REVISTA IBEROAMERICANA DE
FERTILIDAD

Marco legal y tecnológico español para la gestión de datos clínicos en los servicios de Reproducción Asistida (parte I).

Spanish legal and technological framework for the management of clinical data related to assisted Human Reproduction (phase I).

Almudena Alcaide Raya[1], Antonio Alcaide Raya[2], Nacho Martín Martín[3], Silvia Jiménez Bravo[4].

[1]Dpto. de Informática. Universidad Carlos III de Madrid. aalcaide@inf.uc3m.es

[2]Especialista en Diagnóstico Genético Preimplantacional de ReproFiv, Madrid. aalcaide@dgpalcaide.com

[3] Dpto. de Informática. Universidad Carlos III de Madrid. 100033610@alumnos.uc3m.es

[4] Directora de Laboratorio de ReproFiv, Madrid. silviajimenez@reprofiv.com

RESUMEN

Este trabajo constituye la primera parte de un estudio global realizado bajo el título: Marco legal y tecnológico español para la gestión de datos clínicos en los servicios de reproducción asistida.
En esta primera fase del proyecto se realiza un estudio exhaustivo de la normativa española vigente acerca del tratamiento automatizado de datos clínicos de carácter personal en el ámbito de la reproducción asistida humana, así como de las obligaciones que la Ley impone sobre los centros públicos y privados que ofrecen estos servicios. Se realizará una exposición detallada de las obligaciones y derechos de los actores involucrados en estas actividades, y se dejarán marcadas las pautas de actuación para la segunda fase del proyecto. En la segunda fase del trabajo se llevará a cabo un estudio del marco tecnológico existente para la automatización de procesos y el diseño novel de una base de datos normalizada, para la custodia de este tipo de datos y tratamientos, mejorando el planteamiento actual. El objetivo de este diseño es homogeneizar el conjunto de valores, atributos, actores y actividades en el ámbito descrito, así como definir e implementar mecanismos seguros y estandarizados de acceso y gestión de datos clínicos propios de los servicios de reproducción asistida, dentro del marco legal vigente descrito en la fase primera del proyecto. Adicionalmente, esta base de datos proporcionará una base para la creación de almacenes de datos (data warehouses) en los que llevar a cabo estudios estadísticos y de investigación, que facilite además las tareas de auditoría y control sobre las actividades que se realizan en este campo, protegiendo siempre la privacidad de los actores. En definitiva, el estudio, desde el punto de vista legal y operativo de los parámetros y variables in-

Aceptado definitivamente: 13/12/12
Almudena Alcaide Raya, Dpto. de Informática. Universidad Carlos III de Madrid. aalcaide@inf.uc3m.es
SOLICITUD REIMPRESIÓN: Email: contacto@editorialmedica.com

herentes a las actividades realizadas en este tipo de servicios, la homogeneización de los datos, la disociación de datos clínicos, el diseño de un sistema de gestión y procesamiento de datos y tratamientos, la construcción almacenes de datos anonimizados y homogéneos, sienta las bases y abre vías de investigación para la aplicación de técnicas avanzadas de inteligencia artificial, minería de datos, estadística, o computación evolutiva, por mencionar algunas, con el objetivo común de definir modelos de soporte a la decisión a la selección de embriones, mejorar las tasas de éxito y el servicio prestado

(Rev. Iberoam. Fert Rep Hum, 2013; **30**; xxx-xxx © Revista Iberoamericana de Fertilidad y Reproducción Humana.

Palabras clave : *Reproducción, Procesamiento Automatizado de Datos, Bases de Datos, Privacidad.*

SUMMARY

This article is the first part of a global study entitled: spanish legal and technological framework for the management of clinical data related to assisted human reproduction.
In this first phase of the project we present a comprehensive study of the Spanish legislation on the automated processing of personal clinical data in the context of assisted human reproduction, as well as the analysis of the obligations that the Law imposes on public and private institutions offering these services.
In the second phase of this project, we will carry out a novel design of a standardized database for the management of such types of data and treatments, enhancing the current approach. The objective of this design is to standardize the set of values, attributes, actors and activities in the area described and to define secure and standardized mechanisms for accessing and managing clinical data specific to the assisted reproductive services. Moreover, our study provides the basis for the creation of anonymous data warehouses in which to conduct advanced statistical studies, thus facilitating the work of audit and control, while protecting the privacy of the actors involved and in compliance with the current legislation. Finally, a homogenized data warehouse allows for the application of artificial intelligence techniques to support the evaluation and the decision process in selecting embryos for transfer. In short, several aspects of this work are of high significance in the health field that concerns us, as it is, from a legal and operational standpoint, a novel in-depth analysis of the parameters and variables involved in these services. The homogenization of the data, the dissociation of clinical and personal data, the efficient design of a system for capturing, managing and processing data and treatments, provides the basis and opens lines of research for the application of techniques from artificial intelligence, data mining, statistics, biomedicine and evolutionary computation, to name a few, with the common goal of improving success rates and the service provided.

