APLICACIÓN DE LA LOPD A LOS FICHEROS MANUALES

M.ª PILAR MORALES MORALES
Diplomada en Gestión Protección de Datos
Técnico Ayuntamiento Valdemoro

TRATAMIENTO DE DATOS PERSONALES

La Audiencia Nacional, en su Sentencia de fecha 16 de febrero de 2006, considera que para abordar el concepto de "tratamiento de datos personales" y el de "fichero" desde la perspectiva legal hemos de partir de la Directiva 95/46, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Directiva de la que nuestra actual ley es tributaria en gran medida.

Esta Directiva nos dice, en primer lugar, que el concepto de "tratamiento" no puede depender de la técnica utilizada para el manejo de los datos, de ahí que incluya tanto el tratamiento automatizado como el manual (considerando 27 de su Preámbulo). Así, lo relevante para que estemos ante un "tratamiento de datos personales" es la realización de determinadas actuaciones en relación con los mismos, actuaciones que en su descripción son muy amplias y variadas.

Desarrollando este principio el artículo 2 de la Directiva describe las actuaciones que aplicadas a los datos personales constituyen "tratamiento": "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a 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".

Nuestra ley lo define de forma muy similar en el arto 3.c) de la Ley Orgánica 15/1999.

"c) 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." No basta, sin embargo, la realización de una de estas actuaciones en relación con datos personales para que la ley despliegue sus efectos protectores y sus garantías y derechos del afectado. Es preciso algo más: que las actuaciones de recogida, grabación, conservación etc., se realicen de forma automatizada o bien, si se realizan de forma manual, que los datos personales estén contenidos o destinados a un fichero.

Para que una actuación manual sobre datos personales (recogida, grabación, conservación, elaboración, modificación, bloqueo...) tenga la consideración de "tratamiento de datos personales" sujeto al sistema de protección de la Ley Orgánica 15/1999 es -necesario que dichos datos estén contenidos o destinados a ser incluidos en un fichero, esto es, en un conjunto estructurado u organizado de datos con arreglo a criterios determinados. Si no es así, el tratamiento manual de datos personales quedará fuera del ámbito de aplicación de la ley, no será un "'tratamiento de datos personales" según el concepto normativo que la ley proporciona.

¿Qué es un fichero no automatizado?

Fichero no automatizado: ***"todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica".***

Dentro de este concepto están incluidos los ficheros de datos personales que almacenan la información en documentos en formato papel o cualquier tipo de soporte a través del cual se puedan gestionar manualmente a través de carpetas, archivadores o contenedores, siempre que dichos criterios permitan acceder sin esfuerzos al contenido de la información.

El mejor ejemplo de un fichero no automatizado los tenemos en los archivadores existentes en la mayoría de las organizaciones en los que se almacenan expedientes de documentos organizados por personas físicas (empleados, clientes, proveedores, etc. En empresas privadas; en empresas públicas podemos mencionar los expedientes de servicios sociales y en los cuerpos y fuerzas de seguridad del estado ficheros de identificación genética) y se estructuran de manera que se puede localizar cada expediente utilizando criterios relativos a personas físicas (búsqueda alfabética por nombres o apellidos, por ejemplo).

Con la entrada en vigor del Real Decreto 1720/2007, por el que se aprueba el desarrollo la LOPD, el tratamiento de datos de carácter personal en los ficheros no automatizados, cobra especial interés, ya que la Ley 15/1999 no lo recogía con claridad.

Cabe hacer mención especial a la aplicación de las medidas de seguridad de estos ficheros o tratamientos a la hora de elaborar los correspondientes documentos de seguridad porque al crear y notificar un fichero que contiene datos de carácter personal, deberá tener implantadas, desde el momento de la creación, la totalidad de las medidas de seguridad reguladas en el mismo.

Obligaciones que se derivan de la LOPD: siempre que se respeten las garantías que la propia Ley establece para proteger la intimidad y los derechos de las personas físicas.

Antes de profundizar en los tratamientos o ficheros no automatizados, debemos tener muy en cuenta y de manera general las garantías que establece la Ley y que a rasgos generales son las siguientes:

1. IDENTIFICACIÓN E INVENTARIADO DE FICHEROS

Antes de iniciar el proceso de notificación e inscripción de los ficheros o tratamientos de datos de carácter personal, hay que hacer un estudio de los ficheros que se pretenden crear

para el buen funcionamiento de la organización y/o de los existentes para proceder a la inscripción de los mismos.

2. NOTIFICACIÓN E INSCRIPCIÓN DE LOS FICHEROS

El responsable del fichero deberá notificar a la Agencia Española de Protección de Datos (en adelante AGPD), o a las Agencias de las Comunidades Autónomas que tengan delegación a tal efecto, aquellos ficheros de carácter personal que vaya a utilizar en su organización con la finalidad de que éstos sean inscritos en el Registro General de Protección de Datos.

¿Qué es la notificación e inscripción de ficheros?

Es el procedimiento a través del cual se informa a la AGPD de la existencia de un fichero de datos de carácter personal para que, una vez comprobado que cumple con los requisitos legalmente establecidos, se acuerde su inscripción en el Registro General de Protección de Datos.

¿Qué es el Registro General de Protección de Datos?

Es un órgano integrado en la AGPD, al que corresponde velar por la publicidad de los tratamientos y ficheros de datos personales existentes con la finalidad de facilitar al ciudadano el ejercicio de sus derechos. Los responsables de los ficheros tienen la obligación legal de inscribir en el Registro todos los ficheros de datos personales que posean en su organización para que cuando el ciudadano realice una consulta al registro pueda localizar la información que necesita para ejercer sus derechos.

¿Quién debe notificar los ficheros?

A la hora de determinar quién debe notificar la creación de un fichero y cuál es el momento para hacerlo, hemos de diferenciar entre ficheros de titularidad pública y ficheros de titularidad privada, debido a que la forma de crearlos es diferente en cada caso; mientras que los ficheros de titularidad privada se crean a partir de una simple decisión, los ficheros de titularidad pública se crean a partir de una norma o acuerdo de creación que debe ser publicado en el Diario Oficial que corresponda.

- *Ficheros de titularidad pública.* Serán notificados por el Órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de 30 días desde la publicación de su norma o acuerdo de creación en el Diario Oficial correspondiente.
- *Ficheros de titularidad privada.* Serán notificados por la persona o entidad privada que pretenda crearlos antes de crear el fichero y comenzar el tratamiento de los datos personales.

¿Cómo se notifica un fichero?

Todo lo relacionado con el procedimiento de notificación e inscripción de ficheros, se encuentra regulado en el **Título V** y en el **Título IX** (capítulo V) del **Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de la LOPD.** Teniendo en cuenta lo dispuesto en dicho reglamento, podemos resumir el procedimiento de notificación e inscripción de ficheros de la siguiente manera:

Ficheros de titularidad Privada:

- *Notificación del fichero.* Se realiza cumplimentado el formulario gratuito que la AGPD facilita a través de su página web y que deberán remitirse una vez cumplimentados a la Agencia a través de cualquier vía legalmente permitidas (Internet o soporte papel).
- *Resolución de inscripción del fichero.* Si la notificación contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el director de la AGPD acordará la inscripción del fichero asignándole un código de inscripción.
- *Resolución denegatoria de la inscripción.* En el supuesto de que de los documentos aportados por el responsable se desprenda que la notificación no resulta conforme a lo dispuesto en la LOPD, el director de la AGPD dictará resolución denegando la inscripción.

