FACULTAD DE DERECHO UNIVERSIDAD DE LEÓN

CURSO 2022/ 2023

TRATAMIENTO AUTOMATIZADO DE DATOS DE SALUD: PRINCIPIOS Y GARANTÍAS

AUTOMATED PROCESSING OF HEALTH DATA: PRINCIPLES AND SAFEGUARDS

MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTOR/A: D. ENRIQUE ROBLES SANTOS.

TUTOR/A: DÑA. SUSANA RODRÍGUEZ ESCANCIANO.

ÍNDICE

1. INTRODUCCIÓN.

La normativa de la CE tiene una especial importancia en nuestro día a día. Una de las funciones principales de esta normativa es garantizar el derecho a la intimidad de la persona, derecho regulado en el artículo 18, y garantizar el derecho a la protección de datos, encontrándose este en el punto 4 del mismo artículo. Estos derechos han sido reconocidos tradicionalmente, pero con el paso de los años han sufrido evoluciones, esto es debido al avance de las Tecnologías de la información y la Comunicación y el poder que tienen en la sociedad actual.

La aparición de internet y de las tecnologías han traído muchas cosas positivas a nuestra sociedad, ya que a través de estos mecanismos se nos permite aglutinar una gran cantidad de datos. Aunque, la aparición de estas no solo ha supuesto cosas positivas, ya que un mal uso de ellas puede dañar considerablemente los derechos fundamentales.

La tecnología ha ido entrando directamente en todos los ámbitos de la sociedad, y como no iba a ser otro, ha ido entrando masivamente en el ámbito laboral, especialmente, en el ámbito de la salud. El personal sanitario ha sido participe de esta modificación, ya que se ha cambiado completamente la forma en la que venían trabajado, y es que actualmente casi todo se encuentra digitalizado. Por lo que, vemos un gran número de datos tratados por estos profesionales, datos que afectan a la esfera más íntima de la persona, ya que son datos de carácter personal especialmente protegidos.

Los datos de salud, al ser estos datos de carácter personal, necesitan de una especial protección. Los profesionales sanitarios, que intervengan en el tratamiento de estos datos, tendrán que guardar secreto de toda la información que obtengan debido a la relación médico-paciente, siendo sancionados aquellos que incumplan con este deber, pudiendo incurrir, en el caso más grave, en sanciones penales.

Es importante que haya un sistema eficaz, que sea completo e integral dentro de la protección de los datos del paciente, para poder preservar toda la información obtenida de este.

Más adelante, se analizará la evolución que ha sufrido la nueva normativa de protección de datos, describiendo uno por uno los derechos que podrán ejercitar los pacientes para modificar el tratamiento que se está dando a sus datos, centrándonos, por la temática del trabajo, en el ámbito sanitario.

2. ABREVIATURAS

- **AEPD:** Agencia Española de protección de datos.
- **BOE:** Boletín Oficial del Estado.
- **CE**: Constitución Española.
- **CDFUE**: Carta de los derechos fundamentales de la Unión Europea.
- **Convenio nº108**: Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
- **Derechos ARCO**: Derecho de acceso, rectificación, cancelación y oposición.
- **DPO**: Delegado de Protección de Datos.
- **LBAP**: Ley Básica de Autonomía del Paciente.
- **LGS**: Ley General de Salud.
- **LOPDGDD**: Ley Orgánica 3/2018, de 5 de septiembre de Protección de Datos y Garantía de los Derechos Digitales.
- **OMS:** Organización Mundial de la Salud.
- **RGPD**: Reglamento (UE) 2016/676 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 General de Protección de datos.
- **TEDH:** Tribunal Europeo de Derechos Humanos.
- **TFUE:** Tratado de Funcionamiento de la Unión Europea.
- **TJCE**: Tribunal de Justicia de la Unión Europea.

3. RESUMEN/ABSTRACT.

RESUMEN

Especial importancia tienen en el ámbito sanitario el derecho a la intimidad y el derecho a la protección de datos. Es por esto por lo que, los datos de salud son datos que necesitan de una protección especial, teniendo como normativa jurídica para regular su tratamiento el reglamento y la ley de protección de datos.

Los datos de salud, con normalidad, se encuentran almacenados en la historia clínica. En este sistema de almacenamiento se encuentran datos relevantes del paciente. Las personas que accedan a estos tendrán que guardar el deber de secreto y la de confidencialidad de los mismos. Es importante evitar intromisiones ilegítimas de personas que no tengan autorización para acceder a los datos tratados.

El hecho de que terceros puedan acceder al historial clínico puede llegar a suponer un grave perjuicio para el paciente. Aquellas personas que accedan sin la debida autorización podrán tener sanciones, pudiendo llegar, como mencionamos anteriormente, al ámbito penal.

Es por esto por lo que, es fundamental que todas las personas que traten estos datos conozcan la normativa vigente de protección de datos. También es importante que el paciente conozca la actual normativa de protección de datos y los derechos que podrá ejercitar, en cualquier momento y sin tener que justificar ningún motivo. Estos derechos son: el derecho de acceso, rectificación, cancelación, oposición, limitación del tratamiento, supresión y portabilidad.

PALABRAS CLAVE: Ámbito sanitario, derecho a la intimidad, derecho a la protección de datos, Confidencialidad, Deber de secreto, Historial Clínica, Intromisión Ilegítima, Derechos de los pacientes.

ABSTRACT

The right to privacy and the right to data protection are of particular importance in the field of healthcare. For this reason, health data are data that require special protection, and the legal regulations governing their processing are the data protection regulations and the data protection law.

Health data are normally stored in medical records. This storage system contains relevant patient data. Persons who have access to this data are obliged to maintain secrecy and confidentiality. It is important to avoid unlawful intrusions by unauthorised persons.

The fact that third parties have access to the medical records is a serious detriment to the patient. Those who gain access without due authorisation will be subject to sanctions, and as mentioned above, these sanctions may even go as far as criminal sanctions.

For this reason, it is essential that all persons who process this data are aware of the current data protection regulations. It is also important that the patient is aware of the current data protection regulations and the rights that can be exercised at any time and without having to justify the reason. These rights are: The right of access, rectification, cancellation, opposition, limitation of processing, deletion and portability.

KEYWORDS: Healthcare, right to privacy, right to data protection, confidentiality, duty of secrecy, medical records, unlawful intrusion, patients' rights.

4. OBJETIVOS.

El objetivo del presente estudio es analizar el avance de las nuevas tecnologías y la importancia que tiene proteger al ciudadano contra esta evolución, ya que su intimidad se puede ver más desprotegida. Prestaremos especial atención a la nueva normativa que regula la protección de datos, analizándola desde una vista general hacia un punto más concreto como es el ámbito sanitario.

En relación con el contenido del presente trabajo fin de máster, se verá como son tratados los datos personales en el ámbito sanitario y que derechos se pueden ver afectados cuando se tratan estos datos.

A continuación, analizaremos qué personas están legitimadas para poder acceder y tratar estos datos personales, cuánto tiempo podrán ser tratados y qué ocurrirá a aquellas personas que accedan a estos datos sin consentimiento del titular y sin tener que acceder por motivo de su profesión. En cada apartado, analizaremos doctrina judicial española e internacional, destacando aquellas sentencias que han sido de especial interés. También, veremos aquellas resoluciones de la Agencia Española de Protección de Datos en las que constará alguna sanción económica y administrativa por intromisión ilegítima.

Posteriormente, analizaremos los derechos que pueden ejercitar los titulares de los datos que son tratados, profundizando en cada uno de ellos y describiendo como sería ejercer este derecho en el ámbito de la salud.

Por último, llevaremos a cabo unas conclusiones donde pondremos en práctica lo aprendido a la hora de realizar nuestro trabajo expresando, así, nuestra propia opinión

5. METODOLOGÍA.

A la hora de realizar el presente trabajo, se ha llevado a cabo un análisis jurídico-teórico para poder encontrar así el componente teórico más relevante, en relación con esta materia. Hemos seguido lo siguientes pasos:

A la hora de elegir el tema, nos centramos en el nuevo reglamento y ley de protección de datos, y más concretamente en el ámbito sanitario, ya que desde el primer momento es el tema que más interés me ha despertado desde que inicie el máster en derecho de la ciberseguridad y entorno digital.

La investigación jurídica llevada a cabo se basa en analizar toda la legislación actual referente a este tema, y para ello, es importante, localizar aquellos autores expertos en la protección de datos y, más concretamente, en el ámbito sanitario.

La metodología utilizada ha sido descriptiva y analítica, para poder desarrollar, así, lo mejor posible la protección de los datos de salud.

La investigación se compone de 4 pasos:

1. Encontrar toda la legislación actual relacionado con el tema a tratar.
2. Conocer que interpretación dan los Tribunales y Jueces a la norma.
3. Analizar situaciones de carácter práctico.
4. Descubrir opiniones de carácter crítico.

6. APROXIMACIÓN AL DERECHO A LA PROTECCIÓN DE DATOS.

Cada día crece más el interés en el manejo de los datos debido al gran crecimiento que está teniendo. Cuando tratamos datos estamos asumiendo unos riesgos. Estos riesgos pueden ser muy elevados, sobre todo si se tratan datos especialmente protegidos, como pueden ser los datos de salud.

La protección de datos es una asignatura que está creciendo exponencialmente en nuestro día a día. Esto es gracias a la evolución de las tecnologías en nuestra sociedad. La evolución notoria hace que el legislador quiera proteger con mayor fuerza la intimidad de las personas, derecho fundamental protegido por el artículo 18.1 de nuestra Carta Magna, es decir nuestra Constitución Española (en adelante, CE).

En el año 2016, más concretamente el 25 de mayo, surgieron notables cambios con el nuevo reglamento de protección de datos, "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" (en adelante, RGPD).

El fin de este reglamento es "garantizar a nivel uniforme y elevado de protección de las personas físicas"[1] con la intención de minimizar las posibles desigualdades de los Estados miembros que resultaron de la transposición de la actualmente derogada Directiva 95/46/UE en relación con el nivel de su tutela[2]. El legislador consideraba que se apreciaban grandes

[1] Considerando 10 RGPD

[2] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

diferencias, ya que había una gran obstaculación para la circulación de datos en la Unión, hecho que repercutía negativamente a la hora de explotar actividades de carácter económico[3].

Para poder cumplir estas misiones, el instrumento jurídico elegido fue un Reglamento, ya que tiene una ventaja respecto a otros instrumentos, como puede ser las Directiva. El reglamento tienes unas características muy marcadas. El Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE) señala que el reglamento es "obligatorio en todos sus elementos y directamente aplicable en cada estado miembro".[4]

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) fue publicada en el Boletín Oficial del Estado (en adelante, BOE) el día 6 de diciembre del año 2018. El objetivo principal era acercar nuestro ordenamiento jurídico al RGPD. Esta Ley también se aprobó con la intención de garantizar los derechos digitales recogidos en el artículo 18.4 de la CE.

El artículo 18.4 de la CE establece que "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". Nuestro ordenamiento jurídico, en su norma suprema, no hace un reconocimiento directo a la protección de datos como derecho fundamental, pero sí se encuentra explícitamente en el artículo 8 de la Carta Europea de Derechos Fundamentales:

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

[3] El objetivo es conseguir un mercado digital único.CANTERO MANTERO, J.: "La liberalización de la asistencia sanitaria transfronteriza en Europa", Aranzadi, 2017, BIB 2017\434555

[4] Artículo 288 del TFUE.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente"[5].

6.1. EL DERECHO A LA INTIMIDAD EN RELACIÓN CON LA PROTECCIÓN DE DATOS.

Antes de analizar los datos personales que estén relacionados con los datos de salud, es necesario analizar, en mayor profundidad, el derecho a la intimidad, ya que es un derecho esencial de la persona. Por lo que, subsidiariamente estará relacionado con el derecho a la protección de datos personales.

Como mencionamos anteriormente, la CE menciona que el derecho a la intimidad es un derecho fundamental, derivado de la propia dignidad de la persona y asociado con la propia personalidad[6]. El TC agrupa el derecho a la intimidad, pero lo diferencia en cuatro apartados: En su apartado 1 habla del derecho a la intimidad, honor y propia imagen; en su apartado 2 y 3 habla de la inviolabilidad del domicilio y secreto de las comunicaciones; y en el último apartado menciona el uso de la informática. La intimidad es un derecho fundamental, ya que es un derecho que se refiere a la vida privada de la persona[7].También menciona en el artículo 20 dos derechos más; como son el derecho a la información y el secreto profesional.

