Soraya Sayah Olasolo

¿cómo impacta la protección de datos en la investigación sanitaria?

Trabajo final de Máster Acceso a la Abogacía dirigido por

Eduard Blasi Casagran

Universitat Oberta de Catalunya

2021

Agradecimientos

Quisiera dar las gracias a mi tutor, Eduard Blasi, abogado y vicepresidente tercero APEP, por guiarme por este viaje y aportar luz cuando me he perdido. Sin él estas paginas no tendrían sentido.

A mi familia, a la Dra. Silvia Olasolo i Ausió i Celia Olasolo i Ausió, fisioterapeuta, sanitarias que han aportado su experiencia y conocimiento en todo momento.

A mi equipo, al EAP Martí Julià, en especial al Dr. Manrique, Dra. Botanes y a Sandra Gómez, enfermera, todos ellos insaciables de conocimiento y paciencia.

Resumen

El presente trabajo tiene por objeto el análisis de cómo impacta la protección de datos de los usuarios en la evolución tecnológica, en concreto en el área de la investigación sanitaria. Se tratarán conceptos como el BIG DATA y la Inteligencia Artificial, y como se pueden interrelacionar con el ámbito sanitario de una manera más estrecha.

Resum

El present treball té per objecte l'anàlisi de com impacta la protecció de dades dels usuaris en l'evolució tecnológica, en concret en l'àrea de la investigación sanitària. Es tractaràn conceptes com el BIG DATA i la Inteligència Artificial i com es poden interrelacionar amb l'àmbit sanitari d'una manera més estreta.

Abstract

The purpose of this work is to analyze how data protection impacts on technological evolution, specifically in the area of healthcare research. Concepts such as BIG DATA or Artificial Intelligence will be discussed, and how they can be more closely interlinked with the health field.

Keywords / Palabras clave: RGPD, BIG DATA, IA, Protección de Datos Personales, sanidad

Índice

1. ORIGEN Y EVOLUCIÓN DE LA PROTECCIÓN DE DATOS 6

2. OBJETIVOS 11

3. ¿CÓMO CONSEGUIR EL USO EXTENDIDO DEL BIG DATA EN EL SECTOR DE LA SALUD? 14

A) MEDICAL DEVICES 14
B) WEARABLES 14

4. BASES LEGITIMACIÓN 16

A) INTERÉS PÚBLICO 16
B) INTERÉS LEGÍTIMO 16
C) CONSENTIMIENTO 16

5. ¿CUÁL ES EL IMPACTO DE NO APLICAR CORRECTAMENTE UNAS POLÍTICAS O PROCEDIMIENTOS DE PROTECCIÓN DE DATOS EN ESTE SECTOR? 18

6. CONCLUSIONES 20

7. BIBLIOGRAFÍA 21

1. Origen y evolución de la Protección de Datos

La Protección de Datos no pretende proteger cualquier dato sino únicamente aquéllos que son datos de carácter personal. Como veremos, la Protección de Datos no busca proteger propiamente a los datos sino a las personas e individuos que hay detrás de estos. Concretamente, según la Comisión Europea, entendemos el concepto de dato personal como *"cualquier información de una persona física viva identificada o identificable"*, por otro lado, el RGPD lo define como *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables".*

Aunque en el Convenio Europeo de Derechos Humanos (CEDH) de 1950 ya se especifica que la persona tiene derecho a la protección de sus datos personales, no fue hasta la década de los 60, debido al boom del sector informático, que la recopilación y acceso a datos de carácter personal se fue haciendo cada vez más común y empezó a alertar a la sociedad europea sobre una necesaria regulación, generando debates por todo el continente, hecho que dio lugar en la Unión Europea, concretamente en Alemania, a la primera Ley Federal Alemana de Protección de datos en 1976. En los siguientes años se sumaron a la implementación de normativa específica otros países europeos como Dinamarca, Francia o Noruega.

La legislación fue evolucionando, tratando de alcanzar el ritmo vertiginoso de la tecnología en aquel entonces, por lo que a principios de la década de los 80 surgió el Convenio nº 108 del Consejo de Europa, para la protección de datos de las personas con respecto al tratamiento automatizado de datos de carácter personal. Este documento sigue vigente y sufrió una actualización el pasado año 2018 y lo que en un principio se ideó para tener un alcance a nivel europeo trascendió más allá del atlántico, firmándolo países como Uruguay y transformándolo en un documento jurídicamente vinculante internacional y vinculado con directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE).