(Rev. Iberoam. Fert Rep Hum, 2013; **30**; xxx-xxx © Revista Iberoamericana de Fertilidad y Reproducción Humana

Key words: *Reproduction, Automatic Data processing, Database Management Systems, Privacy.*

FASE 1

La creación de la legislación española referida a la protección de datos de carácter personal está basada en el derecho fundamental de las personas físicas a la posibilidad de controlar sus datos personales, explícito en el apartado 4 del artículo 18 de la Constitución Española del año 1978 y en los convenios y directivas internacionales de Consejo y Parlamento Europeos, operativos en toda Europa desde el año 1981. Hasta el año 1992 y el nacimiento de la Ley Orgánica 5/1992, de 29 de octubre (1), de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), no había en España regulación específica en esta materia. Más tarde, se aprobaría el reglamento de desarrollo de la LORTAD, mediante el Real Decreto 994/1999, de 11 de junio (2), regulando las medidas técnicas y organizativas que deben aplicarse a los sistemas de información en los cuales se traten datos de carácter personal de forma automatizada. Esta primera ley estuvo vigente hasta el 14 de enero de 2000. Tanto esta ley, como posteriormente el reglamento se derogan por una nueva y mejorada Ley Orgánica 15/1999, de 13 de diciembre (3), de Protección de Datos de Carácter Personal, (LOPD) que regula "el tratamiento de los datos y ficheros de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan", y por un nuevo Reglamento de desarrollo de la LOPD (RLOPD), aprobado por el Real Decreto 1720/2007, de 21 de diciembre (4). La obligación del cumplimiento de esta ley está dirigida a todas las

personas, empresas y organismos, tanto privados como públicos que dispongan e intervengan en cualquier fase del tratamiento de datos personales. La aplicación de la LOPD y los posibles procesamientos sancionadores o inspecciones en el tratamiento automatizado de datos digitales tendrán repercusión si estos datos (contenidos en documentos, recursos, ficheros digitales, etc.) son identificados como personales. En 1993 se crea en España la Agencia Española de Protección de Datos (AEPD, (8)) definido como un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de la Administración pública en el ejercicio de sus funciones. Esta agencia es la encargada de velar por el cumplimiento de las leyes referentes a la protección de datos de carácter personal. Sólo en el año 2009 se recibieron 4136 denuncias, de los cuales 621 acabaron con sanción con un importe total de 24,8 millones de euros. Finalmente, en 2012 ante un recurso contencioso que interpuso la Asociación Española de Economía Digital, el tribunal supremo determina que algunos aspectos de la LOPD son contrarios al Derecho Comunitario. En particular, para el tratamiento o cesión de datos de carácter personal sin el consentimiento del interesado se elimina la excepción de que los mismos deban constar en fuentes accesibles al público.

En este trabajo se llevará a cabo un estudio del marco legal definido por la LOPD enfocado a la custodia y gestión de datos de carácter personal referentes a la salud y en concreto al ámbito de la reproducción asistida. Este trabajo constituye la fase primera del proyecto global anteriormente descrito.

DATOS DE CARÁCTER PERSONAL

En el RLOPD se establece la definición de dato de carácter personal como *"Cualquier información numérica, alfabética, gráfica, fotográfica acústica o de cualquier otro tipo concerniente a una persona física identificada o identificable"* siendo la definición de 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 desproporcionadas"*[1]. Además el RLOPD establece también la definición de dato de carácter personal relacionado con la salud, "*las informaciones concernientes a la salud pasada, presente o futura, física o mental, de un individuo. En particular se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética*"[2].

TIPOLOGÍA DE LOS DATOS DE CARÁCTER PERSONAL

La LOPD clasifica los datos personales en función de la relación que tienen esos datos con el derecho a la intimidad:

Especialmente protegidos, recogidos en los artículos 7 y 8, son los referidos a la ideología, religión, creencias, afiliación sindical, origen racial o étnico, salud, vida sexual y comisión de infracciones penales o administrativas. En el RLOPD se añadieron los datos relativos a actos de violencia de género.

Resto de datos, el resto de datos el reglamento no les concede una protección especial.

Igualmente se realiza una clasificación basada en las medidas de seguridad que se deben cumplir cuando se posean datos de carácter personal, existen tres niveles:

Datos de Nivel Básico. Se engloban en esta categoría datos identificativos, académicos, de información comercial, características personales, etc. (DNI, nombre, teléfonos, dirección postal o dirección electrónica).

Datos de Nivel Medio. Son datos de nivel medio los relativos a la comisión de infracciones administrativas o penales, datos de los que sean responsables entidades financieras para finalidades relacionadas con las prestación de servicios financieros (multas, infracciones, condenas, datos bancarios en un sistema financiero, etc.)

Datos de Nivel Alto. Son los que se refieren a datos de ideología, afiliación sindical, datos relativos a fines policiales, datos derivados de actos de violencia de género, salud, origen racial, etc. Existen algunas excepciones a la hora de tratar datos de nivel alto, en muchos de estos casos el RLOPD especifica que pueden ser tratados como datos de nivel básico. Por ejemplo destacamos:

- Datos de ideología, afiliación sindical, religión, creencias, origen social, salud o vida sexual. 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.

- 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.

- Datos de minusvalía. Cuando se refiere a un porcentaje de minusvalía para calcular el nivel de retención aplicable en nómina. O cuando contienen información relativa a apto/no

[1] *Artículo 5. f del Reglamento de la Ley Orgánica de Protección de Datos*
[2] *Artículo 5. g del Reglamento de la Ley Orgánica de Protección de Datos*

apto de un reconocimiento médico, discapacidad, invalidez, incapacidad laboral, enfermedad común, accidente laboral, enfermedad profesional, siempre que no describa la enfermedad o situación de salud.