– *Plazo para resolver.* El plazo máximo de que dispone la AGPD para dictar y notificar una resolución acerca de la inscripción será de un mes. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito a todos los efectos.
– *Obligación de mantener actualizada la inscripción.* Una vez inscrito el fichero, el responsable del mismo deberá mantenerlo actualizado, comunicando a la AGPD la cancelación o supresión del fichero, así como los cambios que se produzcan en la finalidad del fichero, en su responsable y en la dirección de su ubicación.

Fichero de titularidad Pública:

– *Identificar e inventariar los ficheros y tratamientos* en los que se almacenen o utilicen datos de carácter personal y que deben ser objeto de declaración.
– *Rellenar los impresos para la notificación* al Registro de Ficheros de Datos personales de la AGPD o de las correspondientes Agencias Autonómicas.
– *Elaborar el proyecto de disposición de carácter general* de regulación de los ficheros (Ordenanza, Decreto, etc.).
– Someter el proyecto de disposición a *trámite de alegaciones.*
– *Solicitar informe preceptivo* a la AGPD o las Agencias Autonómicas.
– *Aprobar la nueva disposición general* por el órgano competente (Pleno de Ayuntamiento, junta de Gobierno…).
– *Remitir la disposición aprobada* (ordenanza o acuerdo) al Boletín Oficial que corresponda, para su publicación.
– *Solicitar la inscripción en el registro de ficheros de datos personales* de las correspondientes agencias del fichero, mediante solicitud dirigida a éstas, acompañando copia de la publicación en el Boletín Oficial correspondiente, en el plazo de 15 días desde su publicación.

Es importante destacar que la inscripción de un fichero en el Registro, únicamente acredita que se ha cumplido con la obligación dispuesta en el artículo 26 de la LOPD, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en la Ley y demás disposiciones reglamentarias.

¿Qué información se debe aportar?

Para cumplimentar el formulario gratuito que la AGPD facilita, va a ser necesario aportar la siguiente documentación:

- La identificación del responsable del fichero.
- La identificación del fichero, sus finalidades y los usos previstos.
- El colectivo de personas sobre el que se obtienen los datos.
- El procedimiento y procedencia de los datos.
- Las categorías de los datos.
- El servicio o unidad de acceso.
- La identificación del nivel de medidas de seguridad básico, medio o alto exigible.
- La identificación del encargado del tratamiento en donde se encuentre ubicado el fichero.
- Los destinatarios de cesiones y transferencias internacionales de datos.

En el caso de ficheros de titularidad pública, igualmente las Agencias Autonómicas disponen de formularios gratuitos desde los que aportar la documentación requerida, que es la relacionada anteriormente.

3. RECOGER Y TRATAR LOS DATOS DE CARÁCTER PERSONAL APLICANDO LOS PRINCIPIOS DE LA PROTECCIÓN DE DATOS.

El responsable del fichero debe recoger, tratar y ceder los datos de carácter personal, aplicando todos y cada uno de los principios de la protección de datos, es decir:

La calidad de los datos.
El deber de información en la recogida de datos.
El consentimiento del afectado.
Los datos especialmente protegidos.
La seguridad en los datos.
El deber de secreto.
La comunicación de datos y Acceso a los datos por cuenta de terceros.

A. Principios de calidad de los datos:

¿Qué es el principio de calidad de los datos?

La calidad de los datos es uno de los nueve principios a través de los cuales el Título II de la Ley orgánica 15/1999 establece las condiciones en que se deben recoger, tratar y ceder los datos de carácter personal para salvaguardar la intimidad y demás derechos fundamentales de los ciudadanos.

A través de este principio la Ley establece un conjunto de reglas que indican al responsable del fichero como debe recoger, almacenar y utilizar los datos de carácter personal para que el tratamiento de los datos pueda ser considerado "leal y lícito". A través de dichas reglas, el artículo 4 de la LOPD establece como se deben recoger los datos, qué datos se pueden recoger, cómo se deben utilizar, cómo deben mantenerse actualizados, cómo deben ser almacenados y cuál es el procedimiento para cancelarlos y eliminarlos definitivamente de los ficheros.

- *Regulación legal:* El principio de calidad de los datos se encuentra regulado en el artículo 4 de la LOPD y en los artículos 8 al 11 del Reglamento que la desarrolla, el Real Decreto 1720/2007.
- *Contenido del principio de calidad de los datos:* Como ya hemos adelantado, para cumplir con el principio de calidad de los datos, el responsable del fichero debe recoger y tratar los datos de carácter personal aplicando todas y cada una de las reglas contenidas en el artículo 4de la LOPD, dichas reglas son las siguientes:
- *Forma de obtener los datos:* El principio de la calidad de los datos obliga al responsable del fichero a recoger los datos de carácter personal con total transparencia para el ciudadano, sin utilizar medios fraudulentos, desleales o ilícitos.
- *Finalidad del tratamiento:* El principio de calidad de los datos impide que el responsable del fichero pueda recoger los datos de carácter personal de los ciudadanos para hacer con ellos lo que le parezca, los datos deben recogerse con una finalidad determinada, explícita y legítima que motiva su recogida.
- *Proporcionalidad de los datos:* El principio de calidad de los datos, impide que el responsable del fichero recoja cuantos datos de carácter personal le venga en gana, estableciendo que sólo se recogerán para su tratamiento aquellos datos que sean adecuados, pertinentes y no excesivos en relación a la finalidad determinada, explícita y legítima que motiva su recogida.
- *Uso de los datos:* El principio de la calidad de los datos establece que los datos de carácter personal no podrán utilizarse para finalidades incompatibles con aquéllas para las que hubieran sido recogidos.
- *Exactitud de los datos:* El principio de calidad de los datos impone al responsable del fichero la obligación de mantener los datos de carácter personal actualizados y puestos al día de manera que reflejen la situación de su titular.
- *Cancelación de los datos:* El principio de calidad de los datos establece que los datos de carácter personal no serán conservados en los ficheros en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines, en base a los cuales hubieran sido recabados o registrados. Sin embargo, una vez finalizado el motivo por el cual se recogieron los datos, éstos no serán eliminados directamente del fichero, sino que se mantendrán **"bloqueados"** de manera que solo puedan acceder a ellos las administraciones públicas, los jueces o los tribunales para gestionar las posibles responsabilidades nacidas durante el tratamiento de los datos.

Una vez finalizados los plazos de prescripción de dichas responsabilidades, los datos de carácter personal serán eliminados definitivamente de los ficheros.

– *Almacenamiento de los datos:* El principio de la calidad de los datos establece que éstos deben ser almacenados de manera que su titular pueda ejercer el derecho de acceso y pueda conocer en cualquier momento qué datos suyos están sometidos a tratamiento y cual es el uso que se está dando a dichos datos. Esto supone que el responsable del fichero debe esta-

blecer un procedimiento de almacenamiento que permita acceder a los datos sin complicaciones y permita ejercitar el derecho de acceso en el plazo de un mes desde la recepción de la solicitud del interesado.