El Convenio tiene como objeto la protección de la vida privada de las personas, así como velar por un uso correcto de sus datos personales. Esto implica que los Estados firmantes deben establecer Autoridades de control independientes y no pueden desligarse de los principios regentes.

Al abrirse una ventana al flujo de datos entre Estados, europeos o no, el Parlamento Europeo y el Consejo elaboraron en la década de los 90' la Directiva 95/46/CE relativa a la libre circulación de datos

y a su tratamiento. Dicha normativa, fue traspuesta por España en 1999 tras la aprobación de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, o lo que es lo mismo, la primera LOPD. Pero esta normativa no fue pionera en España, puesto que en 1992 entró en vigor la LORTAD, Ley Orgánica aunque esta no regulaba todos los tratamientos con datos personales, sino que únicamente se limitaba a aquellos automatizados (o de forma informática).

Ciertamente en 1995 fue cuando el concepto internet se dio a conocer y a hacerse accesible para gran parte de la sociedad, pero en 2003, tras el primer informe sobre la aplicación de la Directiva 95/46/CE, cuando se empezó a dilucidar la necesidad de mejorar la aplicación de dicha Directiva y adaptar la legislación a los tiempos que venían. La realidad es que la Directiva 95/46/CE nació en un contexto donde el acceso a internet estaba al alcance de sólo algunos, y la irrupción de Internet en todos los hogares empezó a presentar la necesidad de actualizar y adaptar la normativa a los nuevos tiempos.

A partir del año 2007, la Comisión Europea estimó que la Directiva fue traspuesta correctamente, y poco después, en 2009 Europa elaboró su Carta de Derechos Fundamentales a través del Tratado de Lisboa y el derecho a la protección de datos personales fue consolidado en la Unión Europea.

En 2010 se dio una disrupción tecnológica donde nuevos retos aparecieron al ocasionarse lo que es conocido como FAANG STOCKS, o lo que es lo mismo, la salida a bolsa (Nasdaq) de superpotencias de la tecnología (inicialmente fueron Facebook, Amazon, Netflix y Google y más tarde se unió Apple). Este hecho evidenció que era necesario reforzar los derechos de las personas, la protección de sus datos, pero no únicamente en el ámbito de las redes sociales, sino en todos los ámbitos donde intervino la tecnología, y era muy complicado regularla puesto que, nuevamente se evidenció que el Derecho siempre va por detrás de esta y era complicado predecir cómo iba a evolucionar la tecnología. La tecnología avanzaba mucho y más rápido y como consecuencia, la protección de datos debía ir de ala mano de ésta, sin frenar la evolución, sino facilitándola, pero hacerlo con garantías. Al hilo de la evolución tecnológica, en septiembre de 2014, se publicó un documento que indicaba que *"data protection principle are no longer valid and appropriate for the development of big data"*[1], es decir, que los principios de protección ya no se consideran validos ni apropiados para el desarrollo de BIG DATA y los propuso como objeto de mejora para el futuro próximo, vislumbrando también la necesidad de iniciar una cooperación internacional en aras de unir fuerzas y avanzar en el campo del BIG DATA tanto

[1] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

a nivel nacional, regional e internacional, proponiendo un marco jurídico de aplicación a nivel global ya que el BIG DATA suponía retos comunes y no entendía de fronteras físicas entre países.
Con la evolución de internet y la irrupción de los dispositivos inteligentes en la sociedad, en 2012 se llegó a la conclusión de que la reforma europea en materia de Protección de Datos no podía correr nuevamente sobre una Directiva, sino un Reglamento[2], con el fin de armonizar la normativa entre los Estados Miembros y evitar divergencias sobre aspectos principales entre países de la Unión Europea. Tras cuatro años intensos, en 2016,[3] con presiones por parte de compañías y gobiernos de distintos países[4], el Parlamento Europeo y el Consejo aprobó el Reglamento General de Protección de Datos (en adelante, RGPD), que entró en vigor el mismo año y no fue de obligado cumplimiento hasta 2 años más tarde.