Estos derechos ostentan la expresión máxima de la dignidad humana, no siendo posible renunciar a estos sin que puedan afectar a la condición de persona. Estos derechos se encuentran dentro de la personalidad, así lo establece el TC "(…) aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la

[5] ORTÍ VALLEJO, A.: "Derecho a la intimidad e informática" (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada); edit. Comares, Granada, 1994, pág. 109 y ss; ORDÁS ALONSO, M.: "Intimidad, secreto médico y protección de datos sanitarios" en GARCÍA AMADO, J.A. (Coord.).: "Razonar sobre derechos", Tirant lo Blanch, Valencia, 2016, pág. 781 y ss

[6] GUTIÉRREZ GUTIÉRREZ, I.: "Dignidad de la persona y derechos fundamentales", Marcial Pons, Madrid, 2005, Pág.85.

[7] REBOLLO DELGADO, L.: "Derechos de la personalidad y datos personales", Revista de Derecho Público, 1998, pág. 158.

«dignidad de la persona», que reconoce el art. 10 de la C.E., y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario -según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana. Se muestran así esos derechos como personalísimos y ligados a la misma existencia del individuo (…)"[8].

Los derechos a la intimidad familiar y personal y a la imagen son "derechos personalísimos y ligados a la existencia misma del individuo". Queremos destacar una sentencia del TC que marca un antes y un después a la hora de interpretar el derecho a la intimidad. Esta sentencia estable que "debe estimarse que, en principio, el derecho a la intimidad personal y familiar se extiende, no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar; aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18 de la C.E. protegen. ...Por lo que existe al respecto un derecho -propio, y no ajeno- a la intimidad, constitucionalmente protegible"[9].

En esta sentencia se recoge un derecho a la vida privada, hecho que hace que se extienda la interpretación del artículo 18.1 de la CE, ya no solo va a incluir su vida privada, sino que va a incluir también la de su familia[10][11]. Se integraría todo lo que tiene que ver con la intimidad de una persona, es decir, aquello que consideramos privado, como pueden ser relaciones de amistad, relaciones interpersonales, etc[12].

[8] Sentencia del Tribunal Constitucional, nº 231/1988, de 2 de diciembre, Fundamento Jurídico 3.
[9] Sentencia del Tribunal Constitucional, nº196/2004, de 15 de noviembre, Fundamento Jurídico 4.
[10] SUÁREZ RUBIO, M.J.: "Constitución y privacidad sanitaria", Tirant Lo Blanc, Valencia, 2017, pág. 53, con cita de DÍEZ-PICAZO GIMÉNEZ, L.M.: "Sistema de Derechos fundamentales", Thompson, Madrid, 2013, pág. 41 y 42.
[11] STC 231/1988, de 2 de diciembre, STC 197/1991 y STC 197/1991, de 17 de octubre
[12] FERNÁNDEZ-RUIZ GÁLVEZ, E.: "Intimidad y confidencialidad en la relación clínica", Servicio de Publicaciones de la Universidad de Navarra, Persona y Derecho, Pamplona, 2013, págs. 61-63.

6.2. LA PROTECCIÓN DE DATOS COMO DERECHO AUTÓNOMO FRENTE A LA INTIMIDAD.

La protección de datos es un derecho autónomo e independiente. El objetivo principal de la LOPDGDD es preservar la intimidad de las personas. Es importante remarcar que la protección que quiere dar la LOPDGDD es global y amplia, abarcando todos aquellos aspectos que tengan que ver con el honor y la intimidad[13]. Esta garantía se amplía a los datos de carácter personal y a la información personal, independientemente de si tienen carácter íntimo o no:

"(…) el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal".

"También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"[14].

Es importante mencionar la diferencia entre privacidad e intimidad. La privacidad abarca más aspectos que la intimidad. La intimidad integra aspectos de la vida privada, es decir tiene un carácter más restrictivo si lo comparamos con la privacidad. Dentro de la privacidad

[13] SERRANO PÉREZ, M.M.: "El derecho fundamental a la protección de datos. Derecho español Comparado", Aranzadi, Pamplona 2004, pág. 33 y ss.
[14] Sentencia del Tribunal Constitucional nª 292/2002 de 30 de noviembre de 2002. (Fundamento jurídico 6.)

podríamos abarcar todos aquellos datos que sean personales, independientemente de si son datos íntimos o no.

El Tribunal Europeo de Derechos Humanos (en adelante, TEDH) ha desglosado la expresión de "vida privada", ampliando más aspectos de la vida personal que se deben proteger, incluyéndose:

1. Comunicaciones entre dos o más personas, siendo estas realizadas de forma verbal.
2. Nombre y apellidos, ya que a través de ellos se puede llegar a conocer la identidad de la persona
3. Nuevos derechos, como son el derecho al honor personal y a la propia imagen, para poder preservar así la dignidad de las personas.
4. Datos personales que se pueden encontrar a través de plataformas tecnológicas, dándole mayor relevancia, en nuestro caso, a aquellos datos de carácter sanitario.
5. La integridad de la persona, abarcando tanto la física como la psíquica. En el ámbito sanitario es necesario que el paciente de consentimiento antes de realizar cualquier tipo de intervención médica en la que puede verse afectado. También, incluye el derecho de cualquier persona a poder decidir libremente su orientación sexual, añadiendo la libertad que tiene toda personal a la hora de mantener relaciones de carácter sexual[15].
6. El libre desarrollo de la persona en relación con el estilo de vida. Este desarrollo abarca relaciones de carácter interpersonal, incluyendo el ámbito laboral y el familiar y personal. El TEDH ve imposible diferenciar el ámbito personal del ámbito laboral, así lo ha expresado en alguna de sus sentencias[16].

[15] Sentencia del Tribunal Europeo de Derechos de 22 de octubre de 1981, caso Dudgeon y 26 de octubre de 1988, caso Norris.

[16] Sentencia del Tribunal Europeo de Derechos de 16 de diciembre de 1992, caso Niemietz y 16 de diciembre de 2000, caso Amann.

6.3. DISPARIDAD ENTRE EL DERECHO A LA INTIMIDAD Y EL DERECHO A LA PROTECCIÓN DE DATOS.

La diferencia principal es el objeto de protección. El derecho de protección de datos no incluye solo datos de carácter íntimo, sino que incluye "cualquier tipo de dato personal, sea íntimo o no, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos", abarcando todos aquellos datos que nos permitan identificar a una persona. La sentencia nª292/2000 del Tribunal Constitucional señalaba que la protección de datos incluía, también, "aquellos datos que identifiquen o permitan la identificación de la persona, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo"[17].

La principal diferencia entre ambos derechos reside en "su distinta función, lo que apareja que su objeto y contenido difieran"[18]. Ambos derechos tienen el mismo objetivo y es preservar la vida privada personal y familiar del individuo. El derecho a la intimidad tiene como objetivo proteger al individuo de futuras intromisiones que pueda sufrir por un tercero en el ámbito personal, mientras que "el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derechos del afectado"[19].

El derecho de a la protección de datos "(…) amplia la garantía constitucional a aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos

[17] Sentencia del Tribunal Constitucional nº 292/2000 de 30 de noviembre (Fundamento jurídico 6).
[18] GARRIGA GONZÁLEZ, A., citando a DENNINGER, E.: "El derecho a la autodeterminación informativa", en PÉREZ LUÑO, A., E.: "Problemas actuales de documentación y la información jurídica", Tecnos, Madrid, 1987, pág. 273., asimismo, CONDE ORTIZ, C.: "La protección de datos personales. Un derecho con base en los conceptos de intimidad y privacidad", Dykinson, Madrid, 2005, págs.19-23.
[19] Sentencia del Tribunal Constitucional 292/2000 (Fundamento jurídico 6).

de las personas, sean o no constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro bien constitucionalmente amparado"[20].

7. CATEGORÍAS ESPECIALES DE DATOS PERSONALES.

Es por ello por lo que, entre la categoría de datos especialmente sensibles se encuentran los datos de salud. Tal enunciado exige parar la atención en su definición, haciendo referencia también a algunas categorías afines como los datos médicos, los datos biométricos, los datos genéticos. Analizaremos que similitudes y diferencias hay entre estos datos, para que podamos entender mejor cuando estamos hablando de un dato y de otro.

7.1 DATOS SENSIBLES ESPECIALMENTE PROTEGIDOS.

Los datos sensibles especialmente protegidos son aquellos que tiene que recibir una protección especial. Como norma general son aquellos datos que "revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales"[21].

Anteriormente estos datos se llamaban "datos especialmente protegidos", así lo recogía la LOPD, ley que no se encuentra vigente en la actualidad. Actualmente han pasado a llamarse "categoría especial de datos", así viene establecido en el artículo 9 del RGPD, como en el artículo 9 del LOPDGDD.

[20] Sentencia del Tribunal Constitucional nº96/2012 de 7 de mayo de 2012.

[21] Así lo establece el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 (en adelante, Convenio nº108)

Con la aparición del nuevo RGPD y la LOPDGDD se ha logrado aumentar el contenido de estos datos. Anteriormente, el artículo 7 punto 1 de la LOPD mencionaba que "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias" y el artículo 7 punto 4 mencionaba que "estaba totalmente prohibido el tratamiento de datos relativo al origen racial, salud y vida sexual". Pues actualmente, se prohíbe "el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida o las orientaciones sexuales de una persona física"[2223].

Como norma general, se prohíbe el tratamiento de estos datos, pero existe una excepción a esta norma:

"(…), entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales"[24].

"(…) cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud"[25].

[22] Artículo 9 del RGPD.
[23] El RGPD también hace mención a la protección especial que tienen que tener estos datos. El considerando 51 estable que "especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales".
[24] Considerando 51 del RGPD.
[25] Considerando 52 del RGPD.

Existen situaciones donde el consentimiento del interesado no será lo suficiente. Para ello, es necesario que tanto el Derecho de la Unión como el de los Estados que pertenezcan a la Unión lo prohíban, teniendo que prohibirlo de una forma específica. La LOPDGDD hace referencia a lo mencionado en este párrafo, estableciendo que "el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico"[26].

El RGPD contempla excepciones a las prohibiciones a las que hacíamos mención anteriormente en el texto, pero se podrán tratar datos siempre y cuando sean necesarios: "para fines de medicina preventiva o laboral, para aquellos que sean imprescindibles para cumplir con la legislación laboral o de seguridad social, aquellos datos que el interesado haya hecho públicos, para celebrar cualquier acto de carácter judicial, ya sea para reclamar o para poder ejercer su defensa, para poder proteger intereses del interesado o de cualquier otra persona jurídica, en el supuesto de que el interesado no esté capacitado para otorgar ese consentimiento y para aquellos supuestos en los que el tratamiento de datos sea realizado por una organización que actúe sin ánimo de lucro, con finalidad política, religiosa o sindical en relación con sus fines"[27].

7.2. DATOS PERSONALES RELATIVOS A LA SALUD DE LOS PACIENTES.

En el artículo 4 del RGPD aparecen unas enumeraciones de definiciones que son utilizadas a posteriori según va transcurriendo su articulado. El punto 1 del artículo 4 ofrece una definición de datos personales[28], considerando dato personal "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física

[26] Artículo 9 de la LOPDGDD.
[27] SANCHEZ CARO, J.: "Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales", 2021, págs. 1181-1200
[28] ROMEO CASABONA, C.M.: "Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal", Aranzadi, 2010, págs. 226-256.

identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"[29]. A la hora de interpretar este artículo, llegamos a la conclusión de que este precepto excluye los datos personales de todas aquellas personas que hayan fallecido[30], sin perjuicio de la protección prevista en la legislación nacional.

Notoria diferencia podemos encontrar entre dato anónimo y dato seudonimizado. La seudonimización es "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona identificada o identificable"[31], mientras que un dato anónimo es aquel donde no se revela, en ningún momento, la identidad de la persona.

Se considera tratamiento a "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"[32]. También tienen consideración de tratamiento los tratamientos que sean automatizados y manuales.

[29] Cabe destacar la Sentencia del Tribunal de Justicia de la Unión Europea de 20 de diciembre del 2017 (C-434/16) en la que se considera las respuestas de un examen como dato personal, al igual que los comentarios realizados en el examen por la persona encargada de corregirlo. En la Sentencia del Tribunal de Justicia de la Unión Europea de 30 mayo de 2013 (C-342/12) se consideró dato personal al control de horas de los trabajadores que realice el empresario.

[30] Así lo establece el RGPD en el Considerando 24 y 160.

[31] Así viene definido en el RGPD, más concretamente en su artículo 4 punto 5.

[32] Así lo establece el artículo 4 punto del RGPD.

Una de las obligaciones de nuestro Derecho debe de ser garantizar la protección de las personas, dotándolas de condiciones óptimas de salud y asistencia sanitaria, teniendo que respetar, en todo momento, el ámbito privado de las personas que se sometan a este tipo de tratamiento y a la legislación actual.

Ninguna persona podrá ser discriminada por tener una enfermedad. Por lo que, habrá que "promover el derecho a la igualdad de trato y no discriminación, respetar la igual dignidad de las personas"[33].