- Datos de afiliación sindical. Cuando se utilicen exclusivamente para realizar la detracción de la cuota sindical o la domiciliación bancaria quedando excluidos de esta excepción los datos de aquellos afiliados que han disfrutado "horas sindicales".

OTROS DATOS PERSONALES

Con la creación de nuevas tecnologías la AEPD ha necesitado ampliar el concepto de datos personales incluyendo dentro de ese concepto los siguientes datos:

- La imagen (fija o grabación de video). "*La grabación de la imagen de una persona, ya sea trabajador o no de la empresa, es un dato personal, siendo éste el criterio de la Agencia Española de Proyección de datos*"[3].

- Datos biométricos (huella, iris, etc.). "*Los datos biométricos tenían la condición de datos de carácter personal y que, dado que los mismos no contienen ningún aspecto concreto de la personalidad, limitando su función a identificar a un sujeto cuando la información se vincula con éste, su tratamiento no tendrá mayor transcendencia que el de los datos relativos a un número de identificación personal, a una ficha que tan solo pueda utilizar una persona o a la combinación de ambos*"[4].

- La dirección de correo electrónico. "*No existe duda de que la dirección de correo electrónico identifica, incluso de manera directa, al titular de una cuenta, por lo que en todo caso dicha dirección ha de ser considerado como dato de carácter personal*"[5].

- La dirección IP. "*Las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal, resultando de aplicación la normativa sobre protección de datos*"[6].

Las distintas tipologías de los datos se encuentran resumidas en la Tabla 1 de este trabajo.

EXCEPCIONES AL TRATAMIENTO

A continuación se enumeran los tipos de datos donde no se aplica el RLOPD, estos son los siguientes:

- Tratamiento de datos referidos a personas jurídicas.

- Ficheros que se limiten a incorporar datos de personas físicas que presten sus servicios en aquellas (funciones, puestos desempeñados, dirección, teléfonos, y fax profesionales).

- Datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciales, industriales o navieros.

- Datos referidos a personas fallecidas.

OBLIGACIONES Y APLICACIÓN

En este apartado realizaremos una exposición de las obligaciones principales que la normativa sobre protección de datos impone a los responsables de los ficheros que contienen datos de carácter personal y demás personas que intervienen en algún momento en el tratamiento de estos ficheros.

Nos centraremos en tres momentos diferentes en el ciclo de vida de los datos:

a)Antes de la recogida de los datos.

b) Durante el tratamiento de los datos.

c) Después del tratamiento de los datos.

a) Obligaciones antes de la recogida de los datos

La LOPD establece como requisito imprescindible para la creación de un fichero con datos de carácter personal que el fichero "*resulte necesario para el logro de la actividad u objeto legítimo de la persona, empresa o entidad titular y se representen las garantías que esta ley establece para la protección de datos*"[7]. Los ficheros de estas características deben ser declarados a la AEPD para su registro en el Registro General de Protección de Datos (en adelante RGPD). Este registro se llevará a cabo en dos modalidades según sea de titularidad privada o de titularidad pública.

Un fichero de titularidad privada es definido como "*los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en*

[3] *Resolución R/00035/2006. Cuestiones generales sobre videovigilancia.*
[4] *Tratamiento de la huella digital de los trabajadores. Informe AEPD 1/1999*
[5] *Cribado de correo elecrónico, Informe Jurídico 0391/2007*
[6] *Carácter de dato personal de la dirección IP. Informe AEPD 327/2003*

[7] *Artículo 56 de la Ley Orgánica de Protección de Datos*

TABLA 1

Tipología de datos de carácter personal

Nivel Básico	Nivel Medio	Nivel Alto
•Identificativos	•Hacienda pública	•Salud
• Características personales	•Los de las administraciones tributarias relacionados con el ejercicio de las potestades tributarias	•Vida Sexual
•Académicos y profesionales		• Ideología
•Empleo y puestos de trabajo		•Creencias
•Información comercial	•Los de las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social	•Afiliación sindical
• Económico- financiero		•Religión
•Transaciones		•Violencia de genero
•IP	•Servicios financieros	•Origen racial
•Correo electrónico	•Solvencia patrimonial y crédito	
•Template biométrico	•Infraciones penales y administrativas	
	•Los que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos	

cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica"[8].

El artículo 27 de la LOPD detalla los pasos a seguir para el registro de un fichero de titularidad privada. Es importante destacar que el registro de los ficheros de carácter personal ante la AEPD es una obligación que corresponde al responsable de los mismos y que en ningún caso conlleva un reconocimiento por parte de la agencia del cumplimiento de ninguna otra obligación que establece la normativa.

Como punto importante debemos destacar que el RLOPD no impone la obligación de registrar ficheros temporales, definidos como "*ficheros de trabajo creados por usuarios o por procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento*"[9], pero sí establece la obligación de que el fichero origen esté debidamente registrado en el Registro General de Protección de Datos.

En cuanto a los ficheros de titularidad pública se definen como "*los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así*

[8] *Artículo 56 de la Ley Orgánica de Protección de Datos*

[9] *Artículo 5.2.g del Reglamento de la La Ley Orgánica de Protección de Datos*

como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público"[10].