El RGPD introdujo varias herramientas para encarar los distintos retos que presentaba el BIG DATA y otras tecnologías. Tras la plena aplicación del RGPD, el concepto BIG DATA siguió creciendo e integrándose cada vez más en organizaciones públicas y privadas. Hay que tener en cuenta que sólo en España el BIG DATA generó ingresos por encima de los 170 millones de euros en el año 2017[5]

Pero antes de conocer más aspectos sobre el BIG DATA y cómo ha impactado en el campo de la salud es necesario conocer bien el concepto de BIG DATA:

BIG DATA se entiende como un tratamiento de grandes cantidades de información con fines analíticos, para realización de perfiles, con fines predictivos, etc. Se entiende como tal el conjunto de datos e información de gran volumen y complejidad que debido a su velocidad de crecimiento se hace muy difícil de gestionar y procesar con herramientas de gestión de bases de datos convencionales. Así pues, no podemos considerar el BIG DATA como una red de información ni una plataforma, ya que no tiene una estructura determinada y las fuentes son muy diversas, como lo pueden ser dispositivos, búsquedas en internet, redes sociales, entre otras. A título meramente orientativo, el tratamiento de datos de BIG DATA difícilmente cabrían en una hoja Excel y por tanto hablamos de procesamientos a gran escala, frecuentemente con sistemas y programas sofisticados.

[2] LexUriServ.do (europa.eu)
[3] 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 (Reglamento general de protección de datos) (boe.es)
[4] EE UU presiona en la sombra para frenar la normativa de privacidad europea | Internacional | EL PAÍS (elpais.com)
[5] Big Data en España: radiografía de este mercado en nuestro país (enzymeadvisinggroup.com)

El hecho de tener tal cantidad de datos de todo tipo abre muchas puertas a diversos sectores, no solo a empresas y comerciales, sino también a otros ámbitos que nos afectan a todos, como lo es el sanitario. El sector de la salud es uno de los más afectados en este sentido. Las técnicas y mecanismos utilizados en esta área cada vez son más avanzados y el volumen de datos de usuarios inmenso. Pensemos que Gracias al BIG DATA, los expertos con acceso a los datos correctos pueden predecir principios de pandemia, tendencias de la gripe, el inicio de infecciones potencialmente mortales antes de que aparezcan los síntomas físicos.[6]

Hasta el momento el volumen de datos con el que se ha trabajado ha sido de un tamaño considerablemente reducido. Se ha podido gestionar con cierta facilidad con las herramientas que teníamos, pero el concepto BIG DATA ha hecho que nos replanteemos nuestros límites. Se es consciente de que explotar esta información se escapa de las manos y de la mente humana por su complejidad, pero a raíz de esta necesidad nace una opción, la Inteligencia Artificial.

A fin de poder optimizar esta BIG DATA en el sector de la salud, una de las herramientas que se pueden usar es la implementación de la Inteligencia Artificial (en adelante IA). Gracias a la elaboración de algoritmos y a la asignación de análisis de parámetros y valores concretos la IA puede ser un complemento perfecto para el BIG DATA, permitiendo explotar todo su potencial. Por citar algún ejemplo, gracias al sistema de reconocimiento de voz aunado con parámetros médicos (tono de voz, agitación o respiración) se creó la herramienta conocida como CORTI[7], usada en llamadas de emergencia para detectar si el usuario que contacta está sufriendo una parada cardiorrespiratoria. De este modo, la IA ayuda en la toma de decisiones del equipo médico en tiempo real. En la misma línea, una empresa española ha desarrollado recientemente un parche que permite administrar fármacos a través de la piel y recabar datos sobre la salud del paciente[8].

EN lo que respecta a su definición, el Parlamento Europeo[9] define la IA como la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento y el aprendizaje o la capacidad de planear. Permite que los sistemas informáticos que la integran perciban los datos de su entorno y sea capaces de tratarlos para resolver situaciones.

[6] El alcance del Big Data en España, un mar de oportunidades (xataka.com)
[7] https://www.corti.ai
[8] La startup que quiere escribir el punto final de las agujas (abc.es)
[9] ¿Qué es la inteligencia artificial y cómo se usa? | Noticias | Parlamento Europeo (europa.eu)

No solo a nivel europeo sino también mundial, la implementación de la IA está tomando cada vez un papel más relevante en la transformación digital de sectores como sanitarios y de naciones enteras, siendo una prioridad para algunos de sus gobiernos. Sin ir más lejos, en España, el pasado mes de diciembre de 2020, se introdujo la Estrategia Nacional de Inteligencia Artificial[10] con la finalidad de establecer unos parámetros base regulatorios a fin de que esta tecnología esté al servicio de una sociedad más moderna y justa, tal y como ha anunciado recientemente Carme Artigas, secretaria del Estado de digitalización e Inteligencia Artificial del Gobierno de España. Ahora bien, en su discurso, identificaba una clara necesidad, y no es regular la evolución tecnológica o de IA, puesto que si se regula *ex ante* se estará frenando y limitando la capacidad de innovación, sino que lo que verdaderamente es mandatorio es la regulación de los usos de esta tecnología

