Que no se te escapen tus datos

PID_00260385

José Enrique Pérez Palaci

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

José Enrique Pérez Palaci

Índice

Introducción..... 5

1. Principios relativos al tratamiento de los datos personales... 7
1.1. Licitud del tratamiento 7
1.1.1. El consentimiento del interesado 7
1.2. Tratamiento de categorías especiales de datos 11
1.2.1. Principio de minimización de los datos 13
1.2.2. Seudonimización de los datos personales 13
1.2.3. Consentimiento, datos de salud 14
1.3. La historia clínica electrónica 15
1.3.1. Evaluación de impacto relativa a la protección de datos (EIPD) 18

Bibliografía..... 23

Introducción

La protección de datos personales es un derecho fundamental establecido por la Carta de los Derechos Fundamentales de la Unión Europea, que aclara:

> Artículo 8: «Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan». La Carta de los Derechos Fundamentales de la Unión Europea (2010/C 83/02) Diario Oficial de la Unión Europea C83/389, (30/03/2010). [acceso el 22/09/18]. Disponible en:
>
> https://www.(texto consolidado) BOE.es/doue/2010/083/Z00389-00403.pdf

También lo establece la Constitución Española, que afirma:

> Artículo 18.1: «Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen» Constitución Española. «(TEXTO CONSOLIDADO) BOE» núm. 311, de 29/12/1978. [Acceso el 22/09/18] Disponible en:
>
> https://www.boe.es/buscar/pdf/1978/BOE-A-1978-31229-consolidado.pdf

. También se ve reflejado en el Reglamento General de Protección de Datos, que cita:

> Considerando 1: «La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental». REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Diario Oficial de la Unión Europea (04/05/2016) [acceso el 22/09/18] Disponible en:
>
> https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

. Se recoge explícitamente el preámbulo del Proyecto de Ley orgánica de protección de datos personales y garantía de los derechos digitales con fecha de entrada en el Senado el 23 de octubre de 2018, que con mención de cuanto recogido por el artículo 18.4 de la CE, aclara:

> Artículo 18.4 de la CE: «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

En este caso, se añade en el título «y garantía de los derechos digitales»; en el título X se regulan los derechos digitales: la neutralidad y acceso universal de Internet, la seguridad digital y la educación digital, frente a cuanto al «olvido» patente de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[1] , y es que ya en diciembre del año 1995 con la prestación del servicio Infovía de Telefónica cabe afirmar que se inicia el

(1)Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. «BOE» núm. 298, de 14/12/1999. [acceso el 22/09/18] Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

lanzamiento del Internet residencial a gran escala, de modo que a finales del año 1998 están conectados a la Red un total de aproximadamente trescientos mil ordenadores[2] , mientras que en el año 1999 Telefónica comienza a comercializar servicios ADSL.

[(2)]elmundo Evolución de Internet en España. Rivero, Raúl. (sede web). Madrid. elmundo.es 2002. (Acceso el 21/10/18) Disponible en: https://www.elmundo.es/imasd/docs/cursos/master-periodismo/2002/rivero-master02-espana.html

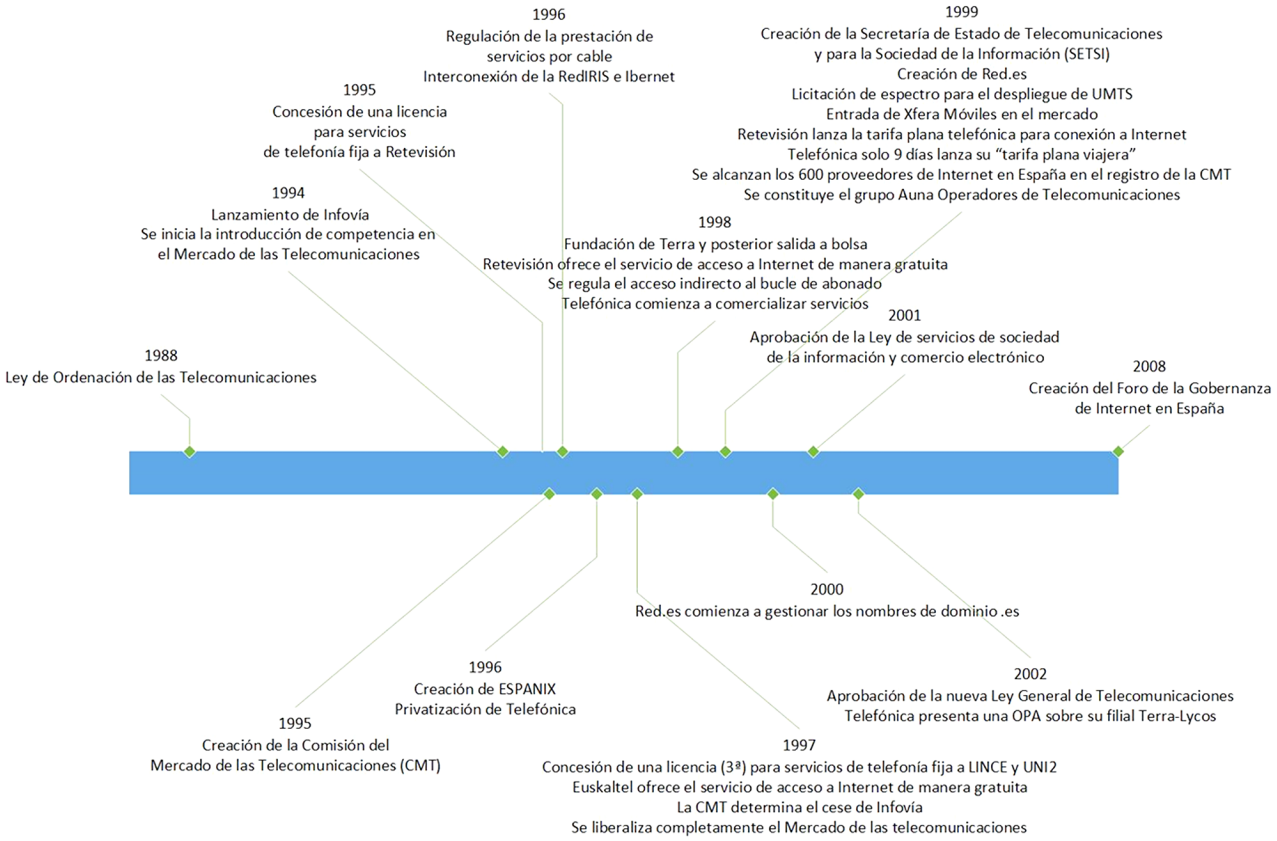
Sobre la protección de datos personales:

«[...] son fundamentales los derechos "que no se pueden comprar ni vender" (Bovero, M. 2005, 219), esto es, aquellos derechos subjetivos que corresponden universalmente a "todos" los seres humanos en cuanto dotados del estatus de personas, de ciudadanos o de sujetos con capacidad de obrar (Ferrajoli, L. 2007, 291). Por su parte, son "derechos subjetivos" todas las expectativas positivas (de prestaciones) o negativas (de no sufrir lesiones) adscritas a un sujeto por una norma jurídica y en razón de su estatus o condición de tal, prevista asimismo por una norma jurídica positiva, "como presupuesto de su idoneidad para ser titular de situaciones jurídicas y/o autor de los actos que son ejercicio de estas"»(Ferrajoli, L. 2004, 37)» Contreras, Sebastián. (2012). Ferrajoli y su teoría de los derechos fundamentales. Estudios de filosofía práctica e historia de las ideas, 14(2), 17-28. [Acceso el 21/10/18] Disponible en:

http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1851-94902012000200002

Pese ante esta realidad social, la LOPD que fue aprobada en 1999 no se adaptó a esos cambios tecnológicos que incidían en la protección de los datos personales, incluso con las modificaciones de los años 2001, 2003 y 2011.

Figura 1. Hitos históricos del desarrollo de las Telecomunicaciones e Internet en España



Fuente: Elaboración propia

1. Principios relativos al tratamiento de los datos personales

1.1. Licitud del tratamiento

A partir de los considerandos 10, 39, 40, 44, 45, 46, 50, 51, 63, y los artículos 5.1 y 6 del RGPD, podemos concluir que el tratamiento será lícito cuando se cumplan las siguientes condiciones:

1) La licitud del tratamiento está íntimamente relacionada con los principios de lealtad y transparencia, puesto que el interesado debe saber y conocer con manifiesta claridad que sus datos no solo están siendo recogidos, sino que están siendo utilizados, consultados o tratados, y para qué son tratados; de ahí que si el interesado no ha sido informado o no es informado con posterioridad al momento en que recogen sus datos del hecho de que estos están siendo tratados para otros fines, el tratamiento será ilícito; por eso los fines deben determinarse cuando los datos son recogidos.
2) La información y la comunicación que debe realizar el responsable del tratamiento (RT) han de ser fáciles de entender, accesibles, con un lenguaje claro y sencillo; información y comunicación que abarca, como mínimo:
   1) la identidad del responsable del tratamiento (quién es);
   2) los fines para los que son tratados los datos, fines que deben ser explícitos y legítimos;
   3) qué tipo de datos son recogidos;
   4) cómo puede el interesado hacer valer sus derechos;
   5) que los datos recabados sean adecuados, pertinentes y limitados a los fines para los que han sido recogidos;
   6) a qué entidades se pueden comunicar los datos personales;
   7) que se conserven solo durante el tiempo necesario, por lo que el RT debe establecer los plazos de conservación, sin perjuicio de la normativa legal específica aplicable en materia de conservación de los datos;
   8) las medidas de seguridad adoptadas por el RT para garantizar la integridad, la confidencialidad, la rectificación y la supresión de los datos personales.

1.1.1. El consentimiento del interesado

El artículo 4 11) del RGPD define como

> «"consentimiento del interesado"»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen».

Por tanto, el interesado debe haber prestado su consentimiento antes del tratamiento de sus datos, o bien dicho tratamiento debe estar amparado en una base legítima, es decir, el RGPD u otra norma legal aplicable, sin que quepa supeditar la ejecución del contrato o servicio a que el interesado consienta el tratamiento de los datos personales para finalidades que no estén relacionadas con el mantenimiento, desarrollo o control de la relación contractual.