En relación a estos ficheros hay que tener en cuenta las disposiciones sectoriales establecidas por la LOPD. En base a las mismas, la creación de los ficheros de las Administraciones Publicas sólo puede hacerse por medio de disposición general publicada en el B.O.E. Dicha disposición debe de contener, la finalidad del fichero y los usos previstos, las personas sobre los que se pretende obtener datos, el procedimiento de recogida, la estructura del fichero y la descripción de los tipos de datos ubicados en el mismo, las cesiones y transferencia de los datos, los órganos responsables del fichero.

Relativo a la calidad de los datos, el responsable del fichero, con carácter previo al tratamiento de los datos, debe tener en cuenta el principio de calidad de los datos definido en la LOPD en su artículo 4, que establece:

- Solo se podrán recoger para su tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades determinadas, explicitas y legítimas para las que se hayan obtenido.

- Queda prohibida la recogida de datos por medios fraudulentos, desleales o ilícitos.

Así mismo, es de obligado cumplimiento que los interesados a los que soliciten los datos personales sean informados previamente a la recogida de los datos de modo expreso, preciso e inequívoco de:

- La existencia del fichero o tratamiento de datos, de la finalidad de la recogida de estos y de los destinatarios de los mismos.

- Del carácter obligatorio o facultativo de su respuesta.

- De las consecuencias de la obtención de los datos.

- De los derechos que tiene como interesado (derecho de acceso, rectificación, cancelación y oposición).

- De la identidad de los responsables del procesamiento de sus datos.

La información del interesado se puede obtener de determinadas fuentes, y en todas ellas el responsable del procesamiento está obligado a informar al interesado. Los medios por los que se puede obtener la información son:

- Del propio interesado.

- De terceros, teniendo el responsable del fichero un plazo máximo de tres meses para informar al interesado del tratamiento de los datos y obtener así el consentimiento del mismo.

- Fuentes de acceso público, las únicas fuentes de acceso público reconocidas por la LOPD son: El censo promocional, las guías de teléfono, las listas de colegios profesionales, los diarios y boletines oficiales, los medios de comunicación social.

Por último, en lo referente al consentimiento del interesado, la LOPD establece que "*el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado salvo que la ley disponga otra cosa*"[11].

También se establece como definición de consentimiento del interesado como "*toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de los datos personales que le conciernen*"[12].

La AEPD expresa en un informe jurídico emitido en 2000[13] la interpretación de los conceptos que definen el consentimiento del interesado:

Libre, supone que el mismo deberá haber sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el código civil.

Específico, referido a una determinada operación de tratamiento de los datos y para una finalidad determinada, explícita y legítima del responsable de dicho tratamiento.

Inequívoco, implica que no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento.

Informado, requiere que el afectado conozca con anterioridad al tratamiento de sus datos la existencia del mismo y las finalidades para las que el mismo se produce.

La ley también establece las formas de prestar el consentimiento, estas formas se determinan en función del nivel de los datos, existen tres categorías definidas.

Tácito, es suficiente para el tratamiento de todos los datos menos los especialmente protegidos.

Expreso, es necesario para los datos que hacen referencia al origen racial, a la salud y a la vida sexual. El consenti-

[10] *Artículo 5.I.m del Reglamento de la Ley Orgánica de protección de Datos*

[11] *Artículo 6.1de la Ley Orgánica de Protección de Datos*

[12] *Artículo 3.h de la Ley Orgánica de Protección de Datos*

[13] *AEDP, Informe Jurídico 2000-0000 Caracteres del consentimiento definitivo por la LOPD*

miento expreso consiste en una afirmación específica del afectado aceptando el tratamiento de sus datos personales mediante una acto positivo y declarativo de la voluntad que se puede manifestar de manera oral (presencial, telefónica, etc.) o escrita (firmando una clausula o rellenando una casilla).

Expreso y por escrito, es necesario para los datos que revelan ideología, afiliación sindical, religión y creencias en los casos de ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones y otras entidades sin ánimo de lucro cuya finalidad sea política, filosófica, religiosa o sindical.

En el RLOPD se establece la forma de llevar a cabo la revocación del consentimiento. Esta revocación debe ser a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento.

Ante una revocación del consentimiento el responsable del fichero o tratamiento tiene las siguientes responsabilidades

- Cesar en el tratamiento de los datos en un plazo máximo de 10 días.

- Responder expresamente a la solicitud de revocación.

- Si los datos han sido cedidos previamente, deberá proceder a la revocación del consentimiento a los cesionarios también en un plazo de 10 días.

b) Obligaciones durante el tratamiento de los datos

El deber del secreto es uno de los principios básicos en materia de protección de datos y se encuentra recogido en el artículo 10 de la LOPD. Este deber se extiende desde el responsable del fichero a todos los que intervengan en cualquier fase durante el procesamiento de los datos de carácter personal. Obligando a éstos al secreto profesional respecto a los mismos y al deber de guardarlos.