Tenemos claro cual es el futuro: la tecnología y digitalización, pero ¿la legislación actual está a la altura de las circunstancias? El contexto sanitario en el que estamos viviendo y la aceleración en cuanto a estrategias digitales se refiere ha dejado entrever que el actual RGPD debería ser revisado a fin de poder establecer unas bases legislativas acordes con la evolución de la sociedad. En este sentido, en marzo de 2021, Axel Voss, parlamentario europeo de la UCD alemana y uno de los padres del Reglamento General de Protección de Datos que entró en vigor en Europa en 2018, opina que la norma ya se está quedando obsoleta, sosteniendo en una de sus declaraciones que *"el RGPD no se hizo ni para el blockchain, ni para el reconocimiento facial o de voz, ni para el minado de datos o la inteligencia artificial".*[11]

[10] https://www.ciencia.gob.es/portal/site/MICINN/menuitem.26172fcf4eb029fa6ec7da6901432ea0/?vgnextoid=70fcdb77ec929610VgnVCM1000001d04140aRCRD

[11] https://www.businessinsider.es/rgpd-ha-quedado-obsoleto-responsables-822071

2. Objetivos

Debemos tener presente que el Derecho a la intimidad, y el derecho a la protección de datos, de creación jurisprudencial[12], forma parte de los Derechos y Libertades constitucionalmente protegidos. El honor y la privacidad deben estar asegurados para poder vivir con libertad.

A pesar de ello, cada vez, gracias o a causa de la tecnología, es más fácil el acceso a cantidades ingentes de información. Ello comporta que en los últimos tiempos y de manera casi periódica, oigamos casos de *hackeo* y compraventa de grandes volúmenes de datos, ciberataques que afectan a todo tipo de empresas y entidades y de lo que hablaré más detalladamente más adelante.

Estas situaciones pueden ocasionar grandes *"crashes"*, pero cobra un sentido distinto cuando lo que está en juego no es solo el coste, sino algo mayor como es la salud de ciudadanos, de pacientes y usuarios. Según datos objetivos, cada brecha de seguridad costó de media al sector sanitario 5,9 millones de euros en 2020. Sin duda el mayor coste sectorial.[13] Pero el coste que ello supone no es el mal mayor de los daños. En 2019 un Hospital rural de EE. UU. sufrió un ataque *Ransomware* y algunos de sus pacientes tuvieron que ser trasladados a más de 200 km (125 millas), a otro Hospital para que pudieran continuar su tratamiento. Las consecuencias informáticas en el ámbito de la salud pueden poner en juego la vida de las personas.

Sin duda la seguridad es uno de los aspectos más importantes. Crear un entorno seguro para la gestión y tratamiento de datos personales, hoy día, es un punto vital para cualquier persona, tanto física como jurídica, a fin de poder aportar seguridad a su actividad, desde una transferencia bancaria hasta la aplicación de un algoritmo para detectar de manera precoz una enfermedad.

Cada usuario, a lo largo de los años genera una gran cantidad de datos. Estos datos de fuentes diversas se pueden identificar como el BIG DATA de un usuario concreto. En el sector de la salud, trabajar con estos datos juntamente con una tecnología capaz de analizarlos como la Inteligencia Artificial, puede conllevar a un paradigma evolutivo: la predicción de enfermedades y la prevención de la salud, entre otros.

[12] Ágora-ElDerechoFundamentalALaProteccionDeDatosPerspectiv-2372613.pdf
[13] Cada brecha de seguridad costó al sector sanitario 7 millones de dólares (isanidad.com)

Teniendo acceso a todo un sistema de información que contenga datos sanitarios, un programa de Inteligencia Artificial dotado de los valores requeridos puede tratar de establecer patrones que ayuden a prever un comportamiento determinado en un estudio de una patología, pudiendo aplicar métodos preventivos para que esta se no desarrolle, evitando, por ejemplo, que un paciente llegara a enfermar o que la dolencia se agravara[14].