- *Infracciones y sanciones aplicables al principio de la calidad de los datos:* El responsable del fichero debe tener en cuenta que recoger, tratar y ceder datos de carácter personal vulnerando los principios y garantías establecidos en la LOPD, puede ser constitutivo de infracción leve, grave o muy grave según sea el caso de que se trate, pudiendo ser sancionado por la Agencia Española de Protección de Datos con multas de hasta 600.000 € por la infracción más grave. En relación al principio de calidad de los datos destacamos las siguientes infracciones:

En cuanto a la forma de obtener los datos: el artículo 44.4.a de la LOPD considera que *"la recogida de datos de forma engañosa y fraudulenta"* constituye una infracción muy grave sancionable con multas desde 300.001 hasta 600.000 €

En cuanto a la finalidad del tratamiento: el artículo 44.3.c de la LOPD considera que "Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave", constituye una infracción de carácter grave, sancionable con multas de 40.001 a 300.000 €

En cuanto a la exactitud y cancelación de los datos, así como su almacenamiento: el artículo 44.3.e de la LOPD considera que "El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición", constituye una infracción de carácter grave sancionable con multas de 40.001 a 300.000 €.

B. El deber de información en la recogida de datos. ¿Qué es el derecho de información?

Es uno de los de los nueve principios a través de los cuales, la LOPD establece las condiciones en que se deben recoger, tratar y ceder los datos de carácter personal para salvaguardar la intimidad y demás derechos de los ciudadanos.

A través del derecho de información en la recogida de datos, la LOPD establece a la vez un **derecho para el ciudadano** y un **deber para el responsable del fichero;** por un lado el ciudadano tiene derecho a saber quién recoge sus datos, para qué los recoge, quién va a ser el destinatario de su información, cuáles son los derechos que le asisten y a donde se tiene que dirigir para poder ejercerlos, y por otro lado, el **responsable** del tratamiento tiene la obligación de informarle de ello en los términos regulados en el artículo 5 de la LOPD, el cual establece unas condiciones diferentes en función de si los datos se han obtenido directamente de su titular o si proceden de otras fuentes.

Datos obtenidos de su titular.

Cuando los datos de carácter personal se soliciten directamente a su titular, el responsable del fichero cumplirá con lo establecido en el art. 5.1 de la LOPD, previamente y de manera expresa, precisa e inequívoca en los siguientes extremos:

a) De la existencia de un fichero o tratamiento 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, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Datos NO obtenidos de su titular

Cuando los datos no hayan sido obtenidos del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero, dentro de los tres

meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, según lo preceptuado en el art. 5.4 de la LOPD y de forma expresa de los siguientes extremos:

– Del contenido del tratamiento.
– De la procedencia de los datos.
– De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
– De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y posición.
– De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Prueba del cumplimiento del deber de información

A la hora de demostrar que se ha informado debidamente al titular de los datos, la carga de la prueba recae sobre el responsable del fichero, por lo que el deber de información deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.

C. El consentimiento del afectado

La LOPD define en su art. 3.h, el consentimiento del afectado como *"toda manifestación de voluntad, libre e inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen" y establece como condición general que "el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa"* (art. 6.1).

Por lo tanto, en aplicación de ambos artículos, podemos decir que el responsable del fichero solamente podrá tratar los datos de carácter personal de las personas físicas si se da alguna de las siguientes circunstancias:

– Si dispone del consentimiento del titular de los datos y éste ha sido obtenido adecuadamente.
– Si está amparado por una ley que, de manera excepcional, le autorice a tratar los datos sin necesidad de contar con el consentimiento del afectado.

La revocación del consentimiento.

Una vez prestado el consentimiento, y tal y como establece el art. 6.3 de la LOPD, **el titular de los datos tiene la posibilidad de revocarlo "cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos,** lo que significa que la revocación del consentimiento impedirá que se continúen tratando los datos personales, pero no podrá evitar los efectos que haya tenido el tratamiento hasta el momento de la revocación.

La oposición al tratamiento de los datos.

En aquellos casos en los que una ley permita el tratamiento de los datos sin disponer del consentimiento del afectado, el titular de los datos no tiene la posibilidad de revocar su consentimiento simplemente porque no lo ha prestado, sin embargo, en estos supuestos, el art. 6.4 de la LOPD le **permite oponerse al tratamiento de sus datos "cuando existan motivos fundados y legítimos relativos a una concreta situación personal",** obligando con ello al responsable del fichero a excluir del tratamiento los datos relativos al afectado.

D. Los datos especialmente protegidos

Son conocidos también como "datos sensibles", son una categoría de datos que por su especial influencia en la intimidad, los derechos fundamentales y las libertades públicas del individuo, requieren de una mayor protección que el resto de sus datos personales. Su tratamiento está regulado en el art. 7 de la LOPD y son los siguientes:

– Datos que revelen la ideología, afiliación sindical, religión y creencias.
– Datos que hagan referencia al origen racial, la salud o la vida sexual.
– Datos relativos a la comisión de infracciones penales o administrativas.

E. El deber de secreto

Es uno de los nueve principios a través de los cuales LOPD establece las condiciones en que se deben recoger, tratar y ceder los datos de carácter personal para salvaguardar la intimidad y demás derechos de los ciudadanos. A través de este principio el art. 10 establece que **"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".**

En aplicación del deber de secreto, tanto el responsable del fichero como cualquier otra persona que tenga acceso a un fichero de datos de carácter personal están obligados a guardar secreto profesional sobre los datos contenidos en dicho fichero. Sin embargo **cuando alguien vulnera el deber de secreto y comete alguna de las infracciones previstas en la LOPD, la AGPD va a sancionar por ello únicamente al responsable del fichero y no al autor de la infracción,** sin perjuicio, claro está, de las posibles acciones civiles y penales que posteriormente se puedan emprender contra la persona que no ha respetado su deber de secreto.

Teniendo en cuenta esta circunstancia, el responsable del fichero, no solo debe preocuparse por respetar su propio deber de secreto, sino también debe de que todo el personal a su servicio mantiene la confidencialidad del tratamiento, para lo cual sería recomendable:

– *Informar al personal de su deber de secreto.*

El responsable del fichero deberá asegurarse de que todo el personal a su cargo (tanto personal interno en régimen laboral, como externos y subcontratados), conoce su obligación de guardar secreto respecto de los datos personales a los que tenga acceso, por lo que sería conveniente informarles del contenido del deber de secreto y de las consecuencias de su incumplimiento, a través de algún medio que sirva de prueba en caso de problemas, como por ejemplo a través de cláusulas de confidencialidad en los contratos.

– *Adoptar las medidas necesarias para garantizar la confidencialidad de los datos.*

Hay que tener en cuenta que la persona que vulnere el deber de secreto, además de incurrir en algunas de las infracciones previstas en la LOPD, puede estar cometiendo un delito de descubrimiento y revelación de secretos, regulado en los artículos 197 a 201 del código penal.

F. La comunicación de datos y Acceso a los datos por cuenta de terceros

Hay que diferenciar entre la comunicación de datos y el acceso a los datos por cuenta de terceros:

La comunicación de datos se encuentra regulada en el artículo 11 de la LOPD y se produce cuando el responsable del fichero cede los datos a un tercero para que los trate por su cuenta y bajo su responsabilidad.

El acceso a datos por cuenta de terceros se regula en el artículo 12 de la LOPD y se produce cuando el responsable del fichero contrata a una persona o entidad ajena a su organización para que le preste algún servicio utilizando los datos de carácter personal almacenados en sus ficheros.