Un punto sumamente importante de este marco legal se establece en el artículo 88 del RLOPD dónde se define el Documento de Seguridad, éste es un documento que el responsable del fichero deber realizar en el que se incluyen las medidas de índole técnica y organizativa acordes a la normativa vigente que será de obligado cumplimiento para el personal con acceso al tratamiento de los datos recogidos. Se puede realizar un único documento con todos los ficheros implicados o realizar un documento por cada fichero o atendiendo a criterios de agrupación del Responsable de Seguridad. Las medidas detalladas en este Documento de Seguridad dependen de la tipología de los datos que se custodian en el fichero/-s referenciado/-s. En el RLOPD se establecen las medidas generales que han de cumplir los ficheros de tratamiento automatizado de datos de carácter personal en función del nivel (Básico, Medio y Alto) en el que se engloben los datos del fichero. Las medidas de seguridad asociadas a cada nivel son inclusivas, es decir, los datos de nivel alto deben de cumplir tanto las medidas de seguridad adoptadas para ese nivel, como para los niveles inferiores (básico y medio).

En las Tablas 2, 3 y 4 se especifican cada una de las medidas para cada uno de los niveles. A continuación se detallan las referentes al nivel alto. Estas medidas de seguridad se aplican a los ficheros de datos de carácter personal que contengan información sobre ideología, religión, salud, vida sexual, datos derivados de actos de violencia de género. Estos ficheros deben cumplir las medidas de seguridad establecidas en el nivel básico y en el nivel medio y adicionalmente las medidas detalladas a continuación:

- Gestión y distribución de soportes[14]

  -Los soportes han de ser etiquetados utilizando un sistema comprensible y que permitan a los usuarios autorizados el acceso a los soportes, pero que dificulten la comprensión a personal no autorizado.

  -La distribución de los soportes que contengan los datos se deber realizar tras haber cifrado los datos o utilizando otro mecanismo que garantice la integridad de dicha información.

  -Cifrar la información, cuando ésta se encuentre fuera de las instalaciones bajo el control del responsable del fichero.

  -Deberá evitarse el tratamiento de los datos en dispositivos portátiles. En caso de que sea estrictamente necesario se adoptarán las medidas expuestas anteriormente.

- Copias de respaldo y recuperación[15]

  -Deberá conservarse una copia en un lugar diferente en el que se encuentren los mismos, cumpliendo además las medidas de seguridad citadas en anteriores medidas.

- Telecomunicaciones[16]

  -Todas las trasmisiones que se realicen a través de redes públicas o redes inalámbricas se realizarán cifrando dichos datos o bien utilizando otro mecanismo que garantice la integridad de la información.

- Registro de accesos[17]

  -Se ha de crear un registro de accesos en el que se reco-

[14] *Artículo 101 del Reglamento de la Ley Orgánica de Protección de Datos*
[15] *Artículo 102 del Reglamento de la Ley Orgánica de Protección de Datos*
[16] *Artículo 104 del Reglamento de la Ley Orgánica de Protección de Datos*
[17] *Artículo 103 del Reglamento de la Ley Orgánica de Protección de Datos*

TABLA 2

Medidas de seguridad

	Nivel básico	Nivel Medio	Nivel Alto
Responsable de Seguridad		+ El responsable del fichero debe designar uno o varios responsables de seguridad. + Es el encargado de controlar y coordinar las medidas del documento	
Personal	+ Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas + Definición de las funciones de control y las autorizaciones delegados por el responsable + Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento		
Incidencias	+ Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras + Procedimiento de notificación y gestión de las incidencias	FICHEROS AUTOMATIZADOS + Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados y en su caso, datos grabados manualmente + Autorización del responsable del fichero para la recuperación de datos	

gerán como mínimo, la identificación del usuario, la fecha y hora en la que se realizó el acceso, el tipo de acceso y el resultado del acceso (autorizado/no autorizado), en el caso que el acceso sea positivo se deberá registrar el registro accedido.

- Estos mecanismos deben de estar bajo el control del responsable de seguridad, revisándolos al menos una vez al mes.

- Se deben conservar los registros durante al menos dos años.

- No deberán tenerse en cuenta estas medidas si el responsable de seguridad es una persona física o si solo él tiene acceso al tratamiento de los datos, en cuyo caso deberá expresarse en el Documento de Seguridad.

Para los ficheros de tratamiento no automatizado se dictaminan las siguientes medidas

- Almacenamiento de la información. Los armarios, archivadores u otros elementos de almacenaje deben estar en áreas con acceso protegido con puertas con llave u otro dispositivo equivalente.

- Copia o reproducción. Se ha de limitar la posibilidad de realizar copias a los usuarios autorizados, destruyendo las copias desechadas.

- Acceso a la documentación, limitando el acceso únicamente al personal autorizado.

- Traslado de la documentación, evitando el acceso a la información durante un traslado.

TABLA 3

Medidas de seguridad (cont.)