Ahora bien, a menudo para lograr sistemas de IA que funcionen correctamente resulta imprescindible entrenar el algoritmo de predicción, con datos de varios pacientes y durante un prolongado tiempo. Esta técnica es comúnmente conocida como el "*machine learning*". El "*machine learning*" permite nutrir el algoritmo de datos y patrones en aras de conseguir mayor fiabilidad y precisión. Sin embargo, para poder trabajar con "*machine learning*" en el campo de la salud es necesario que los datos puedan reutilizarse. La reutilización de los datos en el ámbito de la investigación sanitaria es sin duda una necesidad presente. En este sentido, de acuerdo con las palabras de Mar España, Directora de la Agencia Española de Protección de Datos (AEPD) en el reciente Congreso Internacional de Derecho Digital, estos datos se han de pode reutilizar[15]. En la actualidad, se aplica una protección absoluta sobre los datos de salud que a menudo dificulta la reutilización de los mismos y los avances en el campo de la investigación. De acuerdo con el principio de limitación de finalidad, consagrado en el RGPD, los datos pertenecientes a un individuo son usados para un fin concreto, por ejemplo, un estudio determinado, y no pueden usarse esos mismos datos para un estudio distinto. Ahora bien, la normativa Española de Protección de Datos, la Ley Orgánica de Protección de Datos Personales y garantía de derechos digitales, establece en su disposición adicional 17 la posibilidad de reutilizar los datos en el campo de la investigación de la salud. Dicha disposición adicional es a fecha de hoy una de las únicas herramientas legales que habilitan para la reutilización de información al sector sanitario, cauteloso y a menudo ultraproteccionista con la información que consta en las historias clínicas de los pacientes.

Reutilizar o compartir información no debe ser concebido como un sinónimo de perder el control de la información. Compartir o reutilizar es imprescindible para lograr avances significativos en el sector, sin que ello implique gozar de menos protección o garantías sobre los datos. En Cataluña, por ejemplo, existe la "HC3", la Historia Clínica Compartida. El uso de esta herramienta implica que los datos clínicos de usuarios atendidos en la red pública sanitaria de la Comunidad Autónoma puedan ser consultados entre los centros que forman la propia red en caso de necesidad. Lo que se plantea es ir un paso más allá y dar acceso a estos datos de carácter sanitario a todos los equipos de profesionales facultativos,

[14] https://www.ccma.cat/324/marcapassos-amb-control-remot-per-fer-el-seguiment-dels-pacients-fora-de-lhospital/noticia/3094948/

[15] https://www.enatic.org/evento/5/congreso-internacional-de-derecho-digital-de-enatic/

medicina, enfermería o investigación, bajo el criterio de una necesidad demostrable y proporcional. Evolucionar a un sistema de compartición europeo, no solo autonómico, bajo una misma regulación, que permita que todos los centros sanitarios y profesionales vayan hacia una misma dirección y poder, por ejemplo, mejorar el ámbito de la investigación.

El implementar, por ejemplo, sistemas de Inteligencia Artificial aporta un acompañamiento en la toma de decisiones basado en el análisis de BIG DATA que el humano, por la inmensidad del volumen de los datos, es incapaz de procesar, pero que usando las directrices indicadas puede combinarse a fin de conseguir, por ejemplo, una medicina personalizada, aumentando la esperanza y calidad de vida de la población.

Hasta el momento, los recursos que se han venido aplicando a fin de proteger los datos de los usuarios en investigación, por ejemplo, han sido la anonimización y la minimización, pero a menudo se sesga la usabilidad, destruyendo el factor vital del dato en sí y dejándolo estéril. La anonimización a menudo no resulta viable en el campo de la salud. En este escenario, diversos especialistas e investigadores del sector abogan por la pseudoanonimización, implementando robustas medidas de protección, pudiendo así garantizar la privacidad de los pacientes, sin que ello juegue en detrimento de su salud.

Tengamos en cuenta que la Inteligencia Artificial es compuesta generalmente por sistemas complejos que disponen de componentes y algoritmos, pero no hay que olvidar que los datos son el nutriente o componente esencial para que los algoritmos funcionen correctamente. Por este motivo es vital que los datos que se usen sean útiles y a la vez reales.

3. ¿Cómo conseguir el uso extendido del BIG DATA en el sector de la salud?

En la línea de lo mencionado anteriormente, un usuario, a lo largo de su vida, genera gran cantidad de datos, creando su propio entorno BIG DATA, ahora bien, no todos estos datos generados son de interés a nivel del sector salud.