Ejemplo

el tratamiento de los datos relativos a la salud y los datos identificativos en la gestión y control del servicio médico de una empresa amparándose en el artículo 22 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

Artículo 22.1 «El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo. Esta vigilancia solo podrá llevarse a cabo cuando el trabajador preste su consentimiento. De este carácter voluntario solo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para este, para los demás trabajadores o para otras personas relacionadas con la empresa, o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad». Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales. TEXTO CONSOLIDADO. «BOE» núm. 269, de 10/11/1995. Acceso el 24/10/18.

Disponible en:

https://www.boe.es/buscar/act.php?id=BOE-A-1995-24292

Los requisitos exigidos para entender que el consentimiento es lícito están interrelacionados con el principio de transparencia y control, lo cual comporta que el RT debe ser capaz de demostrar que el interesado ha prestado su consentimiento conscientemente y para qué lo ha prestado; por ello, la declaración del interesado debe documentarse, a partir de un modelo de declaración elaborado previamente por el RT que tiene que cumplir las siguientes condiciones: inteligibilidad, fácil acceso, claridad y sencillez en el lenguaje, y que no contenga cláusulas abusivas, como podría ser el autorizar al RT a modificar unilateralmente (sin motivos válidos especificados en el documento) los términos de este; todo ello, en aplicación de la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores.

Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores. «DOCE» núm. 95, de 21 de abril de 1993, páginas 29 a 34 (6 págs.). Acceso el 24/10/18. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-1993-80526

El consentimiento «ha de proceder de una declaración o de una clara acción afirmativa del afectado» .

Proyecto de Ley orgánica de protección de datos personales y garantía de los derechos digitales. (621/000012) BOLETÍN OFICIAL DE LAS CORTES GENERALES SENADO. N. 289 de 23 de octubre de 2018. Acceso el 24/10/18. Disponible en: http://www.senado.es/legis12/publicaciones/pdf/senado/bocg/BOCG_D_12_289_2209.PDF

En conclusión, el consentimiento no se presume, sino que debe ser probado por el RT, el cual ha de crear las evidencias que demuestren quién lo ha prestado, cómo se ha prestado y para qué se ha prestado; debido a ello, el RT debe adoptar un sistema de gestión que proporcione el cumplimiento de dichos requisitos controlando las interrelaciones e interdependencias entre la documentación creada y asegurando su identificación, descripción, formato, medio de soporte, revisión y aprobación; así como controlar que esté disponible e idónea para el uso, para la cual ha sido creada, debiendo de adoptar las medidas organizativas y técnicas necesarias y proporcionales para proteger los datos personales, en beneficio de la confidencialidad y de la buena gestión.

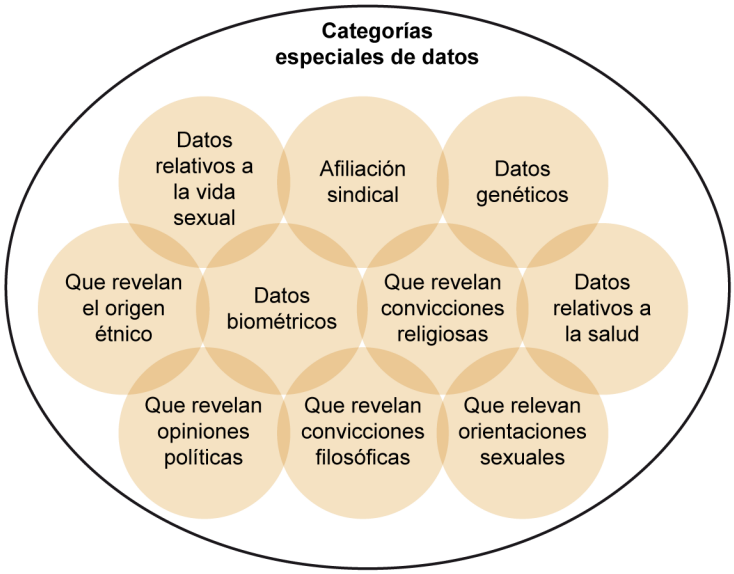
En ningún caso se entenderá prestado libremente, si entre el RT y el interesado existe un desequilibrio que lleve a que el segundo esté obligado a prestar su consentimiento por necesario para que se cumpla el contrato o la prestación del servicio.

Figura 2. Infografía sobre la protección de los datos personales

Fuente: Elaboración propia

1.2. Tratamiento de categorías especiales de datos

Figura 3. Categorías especiales de datos personales



Fuente: Elaboración propia

El artículo 9.1 del RGPD incluye en el conjunto de las categorías especiales de datos que tienen un tratamiento especial a los datos de salud, prohibiendo su tratamiento, salvo no sea de aplicación alguna de las excepciones recogidas en el apartado segundo del mismo artículo, entre las que destacaremos las que se recogen en las letras a, b), c), h), i) y j) :

> Artículo 9 del RGPD: «a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado; b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado; c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; (...) h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3; i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional, j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado».

a) El consentimiento será lícito si el propio interesado ha dado su consentimiento explícito y se han cumplido los requisitos anteriormente señalados para alguno de los fines especificados en el documento por el que el interesado presta su consentimiento.

b) Será lícito el tratamiento cuando el RT trata los datos personales para cumplir obligaciones, para ejercer derechos propios, o del propio interesado por razones relacionadas con el derecho laboral, de la seguridad social y protección social, si está el RT autorizado por la normativa aplicable, siempre y cuando el RT haya implantado las garantías en respeto de los derechos fundamentales y los propios intereses del interesado.