	Nivel básico	Nivel Medio	Nivel Alto
Responsable de Seguridad	+ Relación actualizada de usuarios y accesos autorizados + Control de accesos permitidos a cada usuario según las funciones asignadas + Mecanismos que eviten el acceso a datos o recursos con derechos distintos a los autorizados + Concesión de permisos de acceso solo a personal autorizado + Mismas condiciones para personal ajeno con acceso a los recursos de datos	FICHEROS AUTOMATIZADOS + Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información	FICHEROS AUTOMATIZADOS + Registro de accesos: usuario, fecha, hora, fichero, tipo de acceso, autorizado o denegado + Revisión mensual por parte del responsable de seguridad + Conservación 2 años FICHEROS NO AUTOMATIZADOS + Control de accesos autorizado + Identificación de accesos para documentos accesibles por múltiples usuarios
Identificación y autenticación	FICHEROS AUTOMATIZADOS + Identificación y autenticación personalizada + Procedimiento de asignación y distribución de contraseñas + Almacenamiento ininteligible de las contraseñas + Periodicidad del cambio de contraseña: 1 año	FICHEROS AUTOMATIZADOS + Limite de intentos reiterados de acceso no autorizado	
Gestión de soportes	+ Inventario de soportes + Identificación del tipo de información que contienen o sistema de etiquetado + Acceso restringido al lugar de almacenamiento + Autorización de las salidas de soportes (incluidas a través de e-mail + Medidas para el transporte y el desecho de soportes	FICHEROS AUTOMATIZADOS + Registro de entrada y salida de soportes: documento o soporte, fecha, emisor / destinatario, número, tipo de información, forma de envío.	FICHEROS AUTOMATIZADOS + Sistema de etiquetado confidencial + Cifrado de datos en la distribución de soportes + Evitar distribución de soportes en la medida de lo posible
Copias de respaldo	FICHEROS AUTOMATIZADOS + Copia de respaldo semanal + Procedimiento de generación de copias de respaldo y recuperación de datos + Verificación semanal de los procedimientos + Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita + Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente		FICHEROS AUTOMATIZADOS + Copia de respaldo y procedimiento de recuperación en lugar diferente al que se encuentren los equipos

TABLA 3 (continuación)

Medidas de seguridad (cont.)

	Nivel básico	Nivel Medio	Nivel Alto
Criterios de archivo	FICHEROS NO AUTOMATIZADOS + El archivo de los documentos debe realizarse según criterios que faciliten la consulta y localización para garantizar el ejercicio de los derechos ARCO		

TABLA 4

Medidas de seguridad (cont.)

	Nivel básico	Nivel Medio	Nivel Alto
Almacenamiento	FICHEROS NO AUTOMATIZADOS + Dispositivos de almacenamiento dotados de mecanismos que obstaculicen la apertura		FICHEROS NO AUTOMATIZADOS + Armarios, archivadores de documentos en áreas con acceso protegido con puertas con llave
Custodia de soportes	FICHEROS NO AUTOMATIZADOS + Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados		
Copia o reproducción			FICHEROS NO AUTOMATIZADOS + Solo puede realizarse por usuarios autorizados + Destrucción de copias desechadas
Auditoria		+ Al menos cada dos años, interna o externa + Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad + Verificación y control de la adecuación de las medidas + Informe de detección de deficiencias y propuestas correctoras + Análisis del responsable de seguridad y conclusiones al responsable del fichero	

TABLA 4 (continuación)			
Medidas de seguridad (cont.)			
	Nivel básico	Nivel Medio	Nivel Alto
Telecomunicaciones			FICHEROS AUTOMATIZADOS + Transmisión de datos a través de redes electrónicas cifradas
Traslado de documentación			FICHEROS NO AUTOMATIZADOS + Medidas que impidan el acceso o manipulación

Relativo a la cesión de los datos durante la fase de tratamiento de los datos, la cesión de datos es definida en la LOPD como "*toda revelación de datos realizada a una persona distinta del interesado*"[18]. La cesión de los datos solo puede realizarse si se cumplen estos dos requisitos:

Que se realicen para el cumplimiento de fines directamente relacionados con las funciones legítimas de cedente y del cesionario.

- Consentimiento previo del interesado, éste no debe cumplirse:

  - Cuando la cesión esté autorizada por una ley.
  - Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.
  - Cuando la comunicación que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.
  - Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

c) Obligaciones al finalizar el tratamiento de los datos

La LOPD también establece una normativa acerca de lo que el responsable del fichero debe de hacer una vez cese el tratamiento de los datos de carácter personal.

Los datos de carácter personal deben de ser cancelados en el momento que los mismos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados.

Estos no pueden ser conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales los hubiera recabado o registrado.

El RLOPD establece el periodo en el que dichos datos pueden conservarse estableciendo que podrán conservarse durante el tiempo en el que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de pedidas precontractuales solicitadas por el interesado.

Una vez transcurrido ese tiempo, los datos sólo pueden ser conservados previa disociación de los mismos. Definiendo procedimiento de disociación como "*Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable*"[19]

INFRACCIONES Y SANCIONES

Es importante destacar que los responsables del fichero son los únicos responsables del cumplimiento de las medidas de seguridad expuestas en el apartado anterior y estarán sujetos al régimen sancionador establecido en la LOPD.

La clasificación de las sanciones se definen en tres tipos de sanciones: leves, graves o muy graves.

Infracciones leves

- No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

- No proporcionar la información que solicite la AEPD en el ejercicio de las competencias que tiene legítimamente atribuidas, en relación con los aspectos no sustantivos de la protección de datos.

- No solicitar la inscripción del fichero de datos de carácter personal en el RGPD, cuando no sea constitutivo de infracción grave.

[18] *Artículo 11 de la Ley de Protección de Datos*
[19] *Artículo 5.f de la Ley Orgánica de Protrcción de Datos*

- Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información necesaria.

Infracciones graves

- Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el B.O.E.

- Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

- Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

- Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la LOPD o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

- El impedimento o la obstaculización del ejercicio de los derechos ARCO (Derecho de acceso, rectificación, cancelación y oposición)

- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas.