Históricamente, los datos sanitarios se han originado directamente a través de las visitas presenciales de los usuarios a los centros de salud. No fue hasta finales de los 90 principios de los 2000 que se empezaron a digitalizar las historias clínicas y pasaron a formar parte, junto con las nuevas e-consultas, del BIG DATA sanitario.

Actualmente y gracias a diversos dispositivos, este BIG DATA de carácter clínico se nutre de muchas más fuentes de manera indirecta pero no todo dato se puede considerar como sanitario. En aras de mencionar los principales, existen dos grandes bloques en los que se pueden dividir los dispositivos generadores de información:

a) Medical Devices

El concepto *Medical Device* hace referencia a aquel equipo, usado con la finalidad específica de alcanzar un diagnostico o terapia, es decir, un dispositivo dotado de la tecnología necesaria capaz de emitir conclusiones mediante evaluación de datos y que puede acompañar a un profesional del ámbito a la toma de decisiones.

Algunos ejemplos de estos dispositivos pueden ser tensiómetros, electrocardiogramas o glucómetros. Todos evalúan datos o constantes del usuario y dan como resultados parámetros que pueden ser interpretables por el facultativo con el fin de pautar un tratamiento.

b) Wearables

Weareble es aquel dispositivo que se puede "vestir" o llevar encima y que a través de un microprocesador es capaz de generar métricas o detectar acciones.

En este sentido, aunque los *wearables* son dispositivos que aportan métricas, no todos son considerados *Medical Devices* o dispositivos médicos, puesto que para que sean considerados como tal

han de haber obtenido una certificación que los acredite a nivel europeo. Aun así, aquellos que no son considerados dispositivos médicos siguen siendo son útiles para que el usuario pueda llevar un control de su estado de salud. Un buen ejemplo de ellos son el *Apple Watch*, capaz de medir las pulsaciones o de generar un símil a un electrocardiograma.

Por otra parte, el avance tecnológico ha propiciado dos innovaciones que van a estar cada vez más presentes en el día a día de la sociedad y el sector sanitario.

Uno de estos grandes avances son las *Smart Pills*[16], también conocidas como medicinas inteligentes, pequeños comprimidos que contienen cámaras o sensores y que pueden ser usados en intervenciones quirúrgicas para lograr que estas sean menos lesivas y agresivas para el usuario, como por ejemplo en gastroscopias.

Por otra parte, tenemos los exoesqueletos. Diversos centros de investigación, como el Hospital Sant Joan de Deu, después de años de investigación ha logrado crear un exoesqueleto infantil que ayuda a pacientes con atrofia muscular espinal, afectación que impide la movilidad autónoma. De igual modo, España ha colaborado con Estados Unidos y Suecia para crear Blackfingers, una mano robótica que, mediante la recopilación de estímulos y ordenes a través de sensores, es capaz de usarse como una extremidad más.

Está claro que todas estas herramientas aportan una visión a la medicina personalizada esperanzadora, y nos hace pensar en todo lo que podemos llegar a conseguir con una legislación adecuada que permita una evolución transfronteriza.

[16] Smart pills could 'dumb down' medical care - EPR (europeanpharmaceuticalreview.com)

4. Bases legitimación

Otro punto importante es conocer la base (o bases) jurídica que permite tratar la información en el campo de la salud. ¿Cuándo podemos tratar los datos? La fuerza y motivación del tratamiento de datos personales en el sector sanitario se ha venido debatiendo desde hace un tiempo.

En enero del 2019 la EDPB (*European Data Protection Board*) adoptó una posición cuando se le planteó una consulta respecto al texto de preguntas frecuentes en relación entre el CTR (*Clinical Trial Regulation*)[17] y RGPD.

Veamos en primer lugar cuales son las bases de legitimación:

a) Interés Público

El procesamiento de datos personales podría considerarse "*necesario para el desempeño de una tarea llevada a cabo en interés público*" de conformidad con el artículo 6 (1) (e) del RGPD, el cual establece además que esta base será establecida por la legislación de la Unión o de los Estados miembros y que el propósito del tratamiento se establecerá en dicha base jurídica. El tratamiento de datos personales en el contexto de ensayos clínicos puede, por tanto, considerarse necesario para el desempeño de una tarea realizada en interés público cuando la realización de ensayos clínicos se enmarca directamente en el mandato, misiones y tareas conferidas a un ámbito público

b) Interés Legítimo

En este aspecto y en relación con el anterior apartado, los intereses del responsable prevalecen sobre los del interesado. Diversas Sentencias avalan esta posición siempre que se aplique una regla de ponderación con la cual se pueda valorar si en supuesto concreto a estudiar existe efectivamente un interés legítimo perseguido por el responsable del tratamiento o si se vulneran derechos y libertades fundamentales. Sin embargo, si bien el interés legítimo puede habilitar numerosos tratamientos en el ámbito de la salud, esta base jurídica no permite propiamente sustentar los tratamientos de datos de salud.

