelación

de datos previstos en los artículos 13 y 15 de la L.O. 5/1992, de Oct. 29. (Artículo 23). Igualmente tiene funciones de instrucción de procedimientos de inscripción en el Registro, instrucción, certificación y publicación periódica de anuarios de ficheros o bancos de datos notificados e inscritos ^[95].

Son objeto de inscripción en el Registro General de Protección de datos, los siguientes ficheros o bancos de datos, actos y documentos: a) Los que sean titulares las Administraciones Públicas ^[96]. En los asientos de los ficheros de titularidad pública figurará, la información contenida en la disposición general de creación o modificación del fichero, de conformidad con el artículo 18.2., LORTAD ^[97] (Artículo 24-2. R.D.428 de Marzo 16 de 1993), b) Los de titularidad privada. En los asientos de inscripción de estos ficheros figurarán la información contenida en la notificación del fichero a excepción de las medidas de seguridad, así como los cambios de finalidad del fichero (Artículo 24-3, R.D.428 de Marzo 16 de 1993). c) las autorizaciones en materia informática, tales como las autorizaciones de transferencia temporal o definitiva de datos personales a otros países, siempre que medie autorización del Director de la Agencia de Protección de Datos, y los países ofrezcan un nivel de protección equiparable al de España, sobre tratamiento informatizado de datos (Artículo 25, (a), R.D.428 de Marzo 16 de 1993; conc. Artículo 32, LORTAD), d) *Los códigos tipo*, que con el carácter de normas deontológicas o de buena práctica profesional, se formulan por los responsables de los ficheros de titularidad privada. (Artículo 25, (b), R.D.428 de Marzo 16 de 1993; conc. Artículo 31, LORTAD ^[98]), d) los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación (Artículo 24-4 R.D.428/93 de Mar.16; conc, Arts.13 -15 y 38-3, LORTAD).

En consecuencia, no son objeto de inscripción en el Registro, y por tanto, sujetos de las medidas de protección y seguridad referida a los datos de carácter personal según el ordenamiento jurídico, los datos excluidos de la relación *numerus clausus* anterior.

Sin embargo, cabe interpretar también que no son objeto de inscripción, los ficheros o bancos de datos, cuya información o datos se halla prohibida someterla a procedimiento o alguna fase del tratamiento informatizado según el ordenamiento jurídico. En efecto, quedarían por fuera de la inscripción todos los ficheros que según la LORTAD, se excluye del tratamiento informatizado en forma taxativa, a saber: a) Los ficheros de titularidad pública, cuyo objeto sea el almacenamiento de datos para su publicidad con carácter general, b) los ficheros mantenidos por personas físicas con fines exclusivamente personales, c) los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales, d) los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales, e) los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 LORTAD, salvo que resultara de aplicación el artículo 7 LORTAD, por tratarse de los datos personales en él contenidos. Esta exclusión del tratamiento y de la consiguiente inscripción en el Registro queda explicada en la E. de M. de la LORTAD, al precisar por “exclusión” el ámbito de aplicación de la misma ^[99].

En la *Privacy and data Protection Bill 1994 (NSW) Australiana* ^[100], al referirse al principio 5 del artículo 21 *ab initio*, sobre la “information relating to records kept by record-keeper”, proporciona una serie de directrices aplicables a la fase de registro informático y las subsiguientes actividades de la persona concernida con una información personal, los responsables de un fichero o banco de datos y los derechos y deberes derivados del almacenamiento y registro de datos para unos u otros.

Estas son: 1. El responsable de la posesión o administración de ficheros o bancos de datos que contienen información personal registrada, tomará las medidas necesarias y legales para

permitirle a cualquier persona determinar, lo siguiente: a) Si el responsable de la posesión o administración de los ficheros o banco de datos, tiene en sus archivos información personal, b) Si esa información personal registrada le concierne a una determinada o determinable persona, c) Si el responsable de la posesión y administración de los ficheros o banco de datos contiene información personal, con la cual: i) se reputa de su naturaleza, ii) se determine los propósitos principales para los cuales se utiliza la información; y, iii) se pueda acceder a la información personal registrada. 2. El responsable de los ficheros o banco de datos que no haya sido registrada bajo los pasos del numeral anterior, podrá negarse a dar acceso a la información contenida en éstos, de conformidad con las leyes estatales especiales que rigen en la materia para los documentos.