La protección de la salud está correlacionada con la protección de datos de carácter personal. Poco a poco iremos detallando la importancia de su utilización. La salud puede considerarse como "un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades"[34].

Los datos de carácter personal relativos a la salud incluyen "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo"[35]. A parte de toda la información comentada en este párrafo, también nos podemos encontrar, a la hora de tratar datos de salud, información de personas enfermas o fallecidas, incluyendo informaciones que estén relacionadas con la consumición de drogas y alcohol[36].

Otra definición que queremos destacar es la de "datos médicos", estos datos "hacen referencia a todos los datos de carácter personal relativos a la salud de una persona, afectando igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas"[37].

[33] Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación
[34] Definición aportada por la Organización Mundial de la Salud (en adelante, OMS),
[35] Apartado 45 del Convenio 108 referente a la Memoria Explicativa.
[36] Son considerados datos personales relativos a la salud de las personas los datos donde se aprecia una minusvalía de un sujeto, al igual que aquellos que valoren la aptitud para desempeñar una actividad laboral. (Informe de la AEPD nº0445/2009)-
[37] Recomendación R (97) 5, del Comité de ministros del Consejo de Europa.

Anteriormente, a la hora de hablar de datos de salud, se hablaba de "datos relativos de salud"[38] y no de "datos relativos a la salud de las personas". El Tribunal de Justicia de la Unión Europea (en adelante, TJCE)[39] apreciaba que esta definición debía de ampliarse, ya que consideraba que tendría que comprender toda la información relacionada con la salud de una persona, aglutinando aspectos de carácter físico y psíquico.

El RGPD, también, menciona los "datos relativos a la salud". Como hemos mencionado anteriormente, considera que este tipo de datos tienen que disfrutar de una protección especial. Se entiende por "datos relativos de salud" a aquellos "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud"[40].

A la luz de tales previsiones, el contenido que se trata en la actualidad es mucho más extenso[41], no solo incluye aquellos datos que correspondan con la salud de una persona, sino que, también, incluye aquellos datos que aporten información sobre "el estado de salud".

El "estado de salud" se encuentra regulado en el RGPD estableciendo que "entre los datos personales relativos a la salud se deben incluir 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.

Se incluye 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, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo (1); "todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca

[38] Así lo establecía la Directiva 95/46 CE (Directiva derogada)

[39] Sentencia del Tribunal de Justicia de las Comunidades Europeas de 6 de noviembre de 2003, caso Sra. Lindqvist (C-101/0). Un trabajador que se encontraba en situación de incapacidad temporal había sufrido una lesión en el pie, consultó al tribunal si la información que contenía la baja constituía un dato personal relativo a la salud. El Tribunal declaró que, efectivamente, se consideraba de un dato personal relativo a la salud.

[40] Artículo 4 punto 15 del RGPD.

[41] GT29, Health data in apps and devices. 2015, pág. 2.

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"[42].

El RGPG hace mención del término de "salud pública" y todo aquello que abarca e incluye " (…) debe interpretarse todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad (…)"[43].

Fuerte relación tiene los datos médicos con los datos genéticos[44]. Los datos médicos son aquellos datos relacionados con la salud o estado de un individuo, mientras que los segundos son aquellos que se heredan de otra persona o de varias personas con las que se guarde una relación de consanguinidad[45].

El RGPD considera a los datos genéticos una subclase de los datos de salud, mencionando que son considerados datos genéticos "(…) los datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una

[42] Considerando 35 del RGPD.
[43] Considerando 54 del RGPD.
[44] SÁNCHEZ-CARO, J. y ABELLÁN, F.: "Datos de salud y datos genéticos", Derecho Sanitario Asesores, Granada, 2004, págs. 103-111.
[45] COLLADO GARCÍA-LAJARA, E., Protección de datos de carácter personal (legislación, comentarios, concordancias y jurisprudencia), Comares, Granada 2000, pág. 25.

información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona"[46].

Aunque, los datos genéticos no solo hacen remisión a la salud, ya que algunos dan información en relación con las peculiaridades físicas del individuo en cuestión. Por ejemplo: el tono de la piel, el color del pelo, la sexualidad o el origen étnico[47].

Los datos genéticos nos pueden proporcionar: Información relacionada con una persona física, información relacionada con la salud y un análisis que contenga una muestra de carácter biológico de una persona[48].

No es novedoso la evolución de los instrumentos tecnológicos en el día a día de las personas, esta situación hace que continuamente se estén generando un gran número de datos que tendrán que ser regulados conforme a la normativa de protección de datos de carácter personal[49]. Por ejemplo, también se considera datos personales las posibles huellas encontradas en un lugar donde se haya cometido un crimen[50].

Los datos biométricos no son considerados datos de salud, pero tienen similitudes con estos, ya que reciben una protección similar[51]. El RGPD define datos biométricos a aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos"[52].

---

[46] Artículo 4 punto 13 del RGPD.

[47] SÁNCHEZ URRUTIA, A.V.: "Información genética, intimidad y discriminación", Acta Bioética, 2002.

[48] DE MIGUEL BERIAIN y DE LORENZO Y APARICIO.: "Claves prácticas sanitarias". Datos genéticos, 2020, pág. 31,

[49] Según el Grupo europeo de ética de las ciencias y de las nuevas tecnologías, en su Dictamen sobre Aspectos éticos de los implantes TIC en el cuerpo humano, de 16 de marzo de 2005. http://ec.europa.eu/european group ethics/docs/avis20 fr.pdf.

[50] GT29. Documento de 17 de marzo de 2004, sobre datos genéticos.

[51] ÁLVAREZ RIGAUDIAS, C.: "Tratamiento de datos de salud", en PIÑAR MAÑAS, J.L: "Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad", Reus, 2016. págs. 173 y ss.

[52] Artículo 4 punto 14 del RGPD.

El TJUE hace mención de los datos biométricos que proceden de huellas dactilares, considerando estos datos biométricos datos de carácter personal, ya que a través de ellos podemos conocer a la persona[53].

Para concluir este apartado, queremos destacar que los datos de salud son considerados datos personales, teniendo estos datos un carácter de lo más íntimo, he de ahí la protección especial que ostentan. Estos datos influyen en el derecho a la dignidad del individuo y necesitan el consentimiento expreso del interesado para que puedan ser tratados[54].

7.3. CONFIDENCIALIDAD DE LOS DATOS DE LOS PACIENTES Y DEBER DE SECRETO PROFESIONAL.

El principio de confidencialidad es una pieza fundamental para la protección de los datos relacionados con la salud. La confidencialidad se convierte en un elemento que permite que los pacientes proporcionen, con grandes garantías, datos de salud íntimos a los profesionales sanitarios[55], ya que entre estos debe existir una relación de confianza, no pudiendo el profesional médico, en ningún caso, divulgar esta información[56].

La confidencialidad ostenta un doble alcance: el primero, está relacionado con el conocimiento que se obtiene al recabar datos personales de los pacientes, limitando el acceso, exclusivamente, a personas que tengan autorización para acceder[57]; y, por otro lado, la

[53] STJUE (Sala Cuarta) de 17 de octubre de 2013, asunto C-291/12 (caso Schwartz), apartado 27: "Las impresiones dactilares están comprendidas en este concepto por contener objetivamente información única sobre personas físicas y permitir su identificación precisa"
[54] GT29 sobre el consentimiento en el sentido del Reglamento 2016/679, adoptadas el 28 de noviembre de 2017.
[55] LÓPEZ, P.; MOYA, F.; MARIMÓN, S. y PLANAS, I.: "Protección de datos de salud. Criterios y plan de seguridad", Madrid, 2001, pág. 5.
[56] FERNÁNDEZ COSTALES, J.: "El contrato de servicios médicos", Civitas, Madrid, 1988, págs. 216-217.
[57] La futura regulación del Espacio Económico Europeo, que actualmente se encuentra en el horizonte, supondrá una ventaja para que los pacientes puedan acceder a sus datos y puedan compartirlos. Los profesionales médicos también saldrán beneficiados ante esta propuesta.

obligación que tiene el personal sanitario de guardar secreto de la información que pueda conseguir a la hora de acceder al historial clínico del paciente[58].

Anteriormente mencionamos que, la protección que da nuestra ley se extiende más allá de la intimidad para poder integrar, de esta manera, el ámbito de la privacidad, no teniendo solo en cuenta aspectos íntimos del individuo. Lo íntimo se quiere acercar más al término "privacy"[59], queriendo tener como objetivo limitar el acceso de terceros[60].

La LOPDGDD establece que tendrá la consideración de falta muy grave "La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley"[61].

En relación con el cuidado de la salud, esta protección se materializa en los derechos del paciente y la obligación profesional de confidencialidad que ostenta el personal sanitario, que no es otra que mantener la confidencialidad de los datos de salud.

Los datos de salud, como ya hemos mencionado anteriormente, ostentan la categoría de datos especialmente sensibles, es decir, requieren de una protección especial. Por ello, la Ley General de Sanidad (en adelante, LGS), como parte de los derechos del paciente, vela por la intimidad y confidencialidad de toda información que esté relacionada con su cuidado[62]

La LGS vela, también, por el respeto a la privacidad y seguridad de toda la información relacionada con su cuidado. Otras leyes, como la Ley Básica de Autonomía del Paciente (en adelante, LBAP) también mencionan la necesidad de respetar la vida privada del paciente. El Convenio hecho en Oviedo en abril de 1997 también protege el derecho del paciente,

[58] ROMERO CASABONA, C. M.: "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías", Poder Judicial, núm. 31, 1993, pág.168.
[59] SUÁREZ RUBIO, M.J.: "Constitución y privacidad sanitaria", Tirant Lo Blanc, Valencia, 2017, pág. 53.
[60] Sentencia del Tribunal Constitucional nº196/2004 de 15 de noviembre de 2004.
[61] Artículo 72 LOPDGDD.
[62] Así lo establece el artículo 10.3 de la LGS.

velando por la intimidad y confidencialidad de toda aquella información relacionada con datos médicos de éste[63].

Consideramos el secreto profesional del personal sanitario una herramienta indispensable de esta protección[64], siendo obligatorio mantener secreto y confidencialidad de los datos de salud de los pacientes. El paciente confía plenamente en la profesionalidad del personal sanitario, para ello es necesario que el acceso a estos datos sea limitado, restringiendo el acceso a los datos médicos solo a los profesionales que hayan intervenido al paciente[65].

La obligación de confidencialidad del personal sanitario no se aplica solo a los datos que aparecen en el historial clínico, sino a todos los datos que se han obtenido durante el tratamiento de un paciente. Este deber de obligación afectará a todas aquellas personas que sean responsables del tratamiento de estos, incluyendo a los encargados de tratamiento y a cualquier persona que haya interferido en alguna etapa del tratamiento o recogida de los mismos. Todas estas personas tendrán que guardar el secreto profesional una vez que haya acabado la relación con el paciente[66].

La obligación de conservar la información continuará después de la finalización de su relación. Esta obligación no solo se aplica solo a los profesionales sanitarios sino a todo el personal que haya conocido esta información[67], por ejemplo, un médico en prácticas. En

[63] Se tendrá que respetar el carácter confidencial de los datos de salud. Por lo que, nadie podrá acceder a estos datos si no tienen autorización, así viene establecido en el artículo 7.1 de esta misma Ley.
[64] VERDÚ PASCUAL, V.F.: "Secreto profesional médico. Normas y usos", Granada, 2005, pág. 15 y ss.
[65] Es necesario que el profesional sanitario que acceda al historial clínico del paciente guarde secreto profesional, así lo establece el artículo 16.6 de la LBAP.
También hace mención de la obligación de guardar secreto, en relación con los datos del paciente, la LGS en su artículo 7 y 43 punto 2.
[66] DE LORENZO Y MONTERO, R.: "Derechos y obligaciones de los pacientes. Análisis de la Ley 41/2002, de 14 de noviembre, básica reguladora de autonomía de los pacientes y de los derechos de información y documentación clínica", Colex, Madrid, 2003.
[67] Así lo establece el artículo 2 punto 7 de la LBAP.

consecuencia, "todos los usuarios autorizados a utilizar datos personales de salud tienen una obligación de confidencialidad equivalente a una obligación de secreto profesional"[68].

La ley sanitaria incluye el secreto profesional, especialmente cuando se accede para proteger la salud pública, establece que debe ser realizad por un profesional médico "(...) sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto (…)"[69].

El código de Deontología Médica[70] incluye, los principios fundamentales de este deber profesional:

"1.- El secreto médico es uno de los pilares en los que se fundamenta la relación médico-paciente, basada en la mutua confianza, cualquiera que sea la modalidad de su ejercicio profesional.