c) Cuando el interesado esté incapacitado judicialmente, o bien declarada su incapacidad administrativa, y el tratamiento de sus datos personales sea necesario para proteger bien los intereses vitales del interesado, o bien de otra persona física.

h) Cuando el tratamiento sea necesario por razones de medicina preventiva o laboral y aquellos fines, gestiones y tratamientos médicos relacionados con obligaciones médico-laborales del RT o la gestión de los sistemas y la asistencia sanitaria.

i) Ante razones de interés público (epidemias o amenazas a la salud), o bien para garantizar niveles de calidad y seguridad en la asistencia sanitaria y en los productos sanitarios.

> Artículo 2 letra l) «*Cualquier instrumento, dispositivo, equipo, programa informático, material u otro artículo, utilizado solo o en combinación, incluidos los programas informáticos destinados por su fabricante a finalidades específicas de diagnóstico y/o terapia y que intervengan en su buen funcionamiento, destinado por el fabricante a ser utilizado en seres humanos con fines de:*
>
> *1.º diagnóstico, prevención, control, tratamiento o alivio de una enfermedad;*
>
> *2.º diagnóstico, control, tratamiento, alivio o compensación de una lesión o de una deficiencia;*
>
> *3.º investigación, sustitución o modificación de la anatomía o de un proceso fisiológico;*
>
> *4.º regulación de la concepción,*
>
> *y que no ejerza la acción principal que se desee obtener en el interior o en la superficie del cuerpo humano por medios farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales medios»*. Real decreto legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios. TEXTO CONSOLIDADO.

j) Cuando el tratamiento sea necesario por fines de investigación. En tal caso tendrán que garantizarse los derechos y libertades de los interesados. El RT debe implementar las medidas organizativas y técnicas en respeto del principio

de minimización de los datos y que haya un tratamiento de datos en el que no podamos identificar al interesado (p.ej.: la seudonimización, que veremos posteriormente).

1.2.1. Principio de minimización de los datos

El principio de minimización de los datos se recoge en los artículos 5 y 25 del RGPD (que debe se garantizado su cumplimiento por el RT) está interrelacionado con:

- El principio de calidad de los datos que recoge el artículo 47.2, d) del RGPD y el principio de proporcionalidad y necesidad que regula la evaluación de impacto relativa a la protección de datos, la cual debe incluir, como mínimo «una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad».
- El principio de proporcionalidad: deben recogerse solo los datos necesarios para cada uno de los fines del tratamiento para los que se ha otorgado el consentimiento; tanto en relación con la cantidad de datos como con su plazo de conservación y accesibilidad.
- El principio de necesidad: solo se trataran los datos que sean necesarios para los fines específicos del tratamiento.

Deben recogerse los datos personales que se van a tratar, conservar durante el tiempo de tratamiento, tratarse para los fines declarados, acceder los que traten los datos

1.2.2. Seudonimización de los datos personales

La aplicación de la seudonimización se caracteriza por que el dato personal queda desvinculado del interesado, de modo que para llegar a la persona física identificada o que puede ser identificada es necesario que usemos información adicional, que figura separadamente, y está sujeta a medidas organizativas y técnicas destinadas a garantizar que los datos personales se atribuyan al interesado.

En la seudonimización, el dato personal se sustituye por un código, y la información adicional se almacena separadamente (medidas de custodia de la información), de modo que a partir del código no podamos llegar al interesado (reversión), salvo que usemos la tabla de datos donde consta el dato personal y el código (información adicional). Las técnicas más relevantes de seudonimización son las siguientes: cifrado de clave secreta, función *hash* (función que devuelve un valor de entrada: SHA-1:

Contenido complementario

Hashcodes (web). HASH CODES – versión 1.62. Programa de creación de código hash. Acceso el 24/10/18. Disponible en:

http://hashcodes.com/downloads.html

95F7056E82C1C74C2730ABB2ABC01D347CB0F4AD); función con clave almacenada; cifrado determinista o función *hash* con clave con borrado de clave o la descomposición en *tokens*.

Los principales y más relevantes riesgos del uso de la seudonimización son que se confunda la seudonimización con la anonimización, puesto que en el segundo caso no es posible vincular el dato con el interesado al que hubiese identificado y, por otro lado, que el proceso de reversión de la seudonimización lo realicen personas no autorizadas.

1.2.3. Consentimiento, datos de salud

El artículo 18 de la CE garantiza la intimidad, el secreto de las comunicaciones y la protección de datos como derechos fundamentales en nuestro ordenamiento jurídico, y así la Carta Magna en su artículo 18.1 recoge el derecho a la intimidad, el apartado 3 el secreto de las comunicaciones, mientras que el apartado 4 dice: «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

En consonancia con el derecho a la intimidad personal y familiar el Tribunal Europeo de Derechos Humanos en su sentencia de 25 de febrero de 1997 caso[3] Z v. Finlandia declaró que el respeto de confidencialidad de los datos de salud es un principio esencial que ampara el artículo 8 del Convenio europeo de derechos humanos, en amparo de la protección de la vida privada de los pacientes, y más cuando se trata de enfermedades como el hecho de ser seropositivo «cuya difusión puede conllevar consecuencias devastadoras sobre la vida privada y familiar de la persona en cuestión, y sobre su situación social y profesional, al exponerla al oprobio y a una amenaza de exclusión», y si bien el historial clínico cabe que sea incorporado a expedientes judiciales, no así que los datos personales del paciente (difusión de su identidad y seropositividad) se difundan en la sentencia que fue comunicada a la prensa, lo cual es una violación al respeto de la vida privada y familiar por parte del tribunal de apelación finlandés.