Ahora bien, una vez se ha registrado los datos o informaciones de carácter personal, conforme al ordenamiento jurídico vigente por las autoridades competentes se produce una sub-fase que va ligada al registro, aunque puede identificarse desde el punto de vista jurídico e incluso técnico. Jurídicamente conservar un dato o información personal significa mantenerla en las condiciones de forma y tiempo, fines, propósitos y naturaleza para las cuales fue recolectada, almacenada y registrada por las personas naturales o jurídicas, públicas o privadas, según el ordenamiento jurídico vigente. Tecnológicamente, conservar un dato o información personal es mantener en y con medios electromagnéticos en condiciones de forma y tiempo óptimas que permitan *en o a posteriori* el acceso, uso, utilización y transferencia legítimas por quienes están autorizados por la ley o mandato judicial para esto.

El Convenio de Estrasburgo de 1981, al hacer referencia a un grupo de principios que deben observar los datos de carácter personal que sean objeto de un tratamiento automatizado, bajo el epígrafe de "calidad de los datos"; entre otros, principios, expone el principio y a la vez característica de los datos sometidos a procedimientos informáticos, cual es la conservación de los mismos tanto jurídica como técnicamente. En efecto, expresa que "se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado" (Artículo 5, (e),).

En el ámbito ibérico, la conservación de la información o datos, desde el punto de vista tecnológico, por lo menos en el sector público, esta guiada por las directrices expuestas en el R.D. Núm. 263 de 1996, Febrero 16, que regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado. En lo pertinente sostiene: Cuando se utilicen los soportes, medios y aplicaciones referidos en el apartado anterior, se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. Dichas medidas de seguridad deberán tener en cuenta el estado de la tecnología y ser proporcionadas a la naturaleza de los datos y de los tratamientos y a los riesgos a los que estén expuestos. Las medidas de seguridad aplicadas a los soportes, medios y aplicaciones utilizados por los órganos de la Administración General del Estado y sus entidades de derecho público vinculadas o dependientes deberán garantizar: a) La restricción de su utilización y del acceso a los datos e informaciones en ellos contenidos a las personas autorizadas. b) La prevención de alteraciones o pérdidas de los datos e informaciones (Artículo 4-2 y 4-3).

Jurídicamente, en el derecho español, la conservación de los datos personales sujetos a procedimiento informatizado, está prevista en varias normas de la LORTAD, pero por sobre todo, bajo la calidad y forma de principios que rigen la protección y seguridad de los datos personales.

En la Exposición de Motivos de la LORTAD, se plasma como columna vertebral:

Las garantías de la persona son los nutrientes nucleares de la parte general, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios genéricos. Son, en efecto, los derechos de autodeterminación, de

amparo, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general, principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático (considerando 3).

Souviron ^[101], ubica dentro de la calidad y veracidad de los datos, el almacenamiento y conservación de los datos personales. Al referirse a éste último, expresa que los datos “deberán ser conservados durante los plazos previstos en las disposiciones aplicables, o en caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el afectado (artículo 15.5 LORTAD), y ello en los términos ya expuestos respecto a su conservación y cancelación, serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado. Consecuentemente, si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos por los correspondientes datos rectificadas o completados de oficio o a instancia de los afectados (Artículo 4.3. y 4 y 15)”, [Léase titular de los datos en lugar de “afectado”, por las suficientes razones anteriormente suministradas al efecto].

La conservación de los datos personales en el marco de la LORTAD, además de principio característico de los procedimientos informatizados, constituye un tipo de infracción de carácter “leve”, cuando es inobservado por los responsables de los ficheros. En tal virtud, “no conservar actualizados los datos de carácter personal que se mantengan en ficheros” informatizados, constituye una infracción leve investigada y sancionada por las autoridades competentes de protección y seguridad de los datos personales en el derecho español (Artículo 43, (c), y 45).

En la Directiva 95/46/CE, siguiendo los pasos del Convenio Europeo de 1981 y la LORTAD, bajo el epígrafe de los “principios relativos a la calidad de los datos”, expresa que los Estados miembros dispondrán que los datos personales sean: “conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos” (Artículo 6, (e)).