2.- El secreto comporta para el médico la obligación de mantener la reserva y la confidencialidad de todo aquello que el paciente le haya revelado y confiado, lo que haya visto y deducido como consecuencia de su trabajo y tenga relación con la salud y la intimidad del paciente, incluyendo el contenido de la historia clínica.

3.- El hecho de ser médico no autoriza a conocer información confidencial de un paciente con el que no se tenga relación profesional"[71].

Por si fuera poco, las disposiciones en materia de protección de datos se refieren al secreto profesional. El responsable y encargado del tratamiento deberán tener en cuenta los riesgos más altos que puedan producirse derivado de la "pérdida de confidencialidad de datos

[68] Grupo Europeo de Ética de la Ciencia de las Nuevas Tecnologías, Op.cit.
[69] CARNICERO GIMÉNEZ DE AZCÁRATE, J.: "El derecho a la protección de datos en la historia clínica y la receta electrónica", Aranzadi, Pamplona, 1999, págs. 289-304.
[70] Visto en https://www.cgcom.es/sites/main/files/files/2022-03/codigo_deontologia_medica.pdf.
[71] Artículo 27 del Código de Deontología Médica de la OMC de julio de 2011.

sujetos al secreto profesional"[72]. Para ello tendrán que adoptar todas aquellas medidas necesarias para poder acreditar que el tratamiento realizado es acorde al Reglamento.

El deber de secreto y el deber de confidencialidad tendrán que estar armonizados con el derecho a la protección de datos personales[73], para poder cumplir con este deber, los centros hospitalarios y sanitarios tendrán que implantar normas de régimen interno, normas que tendrán que seguir todas aquellas personas que puedan conocer estos datos de salud, por ejemplo, un enfermero en prácticas.

En cuanto al cumplimiento de las obligaciones de confidencialidad, la responsabilidad del cumplimiento de esta obligación no recae sólo en las personas físicas que interfieren en los datos de los pacientes, sino que también recaerá en los centros de salud y en cualquier alto trabajador[74]. Para poder preservar el deber de secreto, se deberá aplicar medidas para poder anonimizar la identidad de la persona que va a recibir atención médica[75].

8. TRATAMIENTO Y CESIÓN DE LOS DATOS DE SALUD.

El RGPD considera tratamiento a "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales, utilizando o no procedimientos automatizados, viniendo a incluir en estos supuestos la estructuración y la adaptación, además de sustituir la referencia al bloqueo por la limitación, como nueva definición, en la que se alude al marcado de los datos personales conservados a fin de limitar su conservación"[76].

[72] Así lo establece el artículo 28.2. apartado a de la LOPD.
[73] Artículo 90.1 del RGPD.
[74] Se considera una vulneración del deber de secreto cuando un enfermero llama a un paciente a viva voz.
[75] Un ejemplo ilustrativo puede ser el identificativo del paciente a través de un número, que podrá ser visto por el paciente a través de una pantalla.
[76] ARIAS POU, M.: "Definiciones a efectos del Reglamento general de protección de datos", en Reglamento General de protección de datos, 2016, págs. 115-134.

Otros autores señalan que, el tratamiento existe independientemente de si se están utilizando esos datos o no, ya que puede que su utilización no sea de una forma perseverante, por lo que, se considera que se siguen utilizando, ya que estos siguen almacenados y se utilizarán de la forma que establezca el responsable para poder cumplir así con el fin establecido[77]. Otros señalan que, el tratamiento abarca "el todo", señalando que existe tratamiento solo por el hecho de ser poseedor de ellos, no teniendo en cuenta ni la forma ni la licitud del tratamiento[78].

El Convenio 108 recogió por primera vez los principios de protección de datos. El objetivo del Convenio era garantizar el respeto de sus libertades y sus derechos, independientemente de su nacionalidad, lugar de residencia, es decir su privacidad. En cuanto a la "calidad de datos", el convenio reconoció prioridad a ciertas categorías de datos, para garantizar así la seguridad del titular y ofrecerle ciertas garantías.

A la hora de establecer una clasificación de los principios generales de la protección de datos, la mayoría de la doctrina reconoce esta enumeración: principio de calidad., principio de información y principio de seguridad de datos

Con la entrada en vigor del RGPD, se le sigue dando a estos principios una notoria relevancia, ya que son de un gran valor para todo el ordenamiento de la protección de datos. Se considera que gracias a estos principios se les da una utilidad más lógica a los datos de carácter personal[79]. El RPGP, a la hora de regular estos principios, le da una continuidad a lo que establecía, anteriormente, la Directiva 95/46[80].

[77] ÁLVAREZ CIVANTOS, O.: "Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades. 3ª edición", Auren, Granada, 2008, pág.16.
[78] ÁLVAREZ HERNANDO, J.: "Guía Práctica sobre Protección de Datos. Cuestiones y Formularios", Lex Nova, Valladolid, 2011, pág. 64.
[79] HERRAN ORTIZ, A, "El derecho a la protección de datos personales en la sociedad de la información", Cuadernos Deusto de Derechos Humanos, nº 26, Universidad de Deusto, 2003.
[80] PIÑAR MAÑAS, J.L: "El nuevo Reglamento Comunitario de Protección de Datos", Reus, 2016, págs. 15-22

Varios autores destacan varios principios que se encuentran regulados en la LOPD[81]: Principio de calidad de datos, principio de consentimiento, principio de información, principio de finalidad, principio de proporcionalidad y principio de seguridad.

8.1. PRINCIPIO DE CALIDAD DE DATOS.

Este principio se encuentra dentro de la protección de datos. La LOPD mencionaba este principio como "la garantía de adecuación, exactitud, pertinencia y proporcionalidad de los datos de carácter personal, obligando al responsable del tratamiento a su cumplimiento. Así, los datos han de ser pertinentes y adecuados a la finalidad perseguida, utilizándose exclusivamente los datos necesarios para la finalidad solicitada. Por ello, un dato es adecuado, pertinente y no excesivo cuando su recogida y tratamiento guarda relación con el fin determinado para el que se ha obtenido"[82].

El convenio 108 ratifica el principio de calidad de datos y aglutina varios principios que iremos tratando, posteriormente, uno por uno. En otro artículo del convenio se menciona los datos relacionados con la salud, señalando que solo podrán ser tratados los datos si existen garantías para ello[83].

A) PROPORCIONALIDAD.

A la hora de hablar del principio de calidad de datos es necesario hablar de la proporcionalidad, ya que los datos recogidos tienen que ser proporcionales con la finalidad

[81] MURILLO DE LA CUEVA, P.L. y PIÑAR MAÑAS, J.L.: "El Derecho a la autodeterminación Informativa". Fundación coloquio jurídico europeo, Madrid, 2009, pág. 101.
[82] Artículo 4 de la LOPD.
[83] El artículo 6 del Convenio 108 establece que "Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales".

buscada[84]. A parte de ser proporcionales, los datos recogidos deben tener unas características determinadas: tienen que ser adecuados, convenientes y no pueden ser excesivos. El RGPD señala que el tratamiento de datos tendrá que realizarse de una forma que sea lícita, transparente y leal.

Es importante, a la hora de recabar los datos, utilizar la medida que sea menos perjudicial para el titular. Por lo que habrá que realizar un análisis previo para poder determinar cuál es la medida menos invasiva a la hora de menoscabar el derecho a la intimidad del titular. También se podrá recabar información más lastimosa para el titular, si la información es más ventajosa para el interés general. Tiene que haber una coherencia entre el tratamiento que se va a realizar y la finalidad que se quiere perseguir.

Anteriormente mencionamos que, el personal sanitario solo podrá acceder a los datos del paciente cuando sea rigurosamente imprescindible, incluyendo no solo al personal sanitario sino todas aquellas personas que hayan podido intervenir de alguna forma. Por lo que vemos que tienen la obligación de respetar este principio de proporcionalidad.

B) FINALIDAD.

Los datos personales solo pueden recopilarse para cumplir fines específicos, explícitos y legales[85], es decir siempre deben tener una finalidad.

El principio de "finalidad" se encontraba regulado en LOPD, ley que no se encuentra vigente en la actualidad. Esta ley señalaba que "los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos[86]".

[84] AGÚNDEZ LERÍA, I.: "Artículo 8. Principios relativos a la calidad de los datos. Protección de datos. Comentarios al Reglamento", Lex Nova, Valladolid, 2008, págs. 140 y ss

[85] Así lo establece el artículo 4 de la LOPD y el artículo 8 de la RLOPD. La LOPDYGDD menciona de forma indirecta en su artículo 94.2

[86] Así lo establecía el artículo 4.2 de la LOPD (Ley derogada).

La LOPDYGDD señala que cuando haya que expresar el consentimiento para diferentes fines se tendrá que otorgar el consentimiento para cada fin, no pudiendo otorgarse un consentimiento único para todas ellas. El RGPD encamina más está cuestión estableciendo que "los datos serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales[87]", solo se permite identificar al titular cuando su identificación sea necesaria para las personas que estén tratando estos datos, cabiendo, como casi siempre en nuestro derecho, determinadas excepciones[88].

Podemos llegar a la conclusión de que si el titular autoriza que se pueden tratar sus datos para una investigación (por ejemplo: cáncer de colon), estos podrán ser utilizados para investigaciones posteriores que se efectúen sobre esta enfermedad, por lo que no habrá disparidad en los tratamientos que se puedan llegar a realizar.

Por lo que, podemos definir la finalidad del tratamiento como la utilización de los datos que se recaban por parte del responsable con el consentimiento del titular y con la actividad por la cual el responsable dirige la utilización de esta información[89].

Para concluir con la finalidad, la doctrina presta especial importancia al principio de finalidad. El principio de finalidad tiene importancia durante todo el tratamiento, incluso en la recogida de los datos del titular. Para algunos autores, la finalidad es el principio más

[87] Artículo 5.1 del RGPD.

[88] Las excepciones se encuentran a esta norma se encuentran dentro del RGPD, más concretamente en su artículo 4.5.

[89] APARICIO SALOM, J.: "Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal", Aranzadi, Pamplona, 2000, pág.81.

importante, ya que consideran a este principio como un seguro para poder preservar los derechos del titular[90].

C) EXACTITUD Y VERACIDAD.

Los datos tendrán que ser exactos y, también, tendrán que estar actualizados[91]. La obligación de tener los datos actualizados será del responsable del fichero, que tendrá que estar enlazado con la posibilidad de que el titular pueda ejercer el derecho de rectificación y modificar aquellos datos que no sean exactos[92]. Se tendrá que actuar con la mayor brevedad posible para actualizar estos datos, ya sea suprimiendo o rectificando aquellos que no sean exactos[93].

Los datos personales que sean objeto de tratamiento tienen que ser lo más precisos posibles. Más importancia tiene si cabe en el ámbito de la salud la exactitud de estos, ya que es importante que el profesional sanitario trabaje con datos exactos de los pacientes para poder hacer un análisis más objetivo de cómo es su estado de salud y determinar que tratamiento debe seguir.

En un Historial clínico es importante que los datos sean exactos y tengan un estado óptimo, es decir que estén actualizados[94]. Para todo esto es importante la labor del paciente, ya que tendrá que cumplir con el deber de informar aportando datos que sean veraces. También, se tendrá que modificar, cancelar o sustituir aquellos datos que no sean completos o no sean exactos. Si por un motivo el profesional sanitario no pudiera descifrar el significado de estos datos tendrá que acudir a un traductor, que también tendrá que guardar confidencialidad de todos aquellos datos que pueda llegar a conocer.

---

[90] PÉREZ VELASCO, M.M.: "Los Ficheros Públicos, Estudios sobre Administraciones Públicas y Protección de Datos Personales", Thomson-Civitas y APDCM, Madrid, 2006, págs. 4 y ss.
[91] Artículo 4.3 LOPD.
[92] DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación", Derecho y salud, 2018, pág. 235.
[93] Sentencia de la Audiencia Nacional de 23 de marzo de 2013.
[94] Sobre la relevancia de la actualización del estado de salud habla la LBPA en sus artículos 14 a 19.

8.2. PRINCIPIO DE TRANSPARENCIA.

El principio de transparencia es un principio de especial relevancia en la protección de datos, regulado en la LOPD. La persona interesada tendrá que saber quién recogerá sus datos, quién los tratará y para qué fin utilizan estos[95]. El TC se pronunció en su sentencia nº292/2000 sobre este tema, "(…) A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos (FJ 5)"[96].

Este principio se encuentra integro dentro del derecho a la autodeterminación informática. El titular de los datos será informado de los pasos que seguirá el tratamiento y de cómo se van a utilizar estos datos durante el transcurso de este. A través de esto tiene especial importancia el proteger el derecho a la autodeterminación informática[97].

