TFM GABRIEL PLANAS BASURTO

por GABRIEL PLANAS BASURTO

Fecha de entrega: 21-sep-2020 11:39a.m. (UTC+0200)

Identificador de la entrega: 1392746078

Nombre del archivo:
360069_GABRIEL_PLANAS_BASURTO_TFM_GABRIEL_PLANAS_BASURTO_2869618_1414627990.pdf
(702.96K)

Total de palabras: 22664

Total de caracteres: 121985

uc3m | Universidad Carlos III de Madrid

Máster Universitario en Derecho de las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información

Trabajo Fin de Máster

"INFORME PARA LA CONTRATACIÓN DEL SERVICIO MADRILEÑO DE SALUD DE UN SOFTWARE DE INTELIGENCIA ARTIFICIAL PARA EL DIAGNÓSTICO MÉDICO"

Gabriel Planas Basurto

Tutor:

Pr. Dr. D. José Vida Fernández

Madrid, septiembre de 2020

Resumen: La elaboración de este informe tiene como objetivo prestar asesoramiento jurídico-empresarial a la Spin-off de la UC3M *"Evidence-based Behavior"* sobre la implantación del software *eB2MC* de diagnóstico médico en el Servicio Madrileño de Salud. Adicionalmente, el informe incluye asesoramiento sobre su implantación en un hospital privado, o para un proveedor independiente de atención sanitaria.

A pesar de la aproximación eminentemente jurídica del informe, se pretende ofrecer una visión global de la realidad tecnológica actual y mostrar el abanico de posibilidades brindadas por la Inteligencia Artificial y el impacto producido en el ámbito sanitario. Para ello, se han analizado cuestiones tales como la naturaleza jurídica del software informático, la protección de datos personales, el procedimiento de contratación administrativa y la propiedad intelectual del Software.

ABREVIATURAS

- AEPD: Agencia Española de Protección de Datos.
- AIM: Acción Exploratoria de Informática Avanzada de Medicina.
- CAS: Consejo Asesor de Sanidad.
- CPI: Compra Pública de Innovación.
- EBB: Evidenced-based Behavior.
- EIPD: Evaluación de Impacto de Protección de Datos.
- ENS: Esquema Nacional de Seguridad.
- FENIN: Federación Española de Empresas de Tecnología Sanitaria.
- IA: Inteligencia Artificial.
- INCIBE: Instituto Nacional de Ciberseguridad
- LAP: Ley de Autonomía del Paciente.
- LCSP: Ley de Contratos del Sector Público.
- LOPDGDD: Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.
- MINHAFP: Ministerio de Hacienda y Administraciones Públicas.
- NDA: Non-Disclosure Agreement.
- RGPD: Reglamento General de Protección de Datos Personales.
- SERMAS: Servicio Madrileño de Salud.
- STJUE: Sentencia del Tribunal de Justicia de la Unión Europea.
- TIC: Tecnologías de la Información y la Comunicación.
- OMS: Organización Mundial de la Salud.
- OPTI: Observatorio de Prospectiva Tecnológica Industrial.
- TRL: Technology Readiness Level.
- TRLPI: Texto Refundido de la ley de Propiedad Intelectual.
- UE: Unión Europea.