[3] http://hudoc.echr.coe.int/spa?i=001-163986

En el ámbito sanitario, el derecho a la intimidad personal está interrelacionado con la garantía a la protección a los datos de salud que profesionales de la salud y responsables del centro sanitario; están obligados a garantizar en cada una de las fases del tratamiento de los datos personales, desde la entrada del dato personal a su ámbito de control hasta su salida.

Y es que el concepto de dato personal de salud que recoge el RGPD en el considerando 35 es amplio y permite incluir información diversa sobre un individuo determinado; y así incluye en ese amplio abanico a

«todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro [...] la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia (...) todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica *in vitro*»

Por otra parte, la 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, en su artículo 3, define qué debemos entender por documentación clínica, historia clínica, información clínica e informe de alta médica; el denominador común es el hecho de que recogen datos sobre el estado físico y la salud de la persona a la que se le ha prestado asistencia médico-sanitaria. Por tanto, es en la documentación clínica, historia clínica, información clínica e informe de alta médica donde, principalmente, obrarán nuestros datos personales de salud, por lo que el principio básico, en cuanto al consentimiento, del RGPD, es que con anterioridad a la prestación de la asistencia médico-sanitaria el RT debe obtener el consentimiento e informar al interesado de la finalidad para la cual se recogen sus datos personales; sin olvidar que son de aplicación las excepciones ya señaladas en el apartado 2.2 del presente documento.

Contenido complementario

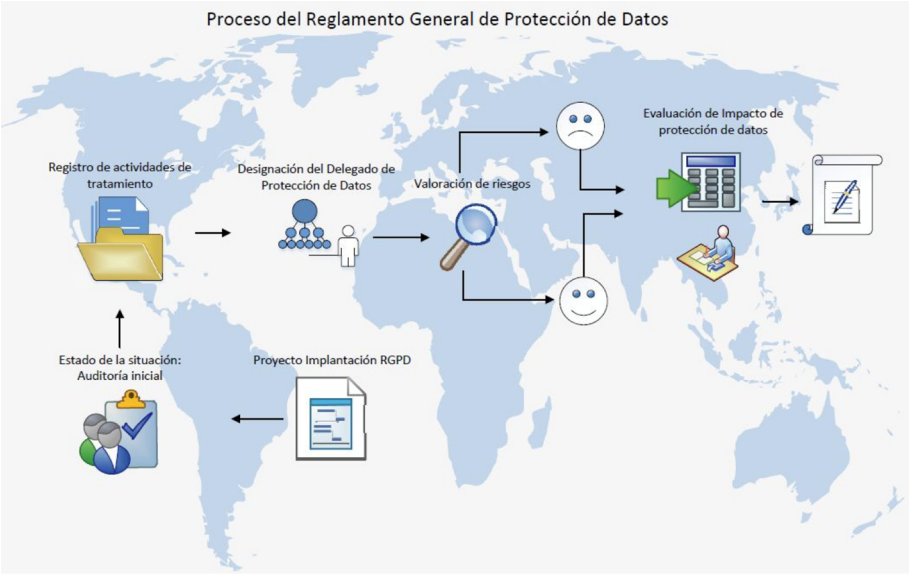
Artículo 3 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica:

«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.

Informe de alta médica: el documento emitido por el médico responsable en un centro sanitario al finalizar cada proceso asistencial de un paciente, que especifica los datos de este, un resumen de su historial clínico, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas».

Figura 4. La ruta del RGPD



Fuente: Elaboración propia

1.3. La historia clínica electrónica

La rápida evolución y el crecimiento exponencial de las nuevas tecnologías y de su uso está transformando la asistencia sanitaria que prestan los profesionales médico-sanitarios; y es que la expansión de los teléfonos inteligentes, las redes 4G y 5G, la fibra óptica y la disponibilidad de tecnologías de navega-

ción por satélite y el Internet de las cosas lleva a que se esté recabando información masiva sobre la actividad diaria (big data), el entorno en el que se halla el paciente, sus datos médicos, fisiológicos, modo de vida (dietas, ejercicio físico) facilitando de ese modo la ubicuidad de la información (acceso desde cualquier lugar y en cualquier momento).

El espíritu de la HCE es recopilar en un documento electrónico el conjunto de datos y documentos digitales médicos y sociosanitarios de actividades referentes a la salud con un horizonte temporal que abarque la vida del paciente, y que esté «alimentado» de modo continuo no solo por aquellos profesionales que prestan asistencia médico-sanitaria en el ámbito del servicio público sanitario, sino incluso por el propio paciente.