- La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficiente para obtener una evaluación de la personalidad del individuo.

- Mantener los ficheros, locales, programas o equipos que contenga datos de carácter personal sin las debidas condiciones de seguridad.

- No remitir a la AEPD las notificaciones.

- La obstrucción al ejercicio de la función inspectora.

- No inscribir el fichero de datos de carácter personal en el RGPD.

Infracciones muy graves

- La recogida de datos de forma engañosa y fraudulenta.

-La comunicación o cesión de los datos, fuera de los casos permitidos.

- Recabar y tratar los datos de carácter personal sin el consentimiento expreso del afectado.

- No cesar en el uso ilegitimo de los tratamientos de datos de carácter personal cuando sea requerido para ello.

- La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización de la AEPD.

- Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

- La vulneración del deber de guardar secreto sobre los datos de carácter personal.

- No atender u obstaculizar de forma sistemática el ejercicio de los derechos ARCO.

- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Para los responsables de fichero que no sean Administraciones Públicas se establecen las sanciones detalladas en la Tabla 5.

En el caso de los ficheros cuyo responsable sean las Administraciones Públicas la AEPD procederá a dictar una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción.

DATOS CLÍNICOS

En el caso de los datos sanitarios, el marco legal existente que establece medidas de control sobre el tratamiento de los datos en este ámbito, lo constituyen las siguientes directivas:

- Ley 14/1986, de 25 de abril, General de Sanidad (5).

- 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 (6).

- Ley 14/2006, de 26 de mayo, sobre Técnicas de Reproducción Humana Asistida (7).

En cuanto a la primera de las leyes comentadas anteriormente son de especial interés los siguientes artículos:

"*Toda persona tiene derecho a la confidencialidad de toda información relacionada con su proceso y con su estancia*

TABLA 5		
Sanciones de la AEPD		
Infracción	Importe	Prescripción
Leve	De 600 a 60.000 €	1 año
Grave	De 60.000 a 300.000 €	2 años
Muy Grave	De 300.000 a 600.000 €	3 años

en instituciones sanitarias públicas y privadas que colaboren con el sistema público"[20].

"*Para la consecución de los objetivos que se desarrollan, las Administraciones Sanitarias, de acuerdo con sus competencias, crearán los Registros y elaborarán los análisis de información necesarios para el conocimiento de las distintas situaciones de las que puedan derivarse acciones de intervención de la autoridad sanitaria*"[21].

TIPOLOGÍA DE LOS DATOS CLÍNICOS

Al igual que en lo referente a los datos de carácter personal, la Ley define, entre otros, los siguientes conceptos:

Consentimiento Informado: conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud.

Documentación clínica: el soporte de cualquier tipo o clase que contiene un conjunto de datos e informaciones de carácter asistencial.

Historia clínica: el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial.

Información clínica: todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona o la forma de preservarla, cuidarla, mejorarla o recuperarla.

CUSTODIA DIGITAL DE LOS DATOS CLÍNICOS

Por otro lado, la Ley 41/2002 especifica cuestiones importantes relacionadas con la protección de datos clínicos y el derecho a la intimidad, en concreto destacamos los siguientes artículos:

"*Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley.* "[22].

"*Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes*"[23].

"*Toda actuación en el ámbito de la sanidad requiere, con carácter general, el previo consentimiento de los pacientes o usuarios… El consentimiento será verbal por regla general. Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente*"[24].

"*El paciente puede revocar libremente por escrito su consentimiento en cualquier momento*"[25].

En lo referente a la historia clínica y a la custodia digital de la misma, caben destacar los siguientes artículos:

"*Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información*"[26].

"*Las Administraciones sanitarias establecerán los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura.*"[27].

[20] *Artículo 10.3 de la Ley General de Sanidad*
[21] *Artículo 23 de la Ley General de Sanidad*

22 Artículo 7.1 de la Ley de Autonomía del Paciente y Documentación
23 Artículo 7.2 de la Ley de Autonomía del Paciente y Documentación
24 Artículos 2.2 y 8.2 de la Ley de Autonomía del Paciente y Documentación
25 Artículo 8.5 de la Ley de Autonomía del Paciente y Documentación
26 Artículo 14.2 de la Ley de Autonomía del Paciente y Documentación
27 Artículo 14.3 de la Ley de Autonomía del Paciente y Documentación

"*Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental*"[28].

"*El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones*"[29].

"*Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial*."[30].

"*Los profesionales sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen*."[31].

"*El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley*."[32].

Por último, se hace referencia a la LOPD en el siguiente artículo:

"*Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.*"[33].

Adicionalmente, de la Ley 14/2006, de 26 de mayo, sobre Técnicas de Reproducción Humana Asistida, se destacan los siguientes puntos relacionados con la confidencialidad de los datos y el consentimiento informado del paciente.