En la *Privacy and data Protection Bill 1994 (NSW) Australiana* ^[102], al referirse al principio 5 del artículo 21 *in fine*, sobre la *information relating to records kept by record-keeper*, hace mención a la conservación de los datos personales registrados, al sostener: 3. El responsable de un fichero o banco de datos personales registrado deberá conservarlo: a) porque la naturaleza de información personal así lo requiere; b) porque constituyen fuentes de información personal, c) porque contiene unos propósitos definidos desde la recolección de la misma por la autoridad correspondiente, d) porque cada información guarda relación con los propósitos generales del fichero, e) porque se individualiza la información personal guardada, f) porque se determina el período para cada tipo de información registrada, g) porque se identifica plenamente a las personas titulares del derecho de acceso a la información contenida en los ficheros, así como las circunstancias o requisitos exigidos para éste; y, h) porque determina los trámites o secuencias seguidas para ejercer el derecho de acceso a la información personal. 4. El Responsable de un fichero o banco de datos, esta obligado: a) mantener esta información personal registrada, según el numeral anterior, disponible para la inspección de las autoridades competentes, y b) Informar en el mes de junio de cada año, al Comisionado para la protección a la intimidad, así como enviar una copia del registro de la información personal que las autoridades competentes están autorizadas a conservarla.

(65) Nuestro trabajo. **LAS MEDIDAS CAUTELARES EN EL PROCEDIMIENTO ADMINISTRATIVO**. Universidad de Navarra (España), Junio 20 de 1986, pág. 456. En: <http://akane.udenar.edu.co/derechopublico>

(66) "Tratamiento automatizado" se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión." (Art. 2, (c), Convenio Europeo de 1981.

- (67) “*Tratamiento de datos personales* (‘tratamiento’) : cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicados a los datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción”. (Art. 2, (b),) . Directiva Comunitaria Europea 95/46/CE.
- (68) **LOPEZ MUÑIZ-GOÑI, Manuel. *INFORMATICA JURIDICA...*** Ob. ut supra cit., pág. 71.
- (69) En otro de nuestros trabajos hemos comentado los sistemas que el profesor López Muñoz-Goñi, clasifica de la siguiente manera: **EL SISTEMA DE DESCRIPTORES** (Thesaurus jurídico). Toma como fundamento las palabras claves o “descriptores” que se utilizan para analizar un documento o una unidad informática siguiendo una serie de pautas lingüísticas, metodológicas e incluso cronológicas y de orden. Este sistema tiene un trabajo humano previo en su realización que no se puede considerar propiamente informático, sino manual, analítico, subjetivo, y muchas veces imperfecto. Por estas razones previas de elaboración, es por lo que el sistema tiene ventajas y desventajas. López Muñoz-Goñi, señala; entre otras: Como ventaja principal, la precisión en la búsqueda de la información requerida al trabajar con un número limitado de palabras claves. El inconveniente o desventaja, es la exigencia a la persona o analista de un trabajo concienzudo e intelectual bastante especializado, según el área del saber humano que se trabaje. Los thesaurus se clasifican así: 1. Según su estructura en: a) estructura arbórea horizontal, b) estructura arbórea vertical; 2. Por el idioma: a) Monolingüe, y b) Multilingüe; 3. Por su contenido: a) Monodisciplinares, b) Interdisciplinares; 4. Por la utilización Informatizada: a) Alfabético, b) numéricos; 5. Por la estructura lingüística: a) De descriptores, y b) Semánticos; 6. Por la forma: a) circulares, y b) Matriciales. **SISTEMA DE TEXTO COMPLETO O “FULL TEXT”**. El sistema de texto integral o literal sirve para ingresar o recuperar información, en la misma forma y contenidos al de su incorporación o extracción. La salida de información se diferencia a la entrada no solo en el tiempo de acción por parte del analista o especialista o del usuario- consultor, según el caso, sino en la accesión a la información por las diferentes unidades periféricas computacionales de software o hardware utilizadas. En efecto las unidades (E/S) pueden ser: teclado, monitor, impresoras, mouse, etc. La información puede recuperarse también desde unidades de memoria central de un ordenador conectado *on line e incluso off line*, siempre que se disponga de los medios electrónicos o telemáticos idóneos. **SISTEMA DE RESUMENES O “ABSTRACTS”**. Es aquél que combina las ventajas de los sistemas anteriores al realizar un sistema informático organizado por resúmenes enriquecidos de información que no suelen pasar de diez a quince renglones sobre los distintos textos analizados. A la vez utiliza un sistema de descriptores para poder ingresar y extraer información más rápidamente para el usuario. A pesar de unir ventajas sigue teniendo desventajas como la subjetividad de los analistas y un margen de error más grande que el del texto completo al realizar resúmenes de textos no elaborados por ellos. Este sistema se utiliza mucho en materiales jurisprudenciales en todo el mundo. En la obra del autor citado y en nuestro trabajo un análisis más completo al respecto. **LA CONSTITUCION DE 1991 Y LA INFORMATICA...** Ob. ut supra cit., pág. 73 y ss. En: <http://akane.udenar.edu.co/derechopublico>
- (70) **LOPEZ MUÑIZ-GOÑI, M.**, Ob. cit ut supra., pág. 39 y ss.
- (71) **MORALES PRATS, Fermín. *LA TUTELA PENAL DE LA INTIMIDAD...*** Ob. cit., pág. 65 y ss.
- (72) *Ibidem*, pág. 70 y ss.
- (73) *Ibidem*, pág. 70 y ss.
- (74) **ORTI VALLEJO, Antonio. *DERECHO A LA INTIMIDAD E INFORMÁTICA***. Ed. Comares, Peligros (Granada), Esp., 1994, pág.71.
- (75) **LOPEZ DIAZ, Elvira. *EL DERECHO AL HONOR Y EL DERECHO A LA INTIMIDAD***. -- Jurisprudencia y doctrina-- . Ed. Dykinson, Madrid (Esp.), 1996, pág.169 y ss.
- (76) **DAVARA R. Miguel A., *MANUAL DE DERECHO INFORMATICO***. Ed. Aranzadi S.A., Pamplona, 1997, pág. 33
- (77) **SOUVIRON, J.M. *EN TORNO A LA JURISDICCION DEL PODER INFORMATICO DEL ESTADO Y EL CONTROL DE DATOS POR LA ADMINISTRACION***. En: Revista Vasca de Administración Pública. R.V.A.P. No. 40, Ed Araila, Arendua, Sep-Dic., 1994, pág. 34.
- (78) Texto completo en: **AA.VV. *DISCOS COMPACTOS ARANZADI...*** Ed. Aranzadi, 1998.
- (79) Texto completo en: WWW.UMONTREAL.EDU.CA.
- (80) **MORALES PRATS, Fermín. *LA TUTELA...*** Ob. cit. pág. 67-68.