Si bien el objetivo de la HCE es un modelo de sanidad único y homogéneo en red, la actual diversidad de los sistemas sanitarios de los Estados miembros, y entre el propio Estado miembro (p. ej.: en España las CC. AA. tienen asumidas las competencias en materia de sanidad, según cuanto dispuesto por el artículo 148, 21.ª de la CE) están dificultando este objetivo principal. La falta de interoperabilidad de los sistemas de historiales médicos electrónicos es uno de los mayores obstáculos para la consecución de las ventajas económicas y sociales de la salud electrónica, y una falta de compromiso político estratégico común que parta de una clara y manifiesta cooperación activa de cada uno de los Estados miembros.

Ante esto, la Comisión Europea en la recomendación de 2 de julio de 2008[4] proporcionó un conjunto de orientaciones dirigidas a los países miembros que afectan al ámbito político, organizativo, técnico y semántico con la finalidad de desarrollar la implantación de sistemas de historiales médicos electrónicos interoperables que permitan el efectivo intercambio transfronterizo de datos sobre pacientes.

(4)Recomendación de la Comisión, de 2 de julio de 2008, sobre la interoperabilidad transfronteriza de los sistemas de historiales médicos electrónicos. (2008/594/CE). Diario Oficial de la Unión Europea. L 190/37. 18/07/08. Acceso el 03/11/18. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32008H0594#ntr1-L_2008190ES.01003701-E0001

Por desgracia, y seguramente no por obstáculos idiomáticos, sino más bien por razones políticas, económicas, organizativas y de gestión, hoy solo el ciudadano europeo tiene a su alcance la tarjeta sanitaria que, si bien, permite a los ciudadanos acceder a los servicios públicos sanitarios y a que se le preste tratamiento médico necesario durante una estancia temporal en otro país de la Unión Europea (UE), y ello en las mismas condiciones y beneficios que los ciudadanos del país donde se le presta la atención sanitaria; no así que el prestador del servicio médico sanitario conozca el historial médico del paciente; y ello, pese a que el Parlamento Europeo sea consciente de la necesidad de

una tarjeta sanitaria europea que permita el intercambio de la información de salud entre los distintos proveedores de los servicios sanitarios[5] , y que en último término redundaría en la reducción de los costes sanitarios.

(5)«El Parlamento Europeo (...) Principio 55. Pide a la Comisión que elabore normas técnicas y a los Gobiernos de los Estados miembros que sostengan activamente la instauración de sistemas de información interoperativos transparentes que permitan un intercambio y un reparto eficaces de la información sobre la salud entre prestadores de servicios sanitarios de distintos Estados miembros». Resolución del Parlamento Europeo, de 23 de mayo de 2007, sobre el impacto y las consecuencias de la exclusión de los servicios sanitarios de la Directiva relativa a los servicios en el mercado interior (2006/2275(INI)). Diario Oficial de la Unión Europea C102 E/279, (24/08/2008). Acceso el 03/11/18. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52007IP0201&from=ES

La garantía de la tutela de los ciudadanos y el principio de la libre circulación de personas que recoge el artículo 45 del Tratado de funcionamiento de la Unión Europea están en juego

La Comisión Europea es, por tanto, consciente del futuro de la sanidad móvil, de sus repercusiones en el derecho de los ciudadanos, y que los obstáculos no son solo los señalados, sino que también afectan a la intimidad y los datos de salud, puesto que no es baladí la inquietud que genera el tratamiento de los datos por las aplicaciones y dispositivos de sanidad móvil. La Comisión Europea, en abril de año 2014, publicó el Libro Verde sobre sanidad móvil, que analiza cuál es el potencial de la sanidad móvil y sus aspectos tecnológicos, y presenta las cuestiones sobre las que se solicitan las aportaciones de las partes interesadas, entre las cuales (en el punto 3.1) «La protección de datos, incluida la seguridad de los datos sanitarios»; recoge, asimismo, un listado de ejemplos de sanidad móvil los siguientes:

- dispositivos que integran la práctica de la medicina mediante el uso de las nuevas tecnologías;
- aplicaciones que pueden conectarse a dispositivos médicos o sensores;
- dispositivos de orientación personal, información sanitaria y recordatorios de medicación;
- y la telemedicina inalámbrica.

En el mismo año 2014 el Parlamento Europeo[6] instó a la Comisión a que publicase cada dos años un informe sobre el desarrollo de la aplicación del plan de acción sobre la salud electrónica 2012-2020 en los distintos Estados miembros. En el año 2015, la Comisión Europea informó al Parlamento Europeo y al Consejo sobre los avances y obstáculos del plan de acción sobre la salud electrónica 2012-2020[7] , destacando la propuesta de reglamento de protección de datos (aprobado el 4 de mayo de 2016, y de aplicación desde el 25 de mayo de

Contenido complementario

Tratado de Funcionamiento de la Unión Europea. VERSIÓN CONSOLIDADA. Diario Oficial n.° C 326 de 26/10/2012 p. 0001 - 0390

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012E/TXT&from=ES

Bibliografía

LIBRO VERDE sobre sanidad móvil de la Comisión Europea. COM (2014) 219 final (10/04/2014). Acceso el 04/11/18. Disponible en: http://ec.europa.eu/transparency/regdoc/rep/1/2014/ES/1-2014-219-ES-F1-1.Pdf

2018), el apoyo del mecanismo «Conectar Europa» (MCE) a las inversiones en la salud en línea, habiéndose asignado la financiación para poner en práctica el intercambio de historias clínicas de los pacientes, y las recetas electrónicas.