El principio de transparencia tiene, como la mayoría de los principios, unas limitaciones y unas obligaciones. El titular de los datos tendrá que ser informado con anterioridad y esta información tendrá que realizarse de una forma expresa, precisa e inequívoca. La derogada LOPD establecía que: "Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

" a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la

[95] APARICIO SALOM, J., "Derechos del interesado (Arts. 12-19 RGPD. Arts. 11-16 LOPDGDD)", Wolters Kluwer, Madrid, 2019, págs. 345-346.
[96] STC 292/2000, de 30 de noviembre
[97] MARTÍNEZ MARTÍNEZ, R.: "Tecnologías de la Información, Policía y constitución", Tirant lo Blanch, Valencia, 2001, págs. 203-203.

posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante"[98].

En cambio, no se tendrá la obligación de informar al interesado: "(…) cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados…", o cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial"[99].

No habrá que informar al interesado: "(…) si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban"[100].

El RGPD también hace mención del principio de transparencia, señalando que no solo es una garantía para la protección de datos, sino que, también, es una obligación para el responsable. La obligación para el responsable será recoger los datos del interesado. El RGPD señala obligaciones que tendrá que cumplir el responsable del tratamiento, estas obligaciones no tendrán que cumplirlas si el interesado dispone de dicha información[101]:

a) Tendrá que facilitar al interesado toda la información cuando haya obtenido los datos personales, es decir, todo lo que viene enumerado en el artículo 13.1 del RGPD[102].

[98] Artículo 5.1 de la derogada LOPD.
[99] Excepciones contempladas en el artículo 5.5 de la LOPD.
[100] Artículo 5.3 de la LOPD (DEROGADA):
[101] Artículo 13 del RGPD.
[102] "Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

b) Tendrá que facilitarle toda la información que sea necesaria para poder garantizar que se va a seguir un tratamiento que sea claro y noble, es decir, todo lo que viene enumero en el artículo 13.2 del RGPD[103].

c) "Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2"[104].

A la hora de interpretar la LOPDGDD daba la sensación de que se contradecía con el RGPD, en relación con este principio, ya que esta ley señala que el responsable del tratamiento "podrá dar cumplimiento al deber de información" al interesado". Dejaba la puerta abierta a si el responsable del tratamiento tenía la obligación de trasladar la

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado". (ARTÍCULO 13.1 RGPD)

[103] "Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos; f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado". (ARTÍCULO 13.2 RGPD)

[104] Artículo 13.3 del RGPD.

información, aunque al ser este un principio se sobreentiende que el responsable del tratamiento tiene que cumplir ese deber. La ley establece que:

" 1) Si los datos personales se han obtenido del afectado, el responsable del tratamiento "podrá dar cumplimiento al deber de información establecido en el artículo 13 del RGPD, facilitándole la siguiente información: a) La identidad del responsable del tratamiento y de su representante, en su caso. b) La finalidad del tratamiento. c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento".

2) Cuando los datos personales no hubieran sido obtenidos del afectado, "el responsable "podrá" dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento facilitando a aquel la información básica señalada en el apartado anterior, e incluirá también las categorías de datos objeto de tratamiento y las fuentes de las que procedieran los datos"[105].

Los profesionales sanitarios no tendrán que cumplir siempre con el deber de información, ya que tienen que preservar la confidencialidad y la obligación de secreto, en relación el artículo 14.5 del RGPD. Se produce una excepción para el responsable del tratamiento al deber de información cuando los datos de carácter personal "deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria". Por lo cual, el personal sanitario se encuentra damnificado por el secreto médico, por lo que no podrá suministrar la información que se prevé en el artículo 14 en sus puntos 1, 2 y 4 del RGPD[106].

[105] Artículo 11 del LOPDGDD.

[106] GT 29, Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, Adoptadas el 29 de noviembre de 2017 Revisadas por última vez y adoptadas el 11 de abril de 2018. Aportando como ejemplo "Un profesional de la medicina (responsable del tratamiento) está sujeto a la obligación de secreto profesional respecto de la información médica de sus pacientes. Una paciente (respecto al cual se aplica la obligación de secreto profesional) facilita al profesional de la medicina información sobre su salud relativa a una afección genética que comparte con varios parientes cercanos. Asimismo, la paciente facilita al profesional médico determinados datos personales de los parientes (interesados) que también padecen la enfermedad. El profesional médico no está obligado a facilitar a estos parientes la información a que se refiere el artículo 14, ya que se

8.3. PRINCIPIO DE CONSENTIMIENTO.

Este principio está relacionado con la conformidad del interesado de querer que se traten determinados datos, por lo que el titular tendrá que aprobar el tratamiento de estos datos. El interesado puede decidir libremente que datos quiere que sean tratados, reconociéndole una capacidad de elección muy grande, es decir garantizar la transparencia[107].

La doctrina reconoce que este principio es uno de los aspectos más importantes de la protección de datos. Por lo que, el consentimiento del interesado es, por tanto, el principio mediante el cual se crea el camino para una relación entre la protección de datos del interesado y el uso de la informática "la exigencia del consentimiento informado del afectado como regla que ha de observarse antes de proceder a un tratamiento de este tipo de datos. Consentimiento que solamente puede ser obviado cuando la ley así lo permita; bien autorizando ella misma tratamientos por exigirlo el interés público, bien estableciendo que ante determinados datos, como los procedentes de fuentes accesibles al público, y en determinadas condiciones, no es necesario recabarlo"[108]. En relación con lo mencionado en este párrafo, "el derecho a la protección de datos se sostiene sobre dos pilares fundamentales: el consentimiento y el conjunto de derechos que lo hacen practicable"[109].

La LOPD no exigía[110] el consentimiento del interesado si los datos personales se encontraban en plataformas que fueran públicas, en cambio el nuevo RGPD señala la obligación de informar al titular (en el supuesto de que estos no hayan sido proporcionados el por él) si se extrajeran los datos de una plataforma pública.

---

aplica la excepción recogida en el artículo 14, apartado 5, letra d). Si el profesional médico lo hiciese estaría violando la obligación de secreto profesional que le debe a su paciente".

[107] MARTÍNEZ ROJAS, A.: "Principales aspectos del consentimiento en el Reglamento General de Protección de Datos de la Unión Europea", Aranzadi, 2016, págs. 4 y ss.

[108] MURILLO DE LA CUEVA, L, P.: "El derecho a la autodeterminación informativa y la protección de datos personales", Sociedad de Estudios Vascos, San Sebastián, 2008, págs.43-58.

[109] SERRANO PÉREZ, M.M.: "El derecho fundamental a la protección de datos. Derecho español y Comparado", Aranzadi, Pamplona 2004, págs. 258-260

[110] Artículo 6.2 de la LOPD.

La LOPDGDD está siguiendo una interpretación muy continuista en relación con este tema, por lo que la interpretación se aplica de la antigua Ley; hay que diferenciar si las plataformas son públicas o privadas. Este aspecto es muy importante, ya que solo se podrá recabar datos de aquellas plataformas que tengan acceso público (todo el mundo puede acceder), no teniendo en cuenta aquellas a las que solo pueden acceder un número determinado de usuarios, por ejemplo, Facebook.

La LOGPD considera consentimiento a ""(…) toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"[111].

El TC, se manifestó, señalando que es fundamental obtener el consentimiento del interesado, estableciendo lo siguiente:

"(…) y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele (…)"[112].

[111] Artículo 6.1 de LOPDGDD.
[112] Sentencia del Tribunal Constitucional nº 292/2000 (Fundamento jurídico 7).

En relación con el ámbito que nos incumbe, queremos destacar la LBAP, ley que hemos mencionado y hablado de ella anteriormente en el texto, en concreto, queremos destacar su artículo 2, en ese precepto habla del respeto y dignidad que ostenta las personas y la autonomía de cada una de ellas, todo esto se concreta en la obligación de que el paciente consienta previamente. El consentimiento se tendrá que realizar una vez que se haya escuchado toda la información, y, no menos importante, el paciente podrá en todo momento rechazar el tratamiento, sin tener que justificar un motivo[113].

Cuando se vaya a realizar un acto sanitario, la información tendrá que ser anterior al consentimiento, siendo la información clara y concisa. Además, el profesional sanitario tendrá que informar al paciente de todas las opciones posibles. El profesional sanitario, una vez que haya elegido el paciente la opción que crea más conveniente, tendrá que informar al paciente de todos los riesgos que puede acarrear esa intervención. Esta información previa al consentimiento compone un derecho fundamental, así lo ha establecido el TC en una de sus sentencias[114].

Varios autores señalan que "no estamos ante un consentimiento informado, sino ante un deber de información y un posterior consentimiento; a una posterior decisión consciente y libre por parte del paciente debidamente informado"[115].

Estaríamos ante una responsabilidad del profesional sanitario en el caso de que no trasladará la información previa necesaria para el posterior consentimiento de interesado. Esta situación es uno de los motivos que más se dan, pudiendo conllevar, posteriormente, una sanción por incumplimiento de la responsabilidad civil médica.

[113] El considerando 42 del RGPD establece quel paciente tendrá que conocer, además, quien va a ser el responsable o encargado del tratamiento y que finalidad desea obtener al recabar información de éste.
[114] Sentencia del Tribunal Constitucional de 28 de marzo de 2011 nº 37/2011.
[115] LIZARRAGA BONELL, E.: "La información y la obtención del consentimiento", Thomson-Civitas, Madrid, 2004, págs. 226-228.

8.4. PRINCIPIO DE LICITUD Y TRANSPARENCIA.

Una de las exigencias del tratamiento de datos es que tendrá que ser lícito[116]. Este principio está correlacionado con el principio de transparencia y este último se vincula con el principio de información, teniendo que ser la información clara y fácil de acceder.

El principio de transparencia, como ya mencionamos anteriormente, es un principio de especial importancia para la protección del tratamiento de datos. El interesado tendrá que saber en todo momento quién es el responsable del tratamiento y su finalidad, incluyendo toda aquella información de relevancia[117].

El principio de información está ligado al principio de transparencia. La información tiene que llevarse a cabo de una forma clara; por lo que tendrá que ser fácil de entender y de poder acceder a ella; teniendo que incorporar "(…) la identidad del responsable del tratamiento y sus fines, así como la información necesaria para garantizar que sea leal y transparente y a su derecho a obtener confirmación o comunicación de los datos que les afectan y que son tratados (…)"[118], no incluyendo tratamientos confidenciales.

En relación con el sector de la salud, tiene una mayor relevancia que se traslade al paciente una información clara y precisa de cómo van a ser tratados sus datos de salud. Cuando se ceden los datos del paciente de una Administración sanitaria a una pública se tendrá que, por lo menos, informar al paciente de que se va a realizar este tipo de operaciones.

[116] Artículo 6 del RGPD.
[117] Considerando 39 RGPD
[118] Considerando 39 RGPD.

8.5. PRINCIPIO DE LIMITACIÓN DE LA FINALIDAD.

Por lo general, los datos personales "serán con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines"[119]. La recogida de datos deberá tener un objetivo concreto, no pudiendo ampliarse para otros fines diferentes. Es muy común que una vez comenzado con el tratamiento surjan imprevistos que no estaban planeados, y más cuando se pueda estar realizando el tratamiento para investigaciones[120]. El reglamento permite ampliar este tratamiento si se están realizando investigaciones científicas, por lo que "no se considerará incompatible con los fines iniciales"[121].

Para poder ofrecer garantías de que los datos recogidos no se utilizan por un tiempo superior al necesario, el responsable revisará periódicamente estos datos, suprimiéndolos cuando superen el plazo establecido.

Si hablamos de los datos de salud, la función principal es el cuidado del paciente; cabiendo excepciones y funciones distintas que hemos visto anteriormente y que estarían por encima de la protección del individuo, estas serían: la protección del Estado, la defensa y la salud pública.

8.6. PRINCIPIO DE MINIMIZACIÓN DE DATOS.

El RGPD establece que "los datos tienen que ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"[122]. Interpretamos a la hora de

[119] Artículo 5.1.b del RGPD.
[120] NICOLÁS JIMÉNEZ, P.: "Investigación biomédica y big data sanitarios". En: TRONCOSO REIGADA, A.: "Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos de Carácter Personal". Thomson Reuters, 2019. pág. 7.
[121] Considerando nº 33 del RGPD.
[122] Artículo 5.1.c del RGPD.

leer este precepto que para cumplir estas funciones se tiene que limitar el plazo de conservación, estableciéndose estrictamente un límite[123].

En relación con el ámbito de la salud, llegamos a la conclusión que solo se podrán utilizar aquellos datos que sean totalmente necesarios, incluyéndose, exclusivamente, al historial clínico, aquellos que sean necesarios para la curación del paciente[124].

Se potencia el significado de "necesarios", no siendo necesario recopilar datos si puedo conseguir el objetivo sin tener que realizar un tratamiento de datos. Por lo que, en este caso, estos no deberían de ser procesados: antes de recopilar los datos se tendrá que estudiar cuántos hay que recoger y qué categoría, puesto que "los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios"[125].