Por lo tanto para que una cesión de datos se considere "acceso a datos por cuenta de terceros" y no una "comunicación de datos" se tiene que realizar cumpliendo estrictamente lo dispuesto en el art. 12 de la LOPD.

Cuando se contrata a persona o entidad ajena para la prestación de un servicio en el que tenga que utilizar los datos de carácter personal, se hace necesario la confección de un "Contrato de encargo de tratamiento de datos" cuya forma, contenido y características se encuentran regulados en el art. 12 de la LOPD en los siguientes términos:

– Forma del contrato. Para que el contrato sea válido, deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido.

– Tratamiento de los datos. El encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
– Finalidad del Contrato. En el contrato quedará reflejada la finalidad con la que se deben tratar los datos, y el encargado del tratamiento obligará a no utilizar los datos con otros fines.
– Comunicación de datos. El encargado del tratamiento no comunicará los datos, ni siquiera para su conservación a otras personas.
– Medidas de seguridad. En el contrato se estipularán las medidas de seguridad que el encargado del tratamiento está obligado a implementar.
– Finalización del servicio. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento.
– Consecuencias del incumplimiento del contrato. Si el encargado del tratamiento destina los datos a otra finalidad, los comunica o los utiliza incumpliendo las estipulaciones del contrato, será también considerado responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido.

4. GARANTIZAR LA SEGURIDAD DE LOS DATOS

Antes de analizar este punto debemos diferenciar entre la figura "Responsable" y "Encargado" del tratamiento.

– **Responsable de Fichero:** persona, empresa o entidad responsable de que los datos de carácter personal almacenados en un fichero sean tratados aplicando las garantías que la propia LOPD establece para proteger la intimidad de las personas.

Por lo general, la persona o entidad que en el ejercicio de su actividad decida crear un fichero para tratar los datos de las personas con las que se relaciona (clientes, empleados, proveedores, pacientes, alumnos, etc.) adquiere la condición de responsable del fichero y asume la obligación de tratar los datos aplicando las garantías previstas en la LOPD.

En la definición de responsable se incluye entre otros, a los empresarios autónomos, los profesionales liberales (médicos, abogados, etc.), a las sociedades mercantiles (anónimas, limitadas, etc.), a las sociedades civiles, a las asociaciones y fundaciones sin ánimo de lucro y a los organismos de las administración pública del Estado.

Obligaciones del responsable del fichero: debe poner todos los medios que sean necesarios para que los datos de carácter personal se utilicen aplicando las garantías que la LOPD establece, para garantizar la intimidad y demás derechos fundamentales de los ciudadanos.

– **Encargado del tratamiento (art. 12 de la LOPD y art. 20 a 22 del RD 1720/2007):** Persona o entidad que accede a los datos de carácter personal para prestar algún tipo de servicio al responsable del fichero o tratamiento (contabilidad, nóminas, marketing, hosting, etc.): gestorías contables, asesorías contables, asesoráis laborales, empresas de marketing y en general, a cualquier persona o entidad que preste algún tipo de servicio que implique el tratamiento de datos de carácter personal por cuenta del responsable del fichero.

– **El documento de seguridad.**

La correcta implantación de las medidas de seguridad requiere de la elaboración del documento de seguridad, (art. 88 RD 1720/2007). Dicho documento debe reflejar por escrito todo lo relacionado con las medidas, normas, procedimientos de actuación, reglas y estándares que se deban aplicar para garantizar la seguridad de los datos de carácter personal que sean objeto de tratamiento. Se trata de un documento de carácter interno que *será de obligado cumplimiento para todo aquel que deba tener acceso a los datos de carácter personal.*

El documento de seguridad es un elemento esencial a la hora de aplicar correctamente las

medidas de seguridad, debiendo estar presente en cualquier organización en la que se utilicen datos de carácter personal tanto si el tratamiento de datos se realiza de forma informatizada como a través de **ficheros no automatizados** (gestionados manualmente a través de archivos en formato papel o soportes que permitan su tratamiento).

El documento de seguridad debe ser elaborado por el responsable del fichero y, en su caso, por el encargado del tratamiento. Éste podrá ser único y comprensivo de todos los ficheros o tratamiento, o bien individualizado para cada fichero o tratamiento. También podrá elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado en la organización, o bien atendiendo a criterios organizativos del responsable.

Una vez elaborado el documento de seguridad hay que ponerlo en conocimiento de todo el personal que tenga acceso a los datos de carácter personal, quienes tienen la obligación de tratar los datos cumpliendo con todas y cada una de las normas y procedimientos contenidos en dicho documento.

El contenido mínimo del documento de seguridad:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el reglamento.
- Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Adopción de medidas para el transporte de soportes y documentos, así como medidas para la destrucción de los documentos y soportes.

Además para los niveles medio y alto deberá contener:

- Identificación del responsable de seguridad.
- Controles periódicos que se deben realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

El documento de seguridad deberá mantenerse en todo momento actualizado y se revisará siempre que se produzcan cambios relevantes en la organización.

Los niveles de seguridad. Aspectos a tener en cuenta:

MEDIDAS DE SEGURIDAD

El primer factor considerado, y el más evidente debe ser asegurar el sustrato físico del objeto a proteger. Es preciso establecer un perímetro de seguridad a proteger, y esta protección debe adecuarse a la importancia de lo protegido. La defensa contra agentes nocivos conlleva tanto medidas proactivas (limitar el acceso a la información) como normativas de contingencia (qué hacer en caso de….) o medidas de recuperación. El grado de seguridad solicitado establecerá las necesidades.

Conviene recordar que quien tiene acceso a la información tiene control absoluto de la misma. Por ello, solamente deberían acceder a ella aquellas personas que estrictamente sea necesario.

NIVEL FÍSICO

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra la información.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales como incendios accidentales, tormentas e inundaciones.
2. amenazas ocasionadas por el hombre.
3. deliberados.

- **Nivel físico:** control de acceso a los datos; puertas con registro de entrada, registro de los préstamos de los expedientes, protección de ficheros en papel e informáticos, cerraduras, aislamientos. Una buena medida de seguridad: que no todos sepan cómo acceder a todo.

- **Nivel lógico:** Que se tenga acceso a datos proporcionalmente según se necesiten, en función de la necesidad y del perfil autorizado de quien accede.
- La primera medida de seguridad es el **SENTIDO COMÚN.**
- Algunas cosas en las que hay que pensar: Si se trata de limitar los accesos…Si se trata de destruir documentación con datos personales, cuidado con los trocitos y con las papeleras…
- Alertados con la autoridad judicial: El Poder Judicial no tiene acceso ilimitado a los datos que posee la Administración Pública o cualquier profesional en el ejercicio de sus funciones. Los datos que se ceden a los jueces tienen que ser los necesarios pero no todos.

Niveles de seguridad: MEDIDAS DE SEGURIDAD APLICABLES A LOS FICHEROS Y TRATAMIENTOS NO AUTOMATIZADOS

Aplicación Acumulativa: las medidas de seguridad se aplican acumulativamente, de manera que cuanto mayor nivel de seguridad requieran los ficheros, más medidas de seguridad hay que implementarle. De esta manera a un fichero que requiera de un nivel de seguridad medio, también se les aplicará las medidas previstas para el nivel básico y a los ficheros que requieran de un nivel de seguridad alto también se le aplicarán las medidas de seguridad previstas para los niveles básicos y medio.