(6)Resolución del Parlamento Europeo, de 14 de enero de 2014, sobre el Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI (2013/2061(INI)) Diario Oficial de la Unión Europea (2016/C 482/03) (23/12/16). Acceso el 04/11/18. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52014IP0010(01)&from=ES

(7)Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI. Bruselas, 6.12.2012 COM (2012) 736 final. Acceso el 04/11/18. Disponible en:

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012DC0736&from=EN

1.3.1. Evaluación de impacto relativa a la protección de datos (EIPD)

La EIPD debe de encuadrarse en el contexto de aquellas medidas que el RT toma antes de iniciar las operaciones de tratamiento de los datos personales; es lo que el RGPD identifica como protección de datos desde el diseño (artículo 25), de modo que antes de definir las operaciones de tratamiento que llevar a cabo, y antes de determinar los medios que vamos a usar en el tratamiento de los datos personales hemos de tener en cuenta los principios, derechos y obligaciones que son de aplicación, desde el punto de vista de esa necesidad de gestionar los riesgos que las operaciones de tratamiento puedan comportar a los derechos y libertades fundamentales del interesado.

Características de la EIPD

Podemos definir la EIPD[8] , como una herramienta para prever la identificación, evaluación y gestión de los riesgos a los que están sujetas las actividades de tratamiento que realiza el RT, y que tiene como objetivo garantizar los derechos y libertades fundamentales del interesado, estableciendo las garantías, mecanismos, medidas de seguridad, organizativas y técnicas para reducir el riesgo hasta un nivel que se considere aceptable, para lo cual debe incluir (artículo 35.7 del RGPD):

(8)Agencia Española de Protección de Datos. Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD (monografía en Internet). Madrid. AEPD. [Acceso el 02/11/18]

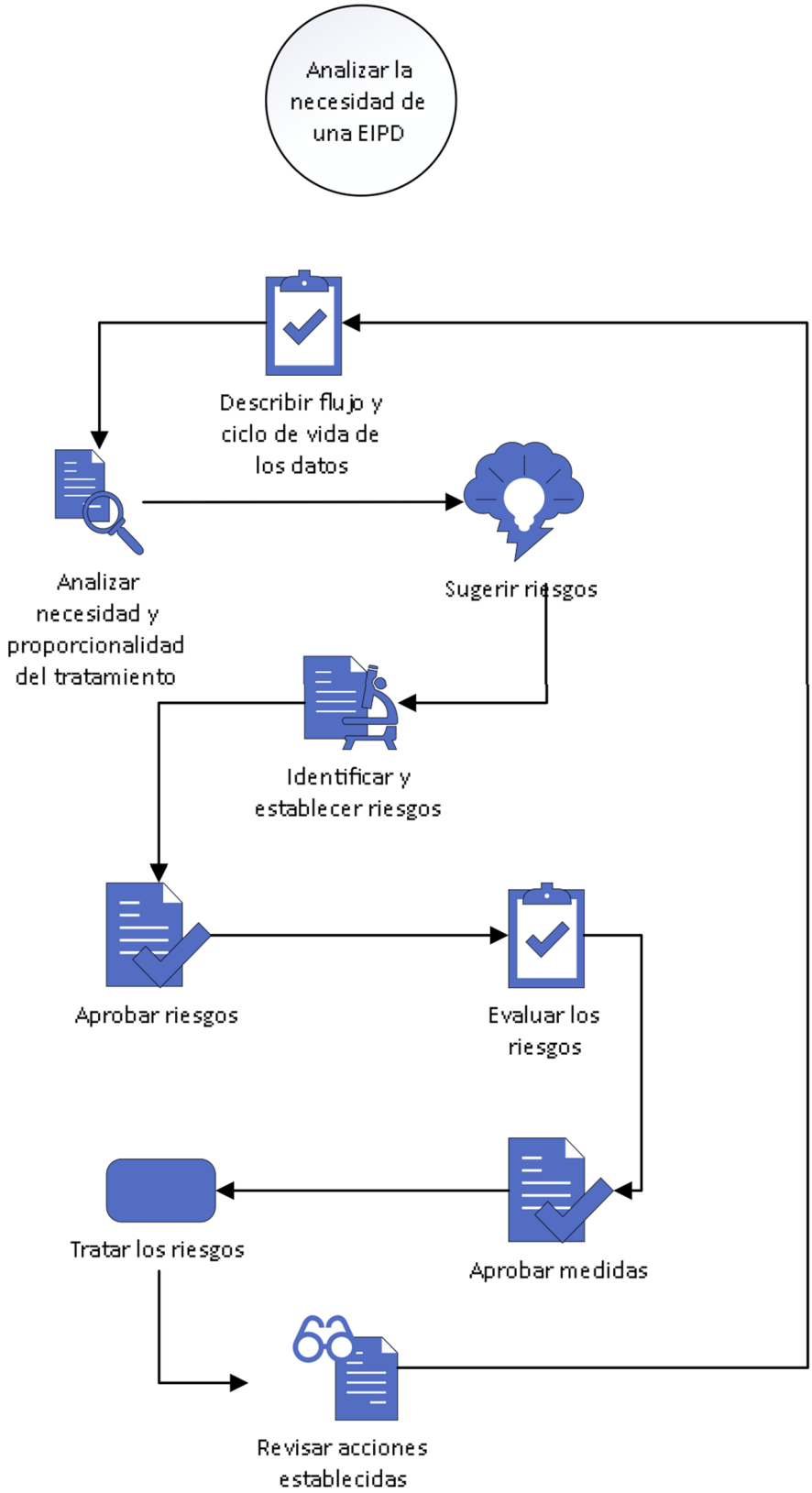
Disponible en:

https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

- Una descripción sistemática de la actividad de tratamiento prevista.
- Una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad.