- (81) **NORTON, Peter.** *EL IBM PC A FONDO*. Técnicas de programación avanzada (“ Inseide The IBM: Acces to avanced features and programming). Trad: José Antonio Daza. Ed. Anaya, Madrid, 1987, pág. 29 y ss.
- (82) *Ibidem*, pág. 29 y ss.
- (83) **FAIREN GUILLEN, Víctor.** *EL HABEAS DATA Y SU PROTECCION ACTUAL SURGIDA EN LA LEY ESPAÑOLA DE INFORMATICA DE 29 DE OCTUBRE DE 1992*. En: Revista de Derecho Procesal. Editoriales de Derecho Reunidas, S.A., Madrid, 1996, pág. 529
- (84) **MORALES P., Fermín.** *LA TUTELA PENAL DE LA INTIMIDAD....* Ob. ut supra cit., pág. 67-68.
- (85) **RIASCOS GOMEZ, L.O.** *LA CONSTITUCION DE 1991 y ...* Ob. cit., pág. 112 y ss. En: <http://akane.udenar.edu.co/derechopublico>
- (86) **AA.VV. DISCOS COMPACTOS ARANZADI. REAL DECRETO 16-2-1996, núm. 263/1996. PUBLICACIONES:** BOE 29-2-1996, núm. 52, [pág. 7942] Regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado. *Artículo 2. Derechos de los ciudadanos y limitaciones.* 1. La utilización de las técnicas señaladas en el artículo anterior tendrá las limitaciones establecidas por la Constitución, la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y el resto del ordenamiento jurídico, respetando el pleno ejercicio por los ciudadanos de los derechos que tienen reconocidos. En especial, se garantizará el honor y la intimidad personal y familiar de los ciudadanos ajustándose, a tal efecto, a lo dispuesto en la Ley Orgánica 5/1992, de Regulación del tratamiento automatizado de los datos de carácter personal, y en las demás Leyes específicas que regulan el tratamiento de la información así como en sus correspondientes normas de desarrollo. La utilización de tales técnicas en ningún caso podrá implicar la existencia de restricciones o discriminaciones de cualquier naturaleza en el acceso de los ciudadanos a la prestación de servicios públicos o a cualquier actuación o procedimiento administrativo. 2. Cuando la Administración General del Estado o las entidades de derecho público vinculadas o dependientes de aquélla utilicen técnicas electrónicas, informáticas y telemáticas en actuaciones o procedimientos que afecten de forma directa o indirecta a derechos o intereses de los ciudadanos, se garantizará la identificación y el ejercicio de la competencia por el órgano correspondiente. En este supuesto, los ciudadanos tendrán derecho a obtener información que permita la identificación de los medios y aplicaciones utilizadas, así como del órgano que ejerce la competencia.
- (87) Texto completo en: **AA.VV. DISCOS COMPACTOS ARANZADI S.A.**
- (88) “*Artículo 5. Derecho de información en la recogida de datos.* 1. Los afectados (por titulares de datos) a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación. e) De la identidad y dirección del responsable del fichero. 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.3. No será necesaria la información a que se refiere el apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban”. Texto completo en: **AA.VV. DISCOS COMPACTOS ARANZADI S.A.**
- (89) Agrega la E.de M., que “La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado (por titular de los datos), y los segundos sólo serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencia de la propia Ley Orgánica, ha de fundarse en razones de interés general; en todo caso, se establece la prohibición de los ficheros creados con la exclusiva finalidad de almacenar datos personales que expresen las mencionadas características. En este punto, y de acuerdo con lo dispuesto en el artículo 10 de la Constitución, se atienden las exigencias y previsiones que para estos datos se contienen en el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, de 1981, ratificado por España”. Texto completo en: **AA.VV. DISCOS COMPACTOS ARANZADI S.A.**
- (90) **ORTI VALLEJO, Antonio.** *DERECHO A LA INTIMIDAD E INFORMATICA...* Ob. cit., pág. 136 y ss. Los autores allí citados. v.gr. Albadalejo, Diez Picaso, entre otros.
- (91) En estos casos, no será aplicable porque “la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos

por la ley. En tales casos, los Estados miembros establecerán las garantías apropiadas” (art. 11-2, Directiva).

- (92) Texto completo en: WWW.UMONTREAL.EDU.CA.
- (93) La Agencia de Protección de los Datos. “El art. 6.5 LGP quedará en la historia de derecho público como ejemplo de lo arriesgado que resulta el poner en manos de los adoradores del Poder preceptos tipo ‘cajón de sastre’. No es el momento de estudiar este precepto. Recuérdese, sin embargo, que dicha ley va agrupando sucesivamente las distintas organizaciones que integran el sector público en organismos autónomos (de carácter administrativo y de carácter comercial, industrial, financiero y análogos) (art. 4.1), Seguridad social (art. 5), sociedades estatales (con participación estatal mayoritaria y entidades de derecho público) (art. 6.1), y “el resto del sector público” (art. 6.5). Esta última frase ha permitido abrir un portillo por el que una serie de organizaciones a las que se conoce ya en la doctrina con el calificativo de organizaciones independientes (tomado, ciertamente, de la terminología que utiliza la norma de creación correspondiente a cada una de ellas) han empezado a buscar el camino de la ‘libertad’ (entiéndase: de la reducción al máximo de cualquier forma de control). Ello ha dado lugar a un problema de enorme gravedad sobre el que ya ha dado la voz de alerta por algunos autores (v.gr. Silvia del Saz). **GONZALEZ NAVARRO, F y GONZALEZ PEREZ, J. COMENTARIOS A LA LEY DE REGIMEN JURIDICO DE LA ADMINISTRACION PUBLICA Y PROCEDIMIENTO ADMINISTRATIVO COMUN.** 1a. ed., Ed. Civitas, S.A., Madrid, 1997, pág. 705.
- (94) A los efectos de este trabajo “Registro informático”, es aquél derivado del análisis de la terminología utilizada por la LORTAD y las normas comunitarias que regulan el tratamiento informatizado de datos. En efecto, La LORTAD, al definir “tratamiento de datos” hace alusión a las operaciones y procedimientos técnicos, de carácter “automatizado” que permitan la “recogida, grabación, ...” (Art.3, c.); en tanto que la Directiva 95/46/CE, utiliza el término “registro” para conceptualizar esa misma parte del tratamiento informatizado de datos (art. 2, b), con lo cual registro informático tiene una doble construcción: una parte tecnológica fundada en la grabación de datos o informaciones con soportes y medios informáticos, electrónicos o telemáticos; y una parte, jurídica, la del registro como actividad jurídico-administrativa
- (95) .
- (96) Cfr. Inscripción y certificaciones.1. Corresponde al Registro General de Protección de Datos instruir los expedientes de inscripción de los ficheros automatizados de titularidad privada y pública. 2. Corresponde asimismo al Registro General de Protección de Datos: a) Instruir los expedientes de modificación y cancelación del contenido de los asientos. b) Instruir los expedientes de autorización de las transferencias internacionales de datos.c) Rectificar de oficio los errores materiales de los asientos. d) Expedir certificaciones de los asientos. e) Publicar una relación anual de los ficheros notificados e inscritos (Art. 26. R.D. Núm. 428/1993, Marzo 26. R.D). en: AA.VV. **DISCOS COMPACTOS ARANZADI.** Ed. Aranzadi, S.A. Madrid, 1998.
- (97) Cfr. *Ficheros de las Administraciones Públicas*. Serán objeto de inscripción en el Registro los ficheros automatizados que contengan datos personales y de los cuales sean titulares: a) La Administración General del Estado, b) Las entidades y organismos de la Seguridad Social, c) Los organismos autónomos del Estado, cualquiera que sea su clasificación, d) Las sociedades estatales y entes del sector público a que se refiere el artículo 6 de la Ley General Presupuestaria, e) Las Administraciones de las Comunidades Autónomas y de sus Territorios Históricos, así como sus entes y organismos dependientes, sin perjuicio de que se inscriban además en los registros a que se refiere el artículo 40.2 de la Ley Orgánica 5/1992, f) Las entidades que integran la Administración Local y los entes y organismos dependientes de la misma (Art. 24-1. R.D. Núm. 428/1993, Marzo 26). Texto completo en: **AA.VV. DISCOS COMPACTOS ARANZADI.** Ed. Aranzadi, 1998.
- (98) Cfr. *Los ficheros de titularidad pública*. Art. 18-2. Las disposiciones de creación o de modificación de los ficheros deberán indicar: a) La finalidad del fichero y los usos previstos para el mismo, b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos, c) El procedimiento de recogida de los datos de carácter personal, d) La estructura básica del fichero automatizado y la descripción de los tipos de datos de carácter personal incluidos en el mismo, e) Las cesiones de datos de carácter personal que, en su caso, se prevean, f) Los órganos de la Administración responsables del fichero automatizado, y, g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación y cancelación. Texto completo en: **AA.VV. DISCOS COMPACTOS ARANZADI.** Ed. Aranzadi, 1998.
- (99) Cfr. *Códigos tipo*.1. Mediante acuerdos sectoriales o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equi-pos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con

pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación. En el supuesto de que tales reglas o estándares no se incorporaran directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél. 2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos, que podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas. (Art. 31, LORTAD). Texto completo en: **AA.VV. DISCOS COMPACTOS.... Ed. Aranzadi, 1998.**

- (99) En efecto, “a título de ejemplo (se) relaciona los datos de carácter personal y los ficheros o banco de datos que los contienen que no son objeto de la LORTAD, y por tanto, no son inscribibles en el Registro mencionado. Sostiene, quedan por fuera “los datos anónimos, que constituyen información de dominio público o recogen información, con la finalidad, precisamente, de darla a conocer al público en general -- como pueden ser los registros de la propiedad o mercantiles--, así como, por último, los de uso estrictamente personal. De otro lado, parece conveniente la permanencia de las regulaciones especiales que contienen ya suficientes normas de protección y que se refieren a ámbitos que revisten tal singularidad en cuanto a sus funciones y sus mecanismos de puesta al día y rectificación que aconsejan el mantenimiento de su régimen específico. Así ocurre, por ejemplo, con las regulaciones de los ficheros electorales, del Registro Civil o del Registro Central de Penados y Rebeldes; así acontece, también, con los ficheros regulados por la Ley 12/1989, de 9 de mayo (RCL 1989\1051 y RCL 1990\1573), sobre función estadística pública, si bien que, en este último caso, con sujeción a la Agencia de Protección de Datos. En fin, quedan también fuera del ámbito de la norma aquellos datos que, en virtud de intereses público prevalentes, no deben estar sometidos a su régimen cautelar”. Texto completo en: **AA.VV. DISCOS ARANZADI. Ed. , 1998.**

(100) *Texto completo, En: www.umontreal.edu.ca*

(101) *SOUVIRON, J.M. En torno a la jurisdicción del poder... Ob . cit., p. 152*

(102) *Texto completo, En: www.umontreal.edu.ca*

Actualización: Pasto, Abril 1 de 2008

INICIO

--