Medidas de seguridad	Nivel básico	Nivel medio	Nivel alto
Art. 89. funciones y obligaciones del personal	Si	Si	Si
Art. 90. Registro de incidencias	Si	Si	Si
Art. 91. control de acceso	Si	Si	Si
Art. 92. gestión de soportes y documentos	Si	Si	Si
Art. 106. criterios de Archivo	Si	Si	Si
Art. 107. Dispositivos de almacenamiento	Si	Si	Si
Art. 108. Custodia de soportes	Si	Si	Si
Art. 109. Responsable de seguridad		Si	Si
Art. 110. Auditoria		Si	Si
Art. 111. Almacenamiento de la información			Si
Art. 112. Copia o reproducción			Si
Art. 113. Acceso a la documentación			Si
Art. 114. Traslado de la documentación			Si

Nivel básico: Las medidas correspondientes al nivel básico se aplican absolutamente a todos los ficheros que contengan datos concernientes a personas físicas identificadas o identificables. Se trata del conjunto de medidas de seguridad que deben estar presentes en toda organización por el mero hecho de tratar datos personales, independientemente de que por el tipo de datos tratados o por el tipo de tratamiento realizado sea preciso añadir las medidas de seguridad previstas para los niveles medio o alto.

Nivel medio: Además de las medidas previstas para el nivel básico, se aplicarán las medias de seguridad de nivel medio a los siguientes ficheros o tratamientos:

- Los relativos a la comisión de infracciones administrativas o penales.
- Aquellos cuya finalidad sea la prestación de servicios de información sobre solvencia patrimonial o de crédito.
- Aquellos de los que sean responsables administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.
- Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
- Aquellos de los que sean responsables las entidades gestoras y servicios comunes de la seguridad social y se relacionen con

el ejercicio de sus competencias. De igual modo aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la seguridad social.
- Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

Nivel alto: Existen determinados ficheros o tratamientos que, por su especial influencia en la intimidad de las personas, deben ser tratados con un nivel de protección superior a cualquier otro tratamiento de datos personales, por lo que además de aplicarles las medidas de seguridad de nivel básico y las de nivel medio, deben estar también protegidos con las medidas clasificadas de nivel alto. Dichos ficheros son los siguientes:

- Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- Aquellos que contengan datos derivados de actos de violencia de género.

Excepción: Existen determinados ficheros o tratamientos de datos que, a pesar de contener datos que requieren de un nivel alto de seguridad, pueden ser protegidos aplicando las medidas previstas para el nivel básico. Estos ficheros o tratamientos son los siguientes:

En caso de ficheros o tratamientos de datos de ***ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual,*** bastará la implantación de las medidas de seguridad de nivel básico cuando los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros, o cuando se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan ***datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado,*** con motivo del cumplimiento de deberes públicos.

Funciones y obligaciones del personal

En el documento de seguridad de los ficheros no automatizados se deben definir claramente cuáles son las funciones y obligaciones del personal que tenga acceso a los datos de carácter personal en los siguientes términos:

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad. También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.
2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Registro de incidencias

Todo fichero no automatizado deberá contar con un registro de incidencias, en el que se hará constar cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos de carácter personal.

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en el que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quien se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Control de acceso

En todos los ficheros no automatizados se debe implantar un mecanismo que controle el acceso de los usuarios a los datos de carácter personal.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Gestión de soportes y documentos

En todos los ficheros no automatizados la gestión de soportes y documentos que contengan datos de carácter personal se debe llevar a cabo de la siguiente manera:

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad. Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.
2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.
3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Criterios de archivo y almacenamiento de la información

En todos los ficheros no automatizados, el archivo con soportes o documentos que contengan datos de carácter personal debe realizarse bajo criterios que garanticen la correcta conservación de los documentos, que faciliten la consulta de la información y que posibiliten al ciudadano el ejercicio de su derechos Arco (Oposición, acceso, rectificación y cancelación) en los siguientes términos:

- El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.
- En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Dispositivos de almacenamiento

En todos los ficheros no automatizados, el responsable del fichero debe adoptar medidas que impidan el acceso de personas no autorizadas a los dispositivos que contengan datos de carácter personal en los siguientes términos:

- Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura.
- Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Custodia de soportes

Tal y como recoge el artículo 108 del Real Decreto 1720/2007, aplicable en todos los ficheros no automatizados, mientras la documentación que contiene datos de carácter personal no se encuentre archivada en un lugar adecuado, la persona que se encuentre a cargo de la misma, deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada en los siguientes términos:

- Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Responsables de seguridad

Tal y como recoge el artículo 109 del Real Decreto 1720/2007, cuando se trate de ficheros no automatizados que requieran de un nivel de seguridad medio-alto se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento, según el cual:

- En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciado según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.
- En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Auditoria

- Tal y como recoge el artículo 110 del Real Decreto 1720/2007, los ficheros no automatizados que requieran de un nivel de seguridad medio o alto, se someterán, al menos cada dos años, a una auditoria interna o externa que verifique el cumplimiento de lo dispuesto en el Título VIII de este real decreto

Almacenamiento de la información

Tal y como recoge el artículo 111 del Real Decreto 1720/2007, en aquellos ficheros que requieran de un nivel alto de seguridad, la información debe ser almacenada cumpliendo con los siguientes requisitos:

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.
2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir

lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Copia o reproducción

Los ficheros no automatizados que requieran de un nivel alto de seguridad, la generación de copias o la reproducción de los documentos que contengan datos de carácter personal únicamente podrán ser realizados en los siguientes términos:

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.
2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Acceso a la documentación

Cuando se trate de ficheros no automatizados que requieran de un nivel alto de seguridad, el acceso a la documentación deberá realizarse cumpliendo con los siguientes requisitos:

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.
2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Traslado de la documentación

Cuando se trate de ficheros no automatizados que requieran de un nivel alto de seguridad, el traslado físico de la documentación debe realizarse de manera que no se pueda acceder o manipular la información durante el traslado, en los siguientes términos:

- Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

5. FACILITAR A LAS PERSONAS EL EJERCICIO DE SUS DERECHOS-DERECHOS ARCO

El responsable del fichero debe atender a los ciudadanos cuando éstos pretendan ejercer alguno de sus derechos Arco (acceso, rectificación, cancelación y oposición), para los cual debe poner en marcha un procedimiento sencillo y gratuito que facilite al interesado el ejercicio de sus derechos y que permita al propio responsable dar una respuesta a las solicitudes dentro de los plazos legalmente establecidos.

Los derechos Arco, son el conjunto de derechos a través de los cuales la LOPD garantiza a las personas el poder de control sobre sus datos personales. Según el Tribunal constitucional en su sentencia n.º 292/2000, estos derechos constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y *"sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer".*

Los derechos Arco (derechos personalísimos e independientes) son los siguientes:

5.1. Derecho de Acceso.

Este derecho permite al ciudadano dirigirse al responsable de un fichero para solicitarle información sobre si sus datos están siendo objeto de tratamiento, de la finalidad del mismo, del origen de los datos y de las comunicaciones realizadas.