c) Consentimiento

[17] https://edpb.europa.eu/sites/default/files/files/file1/201903_edpb_opinion_ctrq_es.pdf

Históricamente ha sido base legitimadora, pero desde la implementación en 2018 del RGPD y hasta en la actualidad ha pasado a un segundo plano y se toma de manera subsidiaria, es decir, se toma el consentimiento cuando no son de aplicación ni el interés público ni en interés legítimo.

Se ha de hacer especial mención en que no es lo mismo el consentimiento en el trato de datos de carácter sanitario que el consentimiento informado en el sector sanitario.

El consentimiento informado ha de ser mandatorio puesto que en él se exponen las contraindicaciones y posibles riesgos o efectos adversos de un tratamiento o ensayo clínico. Así pues, este consentimiento, en materia de salud ha de existir. Pero este hecho no implica necesariamente que se esté otorgando un consentimiento válido para el trato de datos personales ni por ende que esté ligado al tratamiento de datos para investigación sanitaria. El consentimiento podría ser una base jurídica idónea para sustentar aquellos tratamientos derivados de la medicina personalizada y que supongan un tratamiento individualizado del paciente.

Teniendo en cuenta, como se ha dicho anteriormente, que los datos son pseudoanonimizados o encriptados, ¿es necesario un consentimiento explicito adicional para que sean tratados?
¿Aplicando y manteniendo las debidas medidas de seguridad, donde solo se obtienen datos no asignables a un individuo reconocible, debería primar un interés por un bien mayor?

5. ¿Cuál es el impacto de no aplicar correctamente unas políticas o procedimientos de protección de datos en este sector?

En los últimos tiempos el concepto de dato personal ha trascendido de tal manera que ha llegado a convertirse en objeto de ataques, secuestro y moneda de cambio, convirtiéndose en un valor en si mismo.

Como he comentado anteriormente, estamos oyendo de manera casi diaria que han habido *hackeos* en una u otra empresa, que ha habido una brecha de seguridad y como consecuencia se han filtrado miles o millones de datos de usuarios. Cada vez con más asiduidad ocurre que bases de datos son corrompidas con el objetivo de sustraer datos con una clara finalidad, conseguir dinero, ya sea a modo de rescate o de venta.
Cuando estas brechas de seguridad o fugas de datos causadas por ciberataques se dan, pensamos que el victimario podrá tener acceso a nuestra información, como cuenta corriente o teléfono, pero todo esto cobra un especial sentido cuando detrás de estos datos sustraídos se encuentran personas con patologías reales y que su tratamiento puede verse afectado y su calidad de vida mermado.

Uno de los casos más conocidos de como puede afectar un ciberataque a la salud se dio el pasado 2020, en plena pandemia, en el Hospital Universitario de Dusseldorf, Alemania. El sistema informático del Hospital sufrió el ataque de un *ransomwere* (secuestro de datos), motivo por el cual el sistema de registro quedó inutilizado y no se puedo aceptar a pacientes. Una usuaria que acudió al centro, ante tal situación se vio en la necesidad de desplazarse a otro centro médico, libre de ataques maliciosos, a fin de ser tratada. Desgraciadamente la usuaria falleció. [18]

Otro de los ejemplos más recientes es el sufrido por el Ministerio Irlandés de Salud que el mes de mayo de este año sufrió un intento de secuestro de datos. El Centro Nacional de Ciberseguridad detectó la invasión y se vio ante la necesidad de suspender parcialmente su sistema informático, a modo de precaución.

[18] https://www.securityweek.com/german-hospital-hacked-patient-taken-another-city-dies

El avance tecnológico es inevitable e imparable en todos los campos que nos puedan rodear como usuarios. Se trata de un hecho innegable. Nuestros datos son necesarios para nutrir esa red de la que hablábamos anteriormente. Pero no a cualquier coste. Por ello se debe construir alrededor de estos datos una normativa novedosa y en constante evolución.