8.7. PRINCIPIO DE LA LIMITACIÓN DEL PLAZO DE CONVERSACIÓN.

Se deberá conservar los datos de los pacientes durante el plazo necesario, tiempo que dependerá de la finalidad del tratamiento. El tiempo de retención de los datos podrá extenderse por diferentes motivos: cuando exista un interés general de carácter público; cuando la conservación se vea motivada por una investigación de carácter científico o histórico o por finalidades estadísticas. El encargado en seleccionar plazos de supresión y de revisar periódicamente los datos será el responsable del tratamiento[126].

[123] PUYOL MONTERO, J.: "Los principios del derecho a la protección de datos", Reus, Madrid, 2016, págs. 135-150.
[124] El RGPD establece que los datos recopilados tendrán que ser "necesarias", ya que la antigua LODP establecía que no deberían de ser "excesivos".
[125] Considerando 39 RGPD.
[126] Considerando 39 RGPD.

En relación con la salud, el historial clínico se deberá conservar los datos durante un plazo de 5 años[127] , pudiendo ampliar este plazo si el paciente lo necesitará. El plazo dependerá en todo momento de la evolución del paciente y de su propio estado actual. Un enfermo que tenga un tratamiento permanente, como es lógico, tendrá un plazo de tratamiento superior a 5 años. Asimismo, cabe la posibilidad de que un paciente necesite la información de un historial clínica para presentarlo como medio de prueba para reclamar una indemnización o una negligencia[128].

En base a la historia clínica: "La historia clínica deberá conservarse en las condiciones que garanticen la autenticidad, integridad, confidencialidad, preservación y correcto mantenimiento de la información asistencial registrada, y que asegure una completa posibilidad de reproducción en el futuro, todo ello durante el tiempo en que sea obligatorio conservarla e independientemente del soporte en que se encuentre, que podrá no ser el origina"[129].

La AEPD establece que los hospitales sanitarios están obligados a conservar el historial clínico según el tiempo y forma que se establece.

8.8. PRINCIPIO DE INTEGRIDAD Y SEGURIDAD.

A la hora de tratar los datos es fundamental garantizar la seguridad de estos, evitando que se traten aquellos que sean ilícitos o no tengan autorización del interesado para ser tratado. Es importante que el responsable del tratamiento garantice la seguridad de los datos evitando que sean destruidos, perdidos o dañados. Para ello, es fundamental que se lleven a cabos medidas organizativas y técnicas.

[127] El plazo del que estamos hablando en texto es un plazo mínimo de conservación, aunque hay en algunas Comunidades Autónomas donde el plazo mínimo puede ser superior.
[128] ATELA BILBAO, A. y otros: "Autonomía del paciente, información e Historia clínica (Estudios sobre la Ley 41/2002, de 14 de noviembre)", Thomson-Civitas, Pamplona, 2004, pág. 65.
[129] Art. 19.4 del Decreto 38/2012, del País Vasco, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica.

Es imprescindible que haya una actuación proactiva por parte de la persona que trate nuestros datos personales para evitar así cualquier tipo de amenaza.

9. DERECHOS QUE OSTENTAN LOS PACIENTES.

Como ya mencionamos anteriormente, la LOPD y su Reglamento se encuentran derogados, pero acudiremos a estas dos normas, ya que siguen siendo muy apropiadas para hablar de estos derechos[130]. La nueva regulación ha mantenido y matizado en varias situaciones estas dos normas, ya que en algunas situaciones ha habido complicaciones a la hora de interpretarla.

La entrada de la nueva regulación, es decir la LOPDGDD, ha rellenado ciertos matices, ya que otorga a los herederos y familiares[131] de una persona fallecida ciertos derechos a la hora de tratar los datos de la persona fallecida, estos "podrán solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión[132]", salvo que la persona fallecida haya prohibido expresamente este derecho.

Los derechos de acceso, rectificación, cancelación y oposición (en adelante, derechos ARCO) se encuentran fuertemente relacionados con el derecho que tienen los titulares de los datos a la información anterior a su tratamiento. Es necesario que la persona afectada de este tratamiento reciba una información previa, teniendo que ser esta precisa, expresa e

[130] LOPDGDD. Disposición adicional decimocuarta. Artículo 13 de la Directiva 95/46/CE. "Las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas".

[131] Incluye la figura de la pareja de hecho.

[132] Artículo 3 de la LOPDGDD

inequívoca de la finalidad de este, de este modo se le otorgará a la persona afectada el poder solicitar cualquier derecho ARCO[133], sin tener que especificar el motivo de su solicitud.

Con la entrada de la RGPD y la LOGPDD se ha ampliado las facultades que se le otorgaban a las personas afectadas por el tratamiento, reconociéndoles el derecho al olvido y a la portabilidad. También se les ha reconocido el derecho a limitar el tratamiento a no ser afectado por decisiones individualizadas[134].

El RGPD ha conseguido reforzar el poder que tienen las personas sobre sus datos personales, por lo que no debe limitarse solo a los derechos ARCO, ya que hay nueva categoría de derechos regulados en la Directiva anterior, es decir la Directiva 95/46/CE[135].

Próximamente, iremos analizando, uno por uno, los derechos que pueden ejercitar los titulares de los datos.

9.1. DERECHO DE ACCESO.

El derecho de acceso es un derecho que ostenta la persona afectada por el tratamiento. Este derecho es gratuito y se utiliza para obtener información de todos los datos personales que se están tratando, el lugar donde se han obtenido estos, como todas aquellas comunicaciones que se han realizado o quedan por realizarse[136]. Por lo que, se ejercerá el derecho de acceso cuando se quiera conocer aquellos datos que están siendo tratados por la persona encargada y el motivo que busca[137].

[133] DAVARA RODRÍGUEZ, M.: "Una primera aproximación al Reglamento europeo de protección de Datos y su incidencia en el tratamiento de datos de carácter personal de las Administraciones Públicas", Actualidad Administrativa, Revista Acta Judicial,2018.
[134] Artículos 15 a 22 del RGPD y 18 a 22 de LOPDGDD.
[135] ÁLVAREZ CARO, M.: "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones…", en Reglamento General de Protección de Datos, Reus, 2016, pág. 227-240.
[136] De acuerdo con la Sentencia de la Audiencia Nacional de 19 de marzo de 2014 "(…) el derecho de acceso sólo alcanza a los datos personales del titular (…) sin que quepa aceptar que incluye el derecho a acceder a datos de carácter personal de otras personas, pues ello comportaría la vulneración de su derecho fundamental a la protección de datos, consagrado en el art. 18.4 CE"
[137]STEINMEYER ESPINOSA, A.: "¿Permite el derecho de acceso a la información pública, el acceso a datos personales?", Universidad Tecnológica Metropolitana, Chile, 2013, pág. 10

No es necesario especificar el motivo por el cual el interesado quiere acceder. La persona interesada en acceder podrá hacerlo de una forma libre, y sin ninguna restricción, pudiendo aludir a intereses de carácter particular[138].

Para poder preservar el derecho de los pacientes a la intimidad y confidencialidad es fundamental proteger el acceso de los pacientes y de los profesionales sanitarios. Para ello es necesario garantizar de una forma debida el uso y acceso que estos dan a la historia clínica[139]

El derecho de acceso, en relación con los datos de salud, se fundamenta en la facultad que tienen los pacientes para poder acceder a sus historias clínicas[140]. Para poder acceder a estos datos los pacientes deberán acceder a través de portales seguros[141].

9.2. DERECHO DE RECTIFICACIÓN.

En la Carta de Derechos Fundamentales (en adelante, CDFUE) se establece una definición de este derecho señalando que "toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación"[142]. También se puede dar la posibilidad de que "el paciente pueda rectificar aquellos datos que no sean completos ni sean exactos". El RGPD también menciona este derecho señalando que "todo interesado debe tener derecho a que se rectifiquen los datos personales que le conciernen"[143].

La persona afectada deberá acompañar la documentación necesaria para poder acreditar que los datos carecen de exactitud o no son del todo completos[144]. Para que el tratamiento

[138] SÁIZ RAMOS, M. y LARIOS RISCO, D., "El derecho de acceso a la historia clínica por el paciente: Propuesta para la reserva de anotaciones subjetivas", en Derecho y Salud, 2009, págs. 26-27.
[139] GONZÁLEZ GARCÍA, L., "Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos", en Derecho y Salud, 2014, pág. 276.
[140] Así lo establece el artículo 18 de la Ley 41/2012.
[141] ABELLÁN-GARCÍA SÁNCHEZ, F. y GARCÍA DÍAZ, A., Protección de datos personales de salud en el plano asistencial e integrador (en línea), https://cutt.ly/8YgIxUM (consulta 5 de mayo de 2023).
[142] Artículo 8 apartado 2 de la CDFUE.
[143] Considerando 65 del RGPD
[144] Artículo 16 RGPD y 14 LOPDGDD.

sea lícito el responsable se tendrá que encargar, de inmediato, de tomar las medidas oportunas para modificar aquellos datos que no sean exactos.

El derecho de rectificación y de supresión tiene ciertas similitudes, ya que pueden llevar a que, a veces, las personas se confundan a la hora de ejercitar estos derechos. La mayor diferencia está en su aplicación: el derecho de rectificación se ejercitará cuando los datos no sean exactos; pero, en cambio, el derecho de supresión se ejercitará cuando los datos no sean adecuados o sean excesivos.

A la hora de ejercer el derecho de rectificación no se busca poner fin al tratamiento, solo se busca sustituir aquellos datos que no sean exactos ni correctos, para que la persona responsable pueda tratar datos correctos y que estén actualizados[145].

Este derecho es independiente y tiene carácter personal, ya que tiene que ser el titular de los datos quien lo ejerza. El responsable del tratamiento es el encargado de comprobar si la información que aporta el interesado es correcta para, posteriormente, poder modificar así aquellos datos.

Centrándonos en los datos de salud, en este caso, el paciente tiene facultad de poder ejercitar este derecho para modificar aquellos datos que no sean exactos o estén incompletos. El paciente tendrá que aportar toda la documentación que verifique la inexactitud de estos. El profesional médico tendrá que comprobar si la rectificación es procedente o, por lo contrario, si no lo es[146].

9.3. DERECHO DE CANCELACIÓN.

Como mencionábamos anteriormente, el derecho de rectificación se encuentra regulado en el artículo 16 del RGPD. En la legislación anterior se encontraba regulado junto con el

[145] Artículo 14 LOPDGDD.
[146] AEPD, Guía para pacientes y usuarios de la Sanidad, noviembre 2019.

derecho de cancelación. Actualmente, ha aparecido el derecho de supresión, también denominado derecho al olvido, que se encuentra regulado en el artículo 17 del Reglamento actual de protección de datos.

En relación con los datos de salud, la AEPD ha hecho, varias veces, mención a estos. En la historia clínica tendrán que aparecer todos aquellos datos que sean veraces y estén actualizados para poder conocer así el estado actual del titular de los datos. El personal sanitario que esté tratando estos datos determinará la finalidad que da a estos datos[147].

9.4. DERECHO A LA LIMITACIÓN DEL TRATAMIENTO[148].

El RGPD establece una definición a este derecho, estableciendo que hace referencia a ""(…) el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro"[149].

En relación con los datos sanitarios de los pacientes, se pueden dar controversias entre los centros hospitalarios y los titulares de los datos. Por lo que, el paciente podrá ejercer el derecho a la limitación del tratamiento, cuando ocurran las siguientes suposiciones:

- Cuando el centro hospitalario se encuentra decidiendo si los datos carecen de validez o no.
- Cuando ejercer el derecho de oposición sea preciso.
- Cuando el interesado quiera preservar los datos, independientemente de la validez de estos.
- Cuando el paciente necesite estos datos para ejercitar reclamaciones y el responsable del tratamiento no los necesite.

El paciente, que haya ejercitado el derecho de limitación del tratamiento. podrá decidir, mediante autorización, si los datos se pueden seguir utilizando o no, pudiéndose utilizar para

[147] Resolución de la Agencia Española de Protección de Datos R/00549/2004, de 6 de octubre de 2004
[148] Artículo 16 de la LOPGDD Y 18 del RGPD.
[149] Artículo 4 del RGPD.

ejercitar alguna reclamación o para la protección de los derechos de terceros que puedan estar afectados.

Con la aparición del COVID 19 varias agencias de protección de datos como la de Francia y Reino Unido señalaban que a la hora de recoger datos de salud se utilizará el método menos invasivo. Es decir, que se limitase la recogida de los datos de salud, pudiendo utilizar otros medios. Por ejemplo, preguntarle al paciente si había convivido con un positivo o si había estado con personas que habían dado positivo, en vede preguntarle por los síntomas. Por lo que, se exigía que a la hora de tratar datos de salud se respetará todos los principios que se encuentran regulados en el RGPD[150].