5.2. Derecho de rectificación y cancelación.

Son las dos opciones que tienen los ciudadanos cuando sus datos personales sean objeto de tratamiento inexacto, incompleto,

inadecuado o excesivo. En estos supuestos el titular de los datos podrá requerir al responsable del tratamiento para que rectifique los datos y registre los que correspondan o bien para que cancele sus datos y los elimine definitivamente del fichero.

El ejercicio del derecho de **rectificación** dará lugar a la sustitución de los datos erróneos por los datos correctos.

El ejercicio del derecho de **cancelación** dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo los datos serán definitivamente eliminados de los ficheros.

El derecho de cancelación (al igual que el resto de los derechos Arco), son derechos personalísimos, lo que significa que solamente pueden ser ejercidos por el titular de los datos, por su representante legal (en caso de incapacidad o minoría de edad) o por un representante voluntario expresamente designado para el ejercicio del derecho.

Otorgamiento de la CANCELACIÓN de los datos. Cuando se ejercita el derecho de cancelación se hace con la intención de que los datos desaparezcan del fichero, sin embargo, esto no es lo que sucede de inmediato; cuando se otorga el derecho de cancelación de los datos, se bloquean impidiendo su tratamiento, pero se mantienen registrados en los ficheros únicamente a disposición de las administraciones públicas, jueces y tribunales, hasta que prescriban las posibles responsabilidades nacidas del tratamiento.

5.3. derecho de oposición.

Consiste en la facultad que posee el titular de los datos para dirigirse al responsable del fichero o tratamiento y requiere para que deje de tratar sus datos en los siguientes supuestos: cuando se tratan sus datos sin su consentimiento, cuando el tratamiento de sus datos se realice con fines de publicidad o de prospección comercial, y cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

6. COLABORACIÓN CON LA AGPD EN EL EJERCICIO DE SUS FUNCIONES

El responsable del fichero debe colaborar con la Agencia Española de Protección de Datos en el ejercicio de sus funciones, para lo cual le enviará las notificaciones previstas legalmente, le facilitará el ejercicio de la función inspectora y le aportará la información que le sea requerida en cada momento.

7. GESTIÓN DEL CICLO DE VIDA DE LA DOCUMENTACIÓN

Control de acceso a ficheros no automatizados de datos:

El gran reto de la implantación de las medidas de seguridad del RLOPD ha sido instaurar los mecanismos que garanticen que el registro de acceso a los datos sea actual y completo. Para hacernos una idea de la magnitud de este requerimiento, sólo tenemos que plantearnos el acceso como la mera visualización consciente de un documento, e intentar adivinar el número de historias clínicas en papel que se tratan habitualmente en la planta de enfermos de cualquier hospital.

Gestión de documentación:

Indica medidas básicas de seguridad para la gestión de la documentación como son el inventario e identificación documental, así como el establecimiento de procedimientos de desecho y la destrucción de documentación. En relación a la identificación de la documentación sensible, debe ser un método de identificación fácil de reconocer para el personal con acceso autorizado, pero complicado para terceros. También se establece la necesidad de implantar medidas durante el traslado de documentación.

Criterio de archivo:

El responsable del fichero será quién marque los procedimientos de actuación. En todo caso este archivo debe garantizar la localiza-

ción, consulta y conservación de la documentación, así como posibilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Dispositivos de almacenamiento y custodia de soportes:

Los dispositivos de almacenamiento de documentos de nivel básico deben disponer de mecanismos que obstaculicen su apertura, mientras que en relación al almacenamiento de la documentación de nivel alto, éstos estarán ubicados en áreas de acceso restringido. Debemos entender estos dispositivos de almacenamiento aplicables al archivo central documental o situación habitual del documento una vez ha sido clasificado, en contraposición del tratamiento cuando la documentación está en proceso de revisión o tramitación. En ese caso, la persona que se encuentre a su cargo será la responsable de garantizar su custodia. Debemos entender que dicho deber de custodia debe ser aplicado a la documentación original y a todas sus reproducciones.

Copias y reproducción:

En este campo existe un requerimiento específico para documentos catalogados con un nivel alto de seguridad. Las copias sólo podrán ser realizadas y supervisadas por una persona autorizada. Por otra parte, se obliga a la destrucción de la reproducción, garantizando la imposibilidad su recuperación.

En relación a la necesidad de destruir el soporte, las medidas de seguridad deberían ser idénticas para copias y originales, ya que el objetivo es la protección de los datos del individuo y no del soporte en donde residen.

Medidas de seguridad específicas para ficheros y tratamientos no informatizados:

El RD 1720/2007 concede una atención especial a estos dispositivos de almacenamiento y custodia de documentos, con el fin de que se garantice la confidencialidad e integridad de los datos que contienen.

- Se exigirá la aplicación de unos criterios de archivo que garanticen la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación de los datos.
- Los ficheros de nivel MEDIO y ALTO habrán de almacenarse en lugares ignífugos y con acceso restringido y vigilado.
- Habrá que destruir o borrar cualquier documento o soporte que vaya a ser eliminado.
- Los armarios, archivadores y demás elementos de almacenamiento, deberán disponer de mecanismos adecuados de cierre (llave) que impidan el acceso a la documentación por personas no autorizadas.

Mientras esa documentación no esté archivada, la persona que esté a su cargo deberá custodiarla, impidiendo que acceda a ella quien no está autorizado.

Además, los ficheros no automatizados se deberán inventariar y controlar el acceso, en concreto, **para los ficheros de nivel alto habrá que registrar los accesos a documentos (durante 2 años como mínimo) y protegerlos mediante llaves o medidas equivalentes.**

- Cuando estos ficheros contengan datos clasificados de nivel alto, deberán estar en áreas cerradas con el dispositivo de seguridad pertinente (puertas con llave) pero, si por las características de los locales, no puede cumplirse esta medida, se permite aplicar otra alternativa que impida a las personas que no están autorizadas el acceso a esta documentación.
- Habrá que llevar un registro de entradas y salidas de documentos que contengan datos de nivel MEDIO y ALTO. Igualmente, y para dichos niveles de datos, se deberá establecer un procedimiento para la realización de copias y reproducción de los documentos, así como para su traslado.

FICHEROS DE TRATAMIENTO DEL ADN O INFORMACIÓN GENÉTICA

Las dudas e incógnitas que ofrece la regulación normativa de este tipo de bases de datos y/ ficheros de datos de carácter personal, son por norma relativas al tratamiento que posibilitan el riesgo de vulneración del derecho a la protección de datos personales e incluso al derecho a la intimidad, es decir, a la ponderación de riesgos. Se plantean los órganos legislativos cuestiones tales como ¿quién puede ser incluido un perfil de ADN en la base de datos?, ¿en qué momento? y ¿cuánto tiempo se puede conservar esa información? y, en función de las respuestas que se den y la flexibilidad de actuación, se configurará su regulación específica como un sistema de análisis sobre la población y la conservación de todas las muestras tomadas, como un sistema de análisis de un conjunto de muestras específicamente tomadas para investigaciones de carácter policial especiales (violaciones, desaparecidos, asesinatos, terrorismo, etc.), o un sistema limitado al análisis genético de un caso concreto, tanto para el sospechoso como para los vestigios recogidos específicamente para la investigación de ese hecho.