"*La aceptación de la realización de las técnicas de reproducción asistida por cada mujer receptora de ellas se reflejará en un formulario de consentimiento informado en el que se hará mención expresa de todas las condiciones concretas de cada caso en que se lleve a cabo su aplicación*."[34]

"T*odos los datos relativos a la utilización de estas técnicas deberán recogerse en historias clínicas individuales, que deberán ser tratadas con las debidas garantías de confidencialidad respecto a la identidad de los donantes, de los datos y condiciones de los usuarios y de las circunstancias que concurran en el origen de los hijos así nacidos*"[35]

"*La donación de gametos y pre-embriones será anónima y deberá garantizarse la confidencialidad de los datos de identidad de los donantes por los bancos de gametos, así como, en su caso, por los registros de donantes y de actividades de los centros que se constituyan*."[36]

"*Si la mujer estuviera casada, se precisará, además, el consentimiento de su marido, a menos que estuvieran separados legalmente o de hecho y así conste de manera fehaciente*."[37]

Finalmente, en el ámbito de los objetivos acometidos en este trabajo, son de especial interés los artículos relacionados con la actividad de los centros de reproducción asistida y el registro y auditoría de los mismos:

"*Los equipos médicos recogerán en una historia clínica, custodiada con la debida protección y confidencialidad, todas las referencias sobre los donantes y usuarios, así como los consentimientos firmados para la realización de la donación o de las técnicas*."[38]

"*Los centros de reproducción humana asistida se someterán con la periodicidad que establezcan las autoridades sanitarias competentes a auditorías externas que evaluarán tanto los requisitos técnicos y legales como la información transmitida a las Comunidades Autónomas a los efectos registrales correspondientes y los resultados obtenidos en su práctica clínica*."[39]

"*La Comisión Nacional de Reproducción Humana Asistida deberá ser informada, con una periodicidad al menos semestral, de las prácticas de diagnóstico preimplantacional que se lleven a cabo*."[40]

"*El Registro de actividad de los centros y servicios de reproducción asistida deberá hacer públicos con periodicidad, al menos, anual los datos de actividad de los centros relativos al número de técnicas y procedimientos de diferente tipo para los que se encuentren autorizados, así como las tasas de éxito en términos reproductivos obtenidas por*

[28] *Artículo 14.4 de la Ley de Autonomía del Paciente y Documentación*
[29] *Artículo 16.4 de la Ley de Autonomía del Paciente y Documentación*
[30] *Artículo 17.1 de la Ley de Autonomía del Paciente y Documentación*
[31] *Artículo 17.5 de la Ley de Autonomía del Paciente y Documentación*
[32] *Artículo 17.5 de la Ley de Autonomía del Paciente y Documentación*
[33] *Artículo 17.6 de la Ley de Autonomía del Paciente y Documentación*
[34] *Artículo 3.4 de la Ley sobre Técnicas de Reproducción Humana Asistida*
[35] *Artículo 3.6 de la Ley sobre Técnicas de Reproducción Humana Asistida*
[36] *Artículo 5.5 de la Ley sobre Técnicas de Reproducción Humana Asistida*
[37] *Artículo 6.3 de la Ley sobre Técnicas de Reproducción Humana Asistida*
[38] *Artículo 18.3 de la Ley sobre Técnicas de Reproducción Humana Asistida*
[39] *Artículo 19 de la Ley sobre Técnicas de Reproducción Humana Asistida*
[40] *Artículo 20.5 de la Ley sobre Técnicas de Reproducción Humana Asistida*

cada centro con cada técnica, y cualquier otro dato que se considere necesario para que por los usuarios de las técnicas de reproducción asistida se pueda valorar la calidad de la atención proporcionada por cada centro. El Registro de actividad de los centros y servicios de reproducción asistida recogerá también el número de preembriones crioconservados que se conserven, en su caso, en cada centro."[41]

CONCLUSIONES

Con este trabajo se ha pretendido dar una visión exhaustiva del marco legal vigente, que como se ha visto dicta pautas muy específicas para la elección y el desarrollo de un marco tecnológico adecuado al contexto. Con el objetivo de proporcionar ese marco tecnológico, la segunda fase de este proyecto tendrá como cometido principal la homogeneización y estandarización de los datos y la automatización segura de procesos, todo ello dentro de la legalidad descrita en este trabajo. Dentro de la automatización de procesos se llevará a cabo el estudio del marco tecnológico para la firma con DNI electrónico, en sustitución de la firma manuscrita requerida actualmente, sellos de tiempo, mecanismos de cifrado y certificados longevos de integridad y veracidad de los datos clínicos custodiados en formato electrónico.

BIBLIOGRAFÍA

1. **B.O.E. núm. 262,** de 31 de octubre de 1992. Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD)
2. **B.O.E. núm. 151**, de 25 de junio de 1999. Real Decreto 994/1999, de 11 de junio, reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.
3. **B.O.E. núm. 298**, de 14 de diciembre de 1999. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, (LOPD)
4. **B.O.E. núm. 17**, de 19 de enero de 2008. Real Decreto 1720/2007, de 21 de diciembre, reglamento de desarrollo de la Ley Orgánica 15/1999, DE 13 de diciembre, de protección de datos de carácter personal.
5. **B.O.E. núm. 102**, de 29 de abril de 1986. Ley 14/1986, de 25 de abril, General de Sanidad.
6. **B.O.E. núm. 274**, de 15 de noviembre de 2002. 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.
7. **B.O.E. núm. 126**, de 27 de mayo de 2006. Ley 14/2006, de 26 de mayo, sobre Técnicas de Reproducción Humana Asistida.

(8). AEPD, (www.aepd.es)

[41] *Artículo 22.2 de la Ley sobre Técnicas de Reproducción Humana Asistida*