9.5. DERECHO DE OPOSICIÓN.

El derecho de oposición[151] es un derecho que pueden ejercer el titular de los datos para que no se traten los datos o para que se dejen de tratar los datos que ya están siendo tratados[152].

El responsable del tratamiento de los datos tendrá la obligación de no continuar con el tratamiento de estos, excepto cuando el tratamiento sea necesario para proteger los derechos, intereses y libertades del paciente. Para ello es necesario que el responsable del tratamiento acredite la necesidad de continuar con el tratamiento.

En otras finalidades, como por ejemplo la mercadotecnia, este derecho tiene mucha importancia. En relación con los datos de salud no, ya que los interesados tienen la obligación[153] de no impedir este tratamiento. Los pacientes dificultaran el proceso asistencia si no transmiten información que sea veraz y leal.

[150] AEPD, Informe sobre tratamiento de datos en relación con el COVID-19, 12 de marzo de 2020.
[151] Normativa regulado en los artículos 18 de la LOPDGDD Y 21 del RGPD.
[152] GALLEGO RIESTRA, S., "Los derechos de acceso, rectificación, cancelación y oposición del paciente sobre su historia clínica", en Derecho y Salud, 2016, pág. 140
[153] Obligación recogida en la Ley 41/2022.

Podría caber como excepción las instrucciones previas o voluntades anticipadas. El interesado tendrá la posibilidad de elegir que no se lleven a cabo ninguna acción de carácter médico, incluyendo que no se lleve a cabo ningún tratamiento de datos que tenga relación con esta elección. La última palabra la tendrá el profesional sanitario, que tendrá que decidir si esta elección es correcta o no.

9.6. DERECHO A LA SUPRESIÓN O AL OLVIDO.

Aunque este derecho se incluya por primera vez en el RGPD, no es un derecho nuevo. Este derecho esta correlacionado con el derecho a la cancelación, pero en un entorno más concreto, Internet. También se encuentra relacionado con el derecho a la intimidad y con el derecho a la protección de datos. Por lo que, este derecho "consiste en una agrupación entre el derecho de cancelación y el de oposición, pero en el tratamiento de datos, en un ámbito concreto, como es el de Internet"[154].

El derecho de supresión se afianza en una sentencia del TJUE de Google Spain SL contra la Agencia Española de Protección de datos. Esta sentencia genera mucha jurisprudencia haciendo fuerte y sólido al derecho al olvido, fortaleciendo el tratamiento de los datos que se encuentran en Internet, más concretamente en los motores de búsqueda.

A través de esta sentencia se le concede al titular la posibilidad de suprimir o bloquear toda información que esté relacionada con él y que se encuentre en motores de búsqueda de internet.

Este derecho no solo abarca datos que no sean exactos, sino también aquellos "datos que sean inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento, que no estén actualizados o de que se conserven durante un periodo superior al necesario, a menos que se imponga su conservación por fines históricos, estadísticos o científicos"[155].

[154] ÁLVAREZ CARO, M.: "El derecho a la supresión o al olvido", Reus, 2016, págs.241 y ss.
[155] Sentencia del TJUE del 14 de mayo de 2014 Sentencia del TJUE del 14 de mayo de 2014 "Google Spain SL c Agencia Española de Protección de Datos".

El derecho al olvido no es un derecho absoluto, ya que se encuentra limitado por otros derechos. Este derecho no podrá ser ejercido cuando menoscabe un derecho fundamental o cuando a la hora de ejercerlo se menoscabe un interés de carácter público, es decir un legítimo superior[156].

Según el TC, el derecho al olvidado se encuentra integrado dentro del artículo 18 punto 4 de la CE. Este derecho es considerado para el TC como un derecho fundamental relacionado con la libertad de la información a la hora de utilizar herramientas tecnológicas. Por lo que, llegamos a la conclusión que el derecho al olvido es un derecho que garantiza la protección del derecho al honor y a la intimidad.

En relación con el tratamiento de datos de salud, más concretamente el historial clínico del paciente, el suprimir los datos es complicado de que se pueda realizar. El tratamiento de estos datos abarca un gran número de finalidades por lo que es importante que se mantengan y se conserven. En las enfermedades de larga duración[157] no se pierde la finalidad del tratamiento a la hora de utilizar estos datos. Los datos de salud no podrán ser considerados como no pertinentes y no adecuados[158].

9.7. DERECHO A LA PORTABILIDAD.

El derecho a la portabilidad[159] concede, en este caso, al paciente la posibilidad de recopilar, en un formato estructurado, todos aquellos datos que estén relacionados con él y que haya facilitado, con anterioridad, a una empresa o un responsable. Estos datos serán pasados a otra empresa o responsable sin tener que pasar por el paciente. Cabe la posibilidad

[156] MURILLO DE LA CUEVA, L: "Las viscitudes del derecho de la protección de datos personales" Revista Vasca de Adminitración pública, 2000, págs. 211-235.
[157] Enfermedades crónicas o incurables.
[158] AEPD, Guía sobre protección de datos.
[159] Derecho que se encuentra regulado en el artículo 20 del RGPD y 17 de la LOPDGDD.

de que el interesado pueda descargarlos para luego pasarlos a otro[160]. Este hecho hace que se incremente la competencia dentro en el mundo digital[161].

El punto 3 del artículo 20 del RGPD señala que el derecho de portabilidad "no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento".

Una Guía que realizó la Autoridad de Cataluña en relación con la protección de datos mencionaba el derecho a la portabilidad de los datos de salud, señalando que el tratamiento de estos datos encuadra en la excepción mencionada en el anterior párrafo, ya que es considerada una actividad de interés público[162].

Si el paciente quiere ejercer este derecho, en centros de carácter privados, se tendrá que transferir todos aquellos datos que tengan relación con él, pero se tendrá que borrar los datos del resto de personas que hayan intervenido, en un momento determinado, al paciente. Como, por ejemplo, el médico que operó al paciente.

10. CONCLUSIONES

Una vez expuestos y analizados uno por uno los distintos puntos más relevantes derivados de la protección de los datos de salud podemos llegar a sacar las siguientes conclusiones:

PRIMERA: La protección de datos nace con la necesidad de proteger la intimidad personal, englobando toda aquella información que puede hacer identificable a una persona.

[160] AEPD, Guía sobre protección de datos.
[161] FERNÁNDEZ-SAMANIEGO, J.: y FERNÁNDEZ LONGORIA, P.: "El derecho a la portabilidad de datos", en el reglamento general de protección de datos, 2016, pág.273.
[162] AUTORIDAD CATALANA DE PROTECCIÓN DE DATOS, Guia de protección de dades per a pacients i usuaris del serveis de salut (en línea), https://cutt.ly/xYlV69I (consulta 6 de mayo de 2023).

Mención especial hay que hacer al aumento en nuestro día a día de las nuevas tecnologías, ya que ante esto los derechos de las personas se encuentran más amenazados.

El derecho a la protección de datos no solo engloba aquellos aspectos de carácter íntimo sino sobre todos aquellos que sean de carácter personal. Al titular de estos datos se le otorga un poder absoluto, ya que tiene autonomía para decidir qué hacer con ello.

El titular tendrá un poder de control a la hora de determinar si un tercero tiene facultad para tratar sus datos. Para que un tercero pueda tratar los datos del titular tendrá que necesitar de éste un consentimiento expreso y, en el caso de que no exista ese consentimiento, necesitará de una autorización legal que justifique ese tratamiento.

La protección de datos personales se ve reflejada en la LOPDGDD y en el RGPD. Debiendo tener en cuenta, en algunos casos, los cuerpos legales ya derogados (LOPD y anterior Reglamento de protección de datos) y, por último, la AEPD; por la importancia de sus resoluciones.

SEGUNDA: La protección de datos necesita la actuación de un sistema sancionador en caso de incumplimiento, ya que esto ayuda a que su funcionamiento sea más adecuado. La prioridad de este sistema sancionador no es la imposición de sanciones, sino que todas las personas que actúen a la hora de tratar datos lo hagan de la mejor forma posible.

El sistema sancionador podrá imponer multas de carácter administrativo, pudiendo ser sancionado el infractor con 20 millones de euros o con el 4% del valor de negocio de la empresa. Las autoridades nacionales y de control tendrán facultad para imponer dichas sanciones.

El incumplimiento de las normas, a la hora de tratar datos de salud, tendrá la consideración de sanción, siendo esta sanción catalogada muy grave, al integrarse los datos de salud en categorías especialmente protegidas.

TERCERA: Los datos de salud son considerados datos especialmente sensibles, lo que conlleva a que a la hora de tratar estos datos se lleven a cabo medidas de seguridad muy altas, si lo comparamos con el tratamiento de otros datos.

Los datos de salud tienen una característica fundamental ya que, en ciertos casos, sirven para poder mejorar la atención sanitaria del paciente. Por lo que, vemos que existe un conflicto entre: la protección del tratamiento de los datos personales, y el ordenamiento regulador de la salud pública. Estos dos ordenamientos tendrán que ser tratados de una forma conjunta, realizando un tratamiento amplio de la regulación de la protección de datos, no obstaculizando la necesidad del paciente de poder ser tratado, ya que la mejora y evolución del paciente es el objetivo principal.

Con normalidad, los datos de salud se encuentran en la Historia Clínica. La historia clínica contiene una información actual y detallada de la salud del paciente, ya no solo engloba datos de salud sino datos de su vida priva y de su vida familiar; es por esto por lo que merece una importante protección. Los datos de salud también pueden encontrarse en tarjetas sanitarias, recetas electrónicas (incluso recetas en papel); todos estos, al contener datos de carácter personal especialmente sensibles, son merecedores de especial protección.

Es importante que se pueda distinguir de cuando un acceso a la Historia Clínica está facultado y cuándo no lo está. El propio sistema de acceso permite identificar cuando un acceso es lícito y cuándo no lo es.

En relación con el acceso al Historial clínico, es imposible ofrecerle al paciente un sistema que tenga unas garantías absolutas de su buen funcionamiento, ya que siempre puede haber riesgo de que haya un acceso a sus datos que no esté justificado.

El paciente tendrá frente a la historia clínica la posibilidad de ejercitar los siguientes derechos: acceso, rectificación, de cancelación, portabilidad y de limitación del tratamiento.

CUARTA: Se considera que se están tratando datos cuando se realiza frente a ellos cualquier tipo de intervención. Esta intervención se tendrá que realizar sobre cualquier dato que nos permita a través de él identificar a una persona.

El RGPD se basa en una responsabilidad de carácter proactivo y preventivo, anticipándose a un posible riesgo. El responsable y el encargado del tratamiento tendrá que garantizar una seguridad óptima, teniendo que preservar la integridad de todos aquellos datos de los que sean responsables o encargados. Para ello es necesario que implanten medidas organizativas y de seguridad que se adapten al riesgo del que están expuestos.

Los datos de salud deberán tener medidas organizativas y de seguridad muy elevadas, ya que estos datos contienen información privada y esencial para el paciente. Antes de realizar cualquier tipo de tratamiento se tendrá que realizar una Evaluación de impacto. Esta evaluación solo afectará a los datos de carácter clínico de la Historia clínica, no viéndose afectados los datos de carácter personal.

QUINTA: Como mencionamos anteriormente, el paciente tiene autonomía para determinar qué tratamiento pueden llevar a cabo con sus datos. El paciente podrá ejercer los derechos que se encuentran regulados en los artículos 16 a 22 del RGPD. El titular podrá ejercitar el derecho de acceso para poder comprobar si sus datos se están tratando de una forma lícita. También podrá recibir información sobre cómo están siendo tratados y esta información tendrá que ser proporcionada por el responsable.

Con la nueva regulación, los derechos ARCO se vieron aumentados debido al derecho de la portabilidad, al olvido y a la limitación del tratamiento. El ejercicio de estos derechos se tendrá que llevar a cabo en base a los principios de información y transparencia.

La información que contiene la historia clínica está limitada y protegida, esta limitación se realiza para proteger derechos de carácter confidencial de terceros. Es por esto por lo que,

no se podrá a acceder a opiniones de carácter subjetivo de un médico, incluso cuando el paciente necesite un tratamiento terapéutico.

Diversos profesionales pertenecientes al ámbito sanitario pueden acceder a la historia clínica. Todos ellos estarán expuestos al deber de confidencialidad de sus datos, debiendo preservar el secreto de estos, siendo sancionados aquellos que incumplan este deber. Aquellos profesionales que tengan relación directa con el paciente podrán acceder a su historial clínico, siempre y cuando consideren necesario, sin necesidad de recabar consentimiento expreso.