En España el equilibrio para elegir y elaborar una normativa sobre instrumentos de investigación que, por definición, ponen en peligro derechos fundamentales, está condicionado no sólo en el respeto por lo dispuesto en la Constitución sobre la reserva obligatoria de Ley, sino también por lo dispuesto en la normativa europea sobre derechos humanos. En el caso que nos ocupa, ha de estarse en primer lugar al *Convenio Europeo de Derechos Humanos* que, sobre una eventual restricción del derecho a la vida privada, recoge el deber de respeto de intimidad y de los datos de carácter personal, siempre y cuando, estas medidas estén previstas por la Ley, por una Ley concreta que en nuestro ordenamiento no es otra que la Ley Orgánica, la relativa al desarrollo de los derechos fundamentales y de las libertades públicas y que exige para su aprobación, modificación o derogación la votación final favorable sobre el conjunto del texto de la mayoría absoluta del Congreso.

En condiciones normales, cuando nos encontramos con unas gotas de sangre, o algún tipo de cabello, nuestra primera reacción será ponernos un algodón o soplar, respectivamente. La cosa adquiere otro cariz cuando cualquiera de ellos se encuentre inmerso en un ***recipiente cerrado con tapa encarnada en el que se etiqueta un nombre, un número o un código alfanumérico.*** Es precisamente la posibilidad de análisis de estas muestras lo que nos hace centrar el asunto en los **datos o información biomédica.** Así se ha puesto de manifiesto por diferentes organismos y en distintos cuerpos legislativos, tanto de ámbito internacional y comunitario, como en el ámbito nacional, en relación a la protección de la información sobre la salud en su vertiente más genérica: pasada, presente y futura, física y mental, buena o mala; y, particularmente, en relación al **tratamiento del ADN o a la información genética.**

Haciendo mención específica a los ficheros de la Guardia Civil y la Policía Nacional, se reparten distintos programas de tratamiento, de los que cabe destacar para los primeros el Programa Fénix de Identificación Genética de personas desaparecidas (1997) o la base de datos ADNIC, destinada a "cooperar con la Administración de Justicia mediante la identificación genética de vestigios biológicos y la identificación genética de vestigios biológicos y la identificación genética de muestras de origen conocido en usos de investigación policial" (delincuentes) y, para los segundos, el "Programa Genio" (2000) compuesto por dos bases de datos, "Veritas", destinada a "colaborar con la Administración de Justicia en la represión de infracciones penales con identificación genética de vestigios biológicos recogidos en la investigación de presuntos delitos o muestras de la misma naturaleza a solicitud de la autoridad competente" (desaparecidos) y "Humanitas", destinada a la "identificación de restos humanos de víctimas de hechos catastróficos o criminales y cadáveres de desaparecidos por ADN extraído de los mismos, e investigaciones del Cuerpo Nacional de Policía con los citados fines" (delitos).

Documentado cronológicamente, en **1982** arrancando de la Ley 1/1982, de protección civil del derecho al honor, a la intimidad personal, familiar y a la propia imagen, el ADN es

considerado como un dato de carácter personal ya que identifica al sujeto unívocamente.

En **1992** se inaugura el laboratorio conjunto de la Policía Nacional y la Guardia Civil de ADN, en Canillas, teniendo en cuenta la Recomendación R(92)1 del Comité de Ministros a los Estados miembros sobre la utilización de los análisis de ácido desoxirribonucleico (ADN) dentro del marco del sistema de justicia penal, Consejo de Europa, 10/2/1992: *"…No debe comportar vulneración de derechos fundamentales; Se considerará el estado de la ciencia en cada momento; Datos con fines meramente identificativos; Garantías en la protección de datos; Empleo de datos y muestras para los fines previstos; Archivo de datos por un tiempo establecido por ley y posterior destrucción…"*

En **1993,** se inaugura el laboratorio de ADN de la Guardia Civil. Adaptándose posteriormente a la RECOMENDACIÓN Nº R (97)5. Adoptada por el Comité de Ministros del 13 de febrero de 1.997, durante la 584 reunión de los Delegados de los Ministros DEL COMITÉ DE MINISTROS A LOS ESTADOS MIEMBROS RELATIVA A LA PROTECCIÓN DE **DATOS MÉDICOS**

"Datos de carácter personal" significa cualquier información relativa a una persona física identificada o identificable. No se considerará identificable a una persona física si la identificación en sí requiere plazos y actividades al margen de lo razonable. Cuando una persona física no sea identificable, los datos se considerarán anónimos;

"Datos médicos" hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas;

"Datos genéticos" se refiere a todos los datos, de cualquier tipo, relacionados con los caracteres hereditarios de un individuo o que, vinculados a dichos caracteres, compongan el patrimonio de un grupo de individuos emparentados. Hace referencia de la misma manera a todos los datos que afecten a intercambios de información genética (genes) de un individuo o línea genética, con relación a cualquier aspecto de la salud o de una enfermedad, constituya o no un carácter identificable. La línea genética estará constituida por similitudes genéticas resultantes de una procreación y compartidas por dos o más individuos.

En **1997,** se crea el fichero FENIX de la Dirección General de la Guardia Civil (Fichero automatizado dado de alta con el código de inscripción 1983560002 en la Agencia de Protección de Datos; complementario del Anexo de la Orden de 26/06/94 que regula los ficheros con datos de carácter personal gestionados por el Ministerio del Interior).

Finalidad del fichero: Identificación genética de personas desaparecidas y cadáveres sin identificar, con finalidad científica, de interés público y judicial.

Usos previstos: investigaciones de la Guardia Civil.

Personas o colectivos, sobre los que se pretenden obtener datos de carácter personal, o que resulten obligados a suministrarlos: Las personas que voluntariamente deseen contribuir a la identificación de una persona y a las que las autoridades con competencia legal determinen; así como los retos humanos que deban identificarse.

Procedimiento de recogida de datos de carácter personal: Datos aportados por los interesados y otras personas físicas distintas del afectado (con sujeción a lo expresado en el párrafo anterior), administraciones públicas, recogidos mediante formularios, transmisión electrónica / Internet o análisis del laboratorio. Utilizando soporte papel, informático o telemático. Actividades de identificación e investigación de restos humanos realizadas por el Cuerpo de la Guardia Civil.

Estructura básica del fichero y la descripción de los tipos de datos de carácter personal, incluidos en el mismo: Datos de carácter identificativo: Número de registro personal y perfil genético. Datos de características personales. Sexo.

En **1999,** se adapta a la LOPD 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

En **2000,** se crea el fichero ADNIC (Fichero automatizado dado de alta con el código de inscripción 2001170037 en la Agencia de Protección de Datos; complementario del Anexo de la Orden de 26/06/94 que regula los ficheros con datos de carácter personal gestionados por el Ministerio del Interior).

Finalidad del fichero: Cooperar con la Administración de Justicia mediante la identificación genética de vestigios biológicos y la identificación genética de muestras de origen conocido, en investigaciones realizadas por el Cuerpo de la Guardia Civil.

Usos previstos: Investigación policial.

Personas o colectivos, sobre los que se pretenden obtener datos de carácter personal, o que resulten obligados a suministrados: Las personas que determinen las autoridades que tienen atribuidas competencias por ley para exigir el tratamiento de los datos, las que expresamente lo requieran y estén relacionadas con algún hecho, y los vestigios biológicos relacionados con los hechos.