A fin de evitar vulneraciones o que en el caso de que se sufran los daños sean mínimos es de vital importancia contar con un buen plan de seguridad y evaluación de impacto al instaurarse nuevas tecnologías, a través de la figura del *Data Protection Officer* o Delegado de Protección de Datos (en adelante DPO) y de manera previa al inicio del trato de datos. El DPO debe trazar un plan de seguridad acorde con la finalidad del trato que evite cualquier tipo de infracción o ilicitud en el proceso. Así mismo, deberá evaluar el impacto que provoque la instauración de nuevas tecnologías, como la IA, en el trato de datos, por ejemplo, cuando se pretenda elaborar perfiles clínicos automatizados con los que tomar decisiones que puedan conllevar efectos tanto jurídicos como sanitarios a una o varias personas físicas.

Otra herramienta para tratar de evitar filtraciones son las auditorias para evaluar el cumplimiento normativo. En la actualidad, en el sector sanitario, debido a la creciente implementación de IA, ha hecho necesario una actualización de los controles, añadiendo características específicas a evaluar, como por ejemplo el análisis de riesgos de datos de entrada con los que se vayan a tomar decisiones que puedan afectar a un individuo o colectivo.

6. Conclusiones

La pandemia del Coronavirus ha afectado a la población global y nos ha hecho replantear la importancia de la investigación científica y sanitaria, no sólo para mitigar los efectos de la pandemia sino para predecir y estar preparados de cara a las futuras pandemias o acontecimientos sanitarios que vendrán en el futuro. La Directora de la Agencia Española de Protección de Datos recordó que la *"la protección de datos no debería utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades"*[19] y por tanto la protección de datos, debería concebirse no sólo como una herramienta para protección de la información sino también para facilitar la investigación en la salud. A lo largo de este viaje hemos visto conceptos nuevos como *Medical Devices* y *wearables*, otros no tan nuevos como BIG DATA e Inteligencia Artificial. Hemos visto avances y logros tecnológicos impensables hace unos años y como, dotándolos de las herramientas jurídicas necesarias, podrán revolucionar el sector sanitario bajo la premisa de la prevención y la predicción.

Tras este recorrido llego a dos conclusiones:

1. El principio de la limitación de la finalidad complica en demasía y grava enormemente la evolución del sector. La tecnología, así como las necesidades de los equipos sanitarios e investigadores cambian y evolucionan constantemente, motivo por el cual es imposible prever las necesidades a 5 o 10 años vista, por ejemplo. En este sentido se debería tejer una red normativa capaz de velar por la seguridad y protección de los datos de los usuarios sin dejar atrás la interoperabilidad de estos en distintos proyectos o servicios.

2. La normativa vigente probablemente se haya quedado obsoleta y sea necesaria una revisión a fondo, dotando a la nueva legislación europea y con un carácter claramente transnacional de un equipo de profesionales cualificados que la hagan evolucionar a la par que lo hace la tecnología.

[19] La AEPD publica un informe sobre los tratamientos de datos en relación con el COVID-19 | AEPD

7. Bibliografía

- European Data Protection Board - EDPB (2019) - *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b)), Adopted on 23 January 2019.* *https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_es*

  Consorci de Salut I Social de Catalunya (2021). *Codi de Conducta per al tractament de dades personals en l'àmbit sanitari.* http://www.consorci.org/actualitat/noticies/1321/presentat-el-primer-codi-de-conducta-de-tractament-de-dades-en-lambit-sanitari-a-europa

- Agencia Española de Protección de Datos – AEPD (2020). *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial.* https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

- Autoritat Catalana de Protecció de Dades – APDCAT (2020). *Guía de Protección de Datos para Pacientes y Personas Usuarias de los servicios de Salud.* https://apdcat.gencat.cat/web/.content/03-documentacio/documents/Guia-proteccio-de-dades-pacients-v14-CAST.pdf

- Agencia Española de Protección de Datos – AEPD (2021). *Requisitos para auditorías de tratamientos que incluyan IA.* https://www.aepd.es/sites/default/files/2021-01/requisitos-auditorias-tratamientos-incluyan-ia.pdf

- Autoritat Catalana de Protecció de Dades – APDCAT (2018). *Dictamen en relació amb la consulta d'un centre sanitari sobre l'acord d'encarregat del tractament amb les empreses que monitoritzen assajos clínics*. https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2018/Documents/ca_cns_2018_059.pdf

- European Data Protection Supervisor (2020). *A Preliminary Opinion on data Protection and Scientific Research.* https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

- https://www.boe.es/doue/2016/119/L00001-00088.pdf