Si no fuera un personal autorizado el que accediera a estos datos estaríamos ante una intromisión ilegítima, y el afectado, ante este caso, tendría facultad de denunciar estos hechos ante la AEPD. Esta intromisión ilegítima podría conllevar diferentes sanciones: civiles teniendo que indemnizar a la persona que se ha visto perjudicada y en los casos más graves teniendo consecuencias de carácter penal, administrativas conllevando sanciones y, por último, consecuencias deontológicas que pueden tener por ejercer una determinada profesión.

El deber de preservar los datos de salud se ha visto amparado durante la declaración del estado de alarma. Por lo que durante ese tiempo lo derechos y garantías se han seguido respetando, utilizándose aquellos datos que sean imprescindibles para conseguir la finalidad que se buscaba (geolocalización para saber quién había sido positivo, otorgando esta información de una forma anónima):

SEXTA: El paciente podrá ejercer diferentes derechos específicos, que ostentan los titulares de datos de salud, al responsable del tratamiento. Por lo que, podrá solicitar que se rectifiquen o supriman aquellos datos que no se estén tratando conforme a la actual normativa sobre protección de datos, es decir, aquellos que no sean exactos o correctos; teniendo el interesado la facultad de cancelar, para posteriormente bloquear, aquellos que no fueran adecuados o que fueran excesivos. El paciente también tendrá la facultad de poder oponerse

a aquellos datos que estén siendo tratados en basé a un interés legítimo, solicitando, si el interesado considera oportuno, la suspensión del tratamiento.

En relación con los datos de salud, el profesional sanitario será quien determine específicamente que datos pueden ser suprimidos. Aquí surge un gran problema ya que los datos de salud nunca se convierten en impertinentes, innecesarios e inadecuados, ya que estos datos suelen tener una importancia en el futuro que ayudan a que el tratamiento del profesional médico hacia el paciente sea mejor. Es por ello por lo que, el derecho de cancelación hacia estos datos no se dé con frecuencia y si de una forma excepcional.

SÉPTIMA: A la hora de realizar este trabajo hemos observado la evoluación que ha tenido la normativa sobre protección de datos y más concretamente los datos de salud. Podemos observar que está nueva normativa ha hecho que la protección de la privacidad en relación con los datos de salud sea cada vez mejor, reforzándolo más que la ley anterior, ofreciéndole al paciente unas mayores garantías.

La evaluación de impacto antes de tratar los datos de salud y la nueva protección, fundamentándose en las medidas proactiva y preventivas que se le da a estos datos suponen una garantía extra a la hora de protegerles.

Podemos llegar a la conclusión de que, después de haber analizado como afecta en el ámbito sanitario y de la salud la totalidad de los sistemas que engloban la protección de datos de carácter personal (jurisprudencia, resoluciones de la AEPD, normativa jurídica, doctrina): la regulación actual sobre la protección de dados ha añadido mayor protección al garantizarla de una manera más adecuada y adaptando nuevos contornos que pueden verse afectado por las nuevas tecnologías.

Los datos de salud son una categoría especial de datos, ya que su finalidad es diferente, ya que su recopilación puede ser utilizada como medio de curación y protección de la salud. Por lo que se encuentra bastante diferenciado con el resto de datos de carácter personal. Es

por lo que estos datos necesitan una protección mayor que el resto de los datos. Esta garantía no solo se ha manifestado a la hora de prohibir que se traten estos datos, salvo que haya consentimiento del titular y haya una finalidad existente, sino respetando sus especificidades a la hora de compararlos con los diferentes datos generales y también con los datos de la misma categoría. Es por eso por lo que durante el desarrollo de este trabajo podamos observar que, los datos de salud tienen unas características muy particulares (véase el ejemplo del plazo de conservación de los datos de salud) que se encuentran reguladas por la normativa sanitaria (por ejemplo, LBAP). Este hecho ha conllevado que los titulares de estos datos hayan tenido otro tratamiento diferente si lo comparamos con el resto de los datos de carácter personal.

Por lo que, a la hora de aplicar una normativa, es preferible que se apliquen aquellas normativas de carácter sanitario. Este hecho no se puede aplicar de una forma estricta, ya que la normativa del RGPD tiene aplicación directa: por lo que, tendrá que haber una aplicación coordinada y equilibrada entre el RGPD y la LOGPD y la normativa sanitaria. Ante todo, habrá que buscar el beneficio del paciente y poder mejorar así la asistencia sanitaria del mismo.

11. BIBLIOGRAFÍA.

AGÚNDEZ LERÍA, I.: "Artículo 8. Principios relativos a la calidad de los datos. Protección de datos. Comentarios al Reglamento", Lex Nova, Valladolid, 2008, págs. 140 y ss

ÁLVAREZ CARO, M.: "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones…", en Reglamento General de Protección de Datos, Reus, 2016, pág. 227-240.

ÁLVAREZ CARO, M.: "El derecho a la supresión o al olvido", Reus, 2016, págs.241 y ss.

ÁLVAREZ CIVANTOS, O.: "Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades. 3ª edición", Auren, Granada, 2008, pág.16

ÁLVAREZ HERNANDO, J.: "Guía Práctica sobre Protección de Datos. Cuestiones y Formularios", Lex Nova, Valladolid, 2011, pág. 64

APARICIO SALOM, J.: "Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal", Aranzadi, Pamplona, 2000, pág.81.

APARICIO SALOM, J., "Derechos del interesado (Arts. 12-19 RGPD. Arts. 11-16 LOPDGDD)", Wolters Kluwer, Madrid, 2019, págs. 345-346

ARIAS POU, M.: "Definiciones a efectos del Reglamento general de protección de datos", en Reglamento General de protección de datos, 2016, págs. 115-134.

ATELA BILBAO, A. y otros: "Autonomía del paciente, información e Historia clínica (Estudios sobre la Ley 41/2002, de 14 de noviembre)", Thomson-Civitas, Pamplona, 2004, pág. 65

CARNICERO GIMÉNEZ DE AZCÁRATE, J.: "El derecho a la protección de datos en la historia clínica y la receta electrónica", Aranzadi, Pamplona, 1999, págs. 289-304

COLLADO GARCÍA-LAJARA, E., Protección de datos de carácter personal (legislación, comentarios, concordancias y jurisprudencia), Comares, Granada 2000, pág. 25.

CONDE ORTIZ, C.: "La protección de datos personales. Un derecho con base en los conceptos de intimidad y privacidad", Dykinson, Madrid, 2005, págs.19-23.

DAVARA RODRÍGUEZ, M.: "Una primera aproximación al Reglamento europeo de protección de Datos y su incidencia en el tratamiento de datos de carácter personal de las Administraciones Públicas", Actualidad Administrativa, Revista Acta Judicial,2018.

DE MIGUEL BERIAIN y DE LORENZO Y APARICIO, Claves prácticas sanitarias. Datos genéticos y…, , pág. 31,

DE LORENZO Y MONTERO, R.: "Derechos y obligaciones de los pacientes. Análisis de la Ley 41/2002, de 14 de noviembre, básica reguladora de autonomía de los pacientes y de los derechos de información y documentación clínica", Colex, Madrid, 2003.

DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación", Derecho y salud, 2018, pág. 235.

FERNÁNDEZ COSTALES, J.: "El contrato de servicios médicos", Civitas, Madrid, 1988, págs. 216-217.

FERNÁNDEZ-SAMANIEGO, J.: y FERNÁNDEZ LONGORIA, P, "El derecho a la portabilidad de datos", en el reglamento general de protección de datos, 2016, pág.273.

FERNÁNDEZ-RUIZ GÁLVEZ, E.: "Intimidad y confidencialidad en la relación clínica", Servicio de Publicaciones de la Universidad de Navarra, Persona y Derecho, Pamplona, 2013, págs. 61-63.

GALLEGO RIESTRA, S., "Los derechos de acceso, rectificación, cancelación y oposición del paciente sobre su historia clínica", en Derecho y Salud, 2016, pág. 140

GARRIGA GONZÁLEZ, A., citando a DENNINGER, E.: "El derecho a la autodeterminación informativa", en PÉREZ LUÑO, A., E.: "Problemas actuales de documentación y la información jurídica", Tecnos, Madrid, 1987, pág. 273.

GONZÁLEZ GARCÍA, L., "Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos",en Derecho y Salud, 2014, pág. 276.

GUTIÉRREZ GUTIÉRREZ, I., "Dignidad de la persona y derechos fundamentales", Marcial Pons, Madrid, 2005, Pág.85.

HERRAN ORTIZ, A, "El derecho a la protección de datos personales en la sociedad de la información", Cuadernos Deusto de Derechos Humanos, Universidad de Deusto, 2003.

LIZARRAGA BONELL, E.: "La información y la obtención del consentimiento", Thomson-Civitas, Madrid, 2004, págs. 226-228

LÓPEZ, P.; MOYA, F: "Protección de datos de salud. Criterios y plan de seguridad", Madrid 2001, pág. 5.

MARTÍNEZ MARTÍNEZ, R.: "Tecnologías de la Información, Policía y constitución", Tirant lo Blanch, Valencia, 2001, págs. 203-203

MARTÍNEZ ROJAS, A.: "Principales aspectos del consentimiento en el Reglamento General de Protección de Datos de la Unión Europea", Aranzadi, 2016, págs. 4 y ss.

MURILLO DE LA CUEVA, P.L. y PIÑAR MAÑAS, J.L.: "El Derecho a la autodeterminación Informativa", Fundación coloquio jurídico europeo, Madrid, 2009, pág. 101.

MURILLO DE LA CUEVA, L, P.: "El derecho a la autodeterminación informativa y la protección de datos personales", Sociedad de Estudios Vascos, San Sebastián, 2008, págs.43-58

MURILLO DE LA CUEVA, L: “Las viscitudes del derecho de la protección de datos personales”, Revista Vasca de Administración pública, 2000, págs. 211-235.

NICOLÁS JIMÉNEZ, P.: "Investigación biomédica y big data sanitarios". En: TRONCOSO REIGADA, A.: “Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos de Carácter Personal”. Thomson Reuters, 2019. pág. 7.

ORDÁS ALONSO, M., “Intimidad, secreto médico y protección de datos sanitarios” en GARCÍA AMADO, J.A. (Coord.) Razonar sobre derechos, Tirant lo Blanch, Valencia, 2016, pág. 781 y ss.

ORTÍ VALLEJO, A.: “Derecho a la intimidad e informática” (Tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada); edit. Comares, Granada, 1994, pág. 109.

PÉREZ VELASCO, M.M.: “Los Ficheros Públicos, Estudios sobre Administraciones Públicas y Protección de Datos Personales”, Thomson-Civitas y APDCM, Madrid, 2006, págs. 4 y ss.

PIÑAR MAÑAS, J.L: “El nuevo Reglamento Comunitario de Protección de Datos”, Reus, 2016, págs. 15-22

PUYOL MONTERO, J.: “Los principios del derecho a la protección de datos”, Reus, Madrid, 2016, págs. 135-150.

REBOLLO DELGADO, L., “Derechos de la personalidad y datos personales”, Revista de Derecho Público, 1998, pág. 158.

SANCHEZ CARO, J.: "Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales", 2021, , págs. 1181-1200

ROMEO CASABONA, C.M.: "Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal", Aranzadi, 2010, págs. 226-256.

ROMERO CASABONA, C. M.: "Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías", Poder Judicial, núm. 31, 1993, pág.168.

SÁIZ RAMOS, M. y LARIOS RISCO, D., "El derecho de acceso a la historia clínica por el paciente: Propuesta para la reserva de anotaciones subjetivas", en Derecho y Salud, 2009, págs. 26-27

SÁNCHEZ-CARO, J. y ABELLÁN, F.: "Datos de salud y datos genéticos", Derecho Sanitario Asesores, Granada, 2004, págs. 103-111.

SÁNCHEZ URRUTIA, A.V.: "Información genética, intimidad y discriminación", Acta Bioética, 2002.

SERRANO PÉREZ, M.M.: "El derecho fundamental a la protección de datos. Derecho español Comparado", Aranzadi, Pamplona 2004, pág. 33 y ss.

SERRANO PÉREZ, M.M.: "El derecho fundamental a la protección de datos. Derecho español y Comparado", Aranzadi, Pamplona 2004, págs. 258-260

STEINMEYER ESPINOSA, A.: "¿Permite el derecho de acceso a la información pública, el acceso a datos personales?", Universidad Tecnológica Metropolitana, Chile, 2013, pág. 10

SUÁREZ RUBIO, M.J.: "Constitución y privacidad sanitaria", Tirant Lo Blanc, Valencia, 2017, pág. 53, con cita de DÍEZ-PICAZO GIMÉNEZ, L.M., en su libro "Sistema de Derechos fundamentales", Thompson, Madrid, 2013, pág. 41 y 42

VERDÚ PASCUAL, V.F.: "Secreto profesional médico. Normas y usos", Comares, Granada, 2005, pág. 15 y ss.