Procedimiento de recogida de datos de carácter personal: El propio interesado, otras personas físicas distintas del afectado (con sujeción a lo expresarlo en el párrafo anterior y al amparo de la Ley de Enjuiciamiento Criminal), o su representante y las administraciones públicas, mediante formulario, transmisión electrónica de datos/internet y análisis de laboratorio de ADN en soporte papel, vía telemática o soporte informático o magnético.

Posteriormente el Ministerio de Justicia crea en **2003** el fichero "Perfiles de ADN"

Finalidad: Comparación de perfiles de ADN con fines identificativos en casos judiciales concretos (hasta que no exista una regulación legal, no se realizan búsquedas sistemáticas de perfiles genéticos procedentes de distintos casos).

Usos: Investigación analítica. Una vez cumplida la finalidad investigadora los datos se mantendrán completamente anomizados.

Estudio de frecuencias génicas en la población de referencia, previo procedimiento de disociación de los datos que permitan la identificación de los interesados.

Personas y colectivos afectados: Las personas implicadas en los procedimientos judiciales desarrollados en el territorio sobre el que el Departamento de Madrid ejerce sus competencias.

Procedimiento de recogida de datos: Pasivamente a partir de los autos judiciales en los supuestos que establezcan las leyes procesales y activamente mediante entrevista personal (sólo en ciertos casos).

Estructura básica del fichero:

Perfiles de ADN procedentes de vestigios biológicos humanos de origen desconocido.

Perfiles de ADN procedentes de restos cadavéricos humanos de origen desconocido.

Perfiles de ADN procedentes de muestras de referencia de imputados por la autoridad judicial de cometer algún delito.

Perfiles de ADN de muestras de referencia de personas no imputadas que colaboran con la autoridad judicial en el esclarecimiento de hechos delictivos.

Perfiles de ADN de muestras de personas implicadas en casos civiles de investigación biológica de la paternidad y/o maternidad.

Perfiles de ADN anónimos con fines de investigación estadística y científica.

Con las modificaciones de la Ley de Enjuiciamiento Criminal en noviembre de 2003, se promueve la creación del CEMU (Comité Ejecutivo de Mando unificado) e instaurando SUBA (sistema unificado de consultas en las bases de datos FENIX, ADNIC-VERITAS, HUMANITAS), haciendo además una nueva redacción ADNIC

En **2004** se crea el SISTEMA DE GESTIÓN NACIONAL DE PATRONES IDENTIFICATIVOS OBTENIDOS A PARTIR DE MUESTRAS DE ADN DE INTERÉS POLICIAL (SIGENPI).

COMSIGENPI: Comité para la gestión del SIGENPI presidido por el Subdirector General de Sistemas de Información y Comunicaciones para la Seguridad de la Secretaría de Estado de Seguridad. Base de datos nacional, institucionales y equipos locales.

En su redacción el art. 9.–INFORMACION ASOCIADA A UN PERFIL GENETICO, establece:

En el Documento Marco del Sistema de Gestión Nacional de patrones identificativos (SIGENPI) del Ministerio del Interior, consta como una condición para los usuarios: "que se pedirá y exigirá, El archivo de la información de interés judicial y policial asociada a un perfil genético, en forma tal, que cuando ocurra una coincidencia/match/hit; dicha información sea facilitada de forma directa cuando para ello sea requerido".

Cuando se solicite a un laboratorio la información asociada a un perfil genético, se facilitará al menos: Muestra y circunstancias de la misma a partir de la cual se obtuvo el perfil

genético (colilla de cigarro hallada en…; indubitada de….; etc.). Hecho delictivo de que se trata y circunstancias (denunciante, victima, etc.) Unidad policial interviniente (diligencias policiales, atestado, etc.) Unidad judicial que conozca del caso (diligencias previas, procedimiento, sumario, etc.) Informe pericial que se emitió, en el que constaba el resultado del perfil genético (número de informe, fotocopia del informe –si se estima necesario-, etc.)

Cualquier otra información que se considere de interés, en aras al mayor esclarecimiento de los hechos investigados.

En **2007,** todo lo anterior promovió la redacción de la LO 10/2007, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN, que concretamente en su Artículo 3 establece:

Tipos de identificadores obtenidos a partir del ADN incluidos en el Registro Nacional.

Se inscribirán en la base de datos policial de identificadores obtenidos a partir del ADN los siguientes datos:

a) los datos identificativos extraídos a partir del ADN de muestras o fluidos que, en el marco de una investigación criminal, hubieran sido hallados u obtenidos a partir del análisis de las muestras biológicas del sospechoso, detenido o imputado, cuando se trate de delitos graves y, en todo caso, los que afecten a la vida, la libertad, la indemnidad o la libertad sexual, la integridad de las personas, el patrimonio siempre que fuesen realizados con fuerza en las cosas, o violencia o intimidación en las personas, así como en los casos de la delincuencia organizada, debiéndose entenderse incluida, en todo caso, en el termino delincuencia organizada la recogida en el articulo 282 bis, apartado 4 de la Ley de Enjuiciamiento Criminal en relación con los delitos enumerados.

b) los patrones identificativos obtenidos en los procedimientos de identificación de restos cadavéricos o de averiguación de personas desaparecidas.

La inscripción en la base de datos policial de los identificadores obtenidos a partir del ADN a que se refiere este apartado, no precisará el consentimiento del afectado, el cual será informado por escrito de todos los derechos que le asisten respecto a la inclusión en dicha base, quedando constancia de ello en el procedimiento.

Igualmente, podrán inscribirse los datos identificativos obtenidos a partir del ADN cuando el afectado hubiera prestado expresamente su consentimiento.

FIGURAS QUE INTERVIENEN EN EL PROCESO

Las figuras que intervienen en el proceso vienen establecidas en el artículo 5 del Real Decreto 1720/2007.

Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

LEGISLACIÓN APLICABLE

- Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal.
- Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

- Decreto 67/2003, de 22 de mayo, por el que se aprueba el Reglamento de desarrollo de la Agencia de Protección de Datos de la Comunidad de Madrid de tutela de derechos y de control de ficheros de datos de carácter personal.
- LO 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.
- Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.
- Ley de Enjuiciamiento Criminal.

REFERENCIAS

- RECOMENDACIÓN Nº R (97)5. Adoptada por el Comité de Ministros del 13 de febrero de 1.997, durante la 584 reunión de los Delegados de los Ministros DEL COMITÉ DE MINISTROS A LOS ESTADOS MIEMBROS RELATIVA A LA PROTECCIÓN DE **DATOS MÉDICOS.**
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Recomendación 2/2004, de 30 de julio, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas (aprobada por resolución del director de la Agencia de Protección de datos de la CAM con fecha 30 de julio de 2004).
- COMSIGENPI: Comité para la gestión del SIGENPI presidido por el Subdirector General de Sistemas de Información y Comunicaciones para la Seguridad de la Secretaría de Estado de Seguridad.
- Recomendación 1/2008, de 14 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre el tratamiento de datos personales en los servicios sociales de la Administración de los Entes Locales de la Comunidad de Madrid.
- La ley Orgánica 15/1999 de Protección de datos Análisis y Comentario de su jurisprudencia-editorial Lex Nova.
- Protección de datos personales para Administraciones Locales-editorial Thomson Civitas.
- El derecho fundamental a la protección de datos. Derecho español y comparado, por María Mercedes Serrano Pérez.
- Manuales y Guías de la Colección de "Protección de Datos" de la Agencia de protección de datos de la CAM.