- Una evaluación de los riesgos.
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

Figura 5. Flujo de proceso de elaboración de una EIPD



Fuente: Elaboración propia

El RT está obligado a realizar una EIPD, si bien el delegado de protección de datos (DPO) es el que proporcionará asesoramiento al RT y supervisará su aplicación que sea conforme con cuanto dispone el artículo 35 del RGPD.

Artículo 39.1 del RGPD. «Funciones del delegado de protección de datos 1. El delegado de protección de datos tendrá como mínimo las siguientes funciones: a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros; b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35; d) cooperar con la autoridad de control; e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto».

Bibliografía

Agencia Española de Protección de Datos*Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD*. [monografía en Internet]. Madrid: AEPD.

Parlamento Europeo (2012). *Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI*Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Bruselas, 6.12.2012 COM (2012) 736 final.

CEE (1993). Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores. *«DOCE»*, núm. 95, de 21 de abril de 1993, páginas 29 a 34 (6 págs.).

Constitución Española (1978). , «(TEXTO CONSOLIDADO) BOE» núm. 311, de 29/12/1978.

Contreras, Sebastián (2012). Ferrajoli y su teoría de los derechos fundamentales. *Estudios de filosofía práctica e historia de las ideas*, 14(2), 17-28.

EUROSTAT[base de datos en Internet] Oficina Europea de Estadística.

Grupo Protección de Datos (2017). Artículo 29. Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679. *WP 248 rev.01*. 4 de octubre de 2017.

Grupo Protección de datos (2015). Artículo 29. Dictamen 05/2014 sobre técnicas de anonimización. Págs. 22 y 23. 10/04/2015.

Hashcodes [web]. HASH CODES – versión 1.62. Programa de creación de código hash.

INE [base de datos en Internet] Instituto Nacional de Estadística.

Informe de la Comisión sobre el funcionamiento de la Directiva 2011/24/UE relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza. Bruselas, 4.9.2015. (2015)COM 421 final.

Instrumento de ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. «BOE» núm. 243, de 10 de octubre de 1979.

Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales. TEXTO CONSOLIDADO. «BOE» núm. 269, de 10/11/1995.

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. TEXTO CONSOLIDADO. «BOE» núm. 274, de 15/11/2002.

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.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. «BOE» núm. 298, de 14/12/1999.

LIBRO VERDE sobre sanidad móvil de la Comisión Europea. COM (2014) 219 final (10/04/2014)

Pérez Martínez, Jorge; Frías Barroso, Zoraida; Urueña López, Alberto (Mayo 2018). 50 años de la red de redes. La evolución de Internet en España: del Tesys a la economía digital. [Internet].*Red.es*. Madrid.

Proyecto de Ley orgánica de protección de datos personales y garantía de los derechos digitales. (621/000012) BOLETÍN OFICIAL DE LAS CORTES GENERALES SENADO. Núm. 289 de 23 de octubre de 2018

Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios. TEXTO CONSOLIDADO. «BOE» núm. 177, de 25/07/2015.

Recomendación de la Comisión, de 2 de julio de 2008, sobre la interoperabilidad transfronteriza de los sistemas de historiales médicos electrónicos. (2008/594/CE). Diario Oficial de la Unión Europea. L 190/37. 18/07/08.

RED (2018). Información general. [sede web]. *red.es*. Madrid.

Reglamento (CE) No 1338/2008 del Parlamento Europeo y del Consejo de 16 de diciembre de 2008 sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo. Diario Oficial de la Unión Europea. L 354/70 de 31 de diciembre de 2008.

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Diario Oficial de la Unión Europea (04/05/2016).

Resolución del Parlamento Europeo, de 14 de enero de 2014, sobre el Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI (2013/2061(INI)) Diario Oficial de la Unión Europea (2016/C 482/03) (23/12/16).

Resolución del Parlamento Europeo, de 23 de mayo de 2007, sobre el impacto y las consecuencias de la exclusión de los servicios sanitarios de la directiva relativa a los servicios en el mercado interior (2006/2275(INI)). Diario Oficial de la Unión Europea C102 E/279, (24/08/2008).

Rivero, Raúl (2002). Evolución de Internet en España. *elmundo*. [sede web]. Madrid.

Tratado de Funcionamiento de la Unión Europea. VERSIÓN CONSOLIDADA. Diario Oficial núm. C 326 de 26/10/2012 p. 0001 – 0390.

Unión Europea La Carta de los Derechos Fundamentales de la Unión Europea (2010/C 83/02). *Diario Oficial de la Unión Europea*, C83/389, (30/03/2010).