ÍNDICE DE CONTENIDOS

I. INTRODUCCIÓN

1.1. Hacia la modernización de la sanidad pública……6

1.2. ¿Qué es la Inteligencia Artificial?.....6

1.3. El software "*eB2MC*". Características generales……....7

II. ANTECEDENTES Y EVOLUCIÓN DE LA SALUD ELECTRÓNICA.

2.1. Salud Electrónica y Estrategia Europea……..8

2.2. Plan de acción sobre la salud electrónica 2012-2020……8

2.3. Multiannual Work Programme (Red de e-Health)……....9

2.4. Integración de la e-Health en el Sistema Nacional de Salud……....10

2.5. Perspectiva empresarial……11

2.6. La Salud Digital, Inteligencia Artificial y Big Data. Factores relevantes……...12

III. ANÁLISIS JURÍDICO

1. El SOFTWARE *eB2MC* COMO PRODUCTO SANITARIO......14

1.1. Marcado CE. Clasificación y procedimiento de obtención……17

2. PROTECCIÓN DE DATOS PERSONALES.……..18

2.1. Datos relativos a la salud……..19

2.2. Bases de Legitimación……19

2.3. Roles y Responsabilidades……..20

2.4. Incidencias con la Historia Clínica……..21

2.5. Los menores de edad y el dato sanitario……22

2.6. El ejercicio de los derechos ARCO……...22

2.7. Decisiones basadas en un tratamiento automatizado……..24

2.8. La gobernanza de datos, gestión de riesgos y medidas de seguridad…….24

2.8.1. La privacidad como requisito primordial……...25

2.8.2. Medidas de seguridad y Evaluaciones de impacto……26

2.8.3. Conservación y custodia de los datos de salud……..27

2.8.4. Deber de secreto profesional……..28

2.8.5. El Delegado de Protección de Datos……..28

2.8.6. Productos y seguros de ciberseguridad……28

3. RÉGIMEN CONTRACTUAL

3.1. Contratación pública con el SERMAS……30

3.1.2 Delimitación contractual……30

3.1.3. Compra Pública de Innovación. ……..……30

3.1.4. Procedimiento de especiales de adjudicación……...33

3.1.4.1. Procedimientos con negociación……..33

3.1.4.2. Diálogo competitivo con publicidad……34

3.1.4.3. Asociación para la innovación……..34

3.1.5. Criterios de adjudicación……..35

3.1.6. Responsabilidad del SERMAS. ……...36

3.2. Contratación con un proveedor de atención médica……36

3.2.1. La Responsabilidad civil derivada del uso del Software *eB2MC*……..37

4. LA PROPIEDAD INTELECTUAL DEL SOFTWARE

4.1. Tratamiento jurídico del algoritmo……40

4.2. Tipos de contrato de Propiedad Intelectual……42

4.2.1. La licencia de uso o concesión de licencia de uso……42

4.2.2. La licencia de obra derivada……..42

4.2.3. Acuerdo de cesión de los derechos de propiedad intelectual……43

4.2.4. Acuerdo de Investigación y Desarrollo……43

4.2.5. Acuerdo de licencia con el SERMAS……...43

4.2.6. Acuerdo de Confidencialidad……....44

4.3. Responsabilidad civil por infracción de derechos de la propiedad intelectual…44

IV. CONCLUSIONES……..46

V. BIBLIOGRAFÍA……48

VI. ANEXOS.

Anexo A: Legislación y jurisprudencia……53

Anexo B: Modelo de Contrato de licencia de uso del software eB2MC……...55

Anexo C: Términos y condiciones de uso de la aplicación para usuarios……63

I. INTRODUCCIÓN

1.1. Hacia la modernización de la sanidad pública.

Resulta un hecho incontrovertible que el impacto producido por las nuevas tecnologías en las últimas décadas ha sido decisivo en la evolución de los modelos de negocio, pudiéndose afirmar que la aceleración exponencial del desarrollo tecnológico ha transformado el tejido empresarial de manera irreversible. El conglomerado digital enraizado en internet y constituido por un número de tecnologías disruptivas entre las cuales encontramos la robótica, el internet de las cosas, el Big Data, la tecnología 5G, las redes neuronales o la inteligencia artificial, ha modificado el nuevo paradigma digital condicionando el futuro de nuestra estructura social y productiva, al uso de este tipo de herramientas tecnológicas.

Desde esta perspectiva, existen innumerables motivos para dotar a nuestro sistema sanitario de mecanismos necesarios para situarlo en un lugar privilegiado. Durante la elaboración de este trabajo, la humanidad ha sufrido una pandemia a nivel global sin precedentes y con unas consecuencias difícilmente calculables. En este sentido, parece conveniente implementar una actualización y una modernización del sistema sanitario, adaptándolo a las nuevas necesidades y exigencias de la población.

La investigación y el desarrollo en el ámbito sanitario está enteramente ligada a la tecnología. Siempre lo ha estado. No obstante, desde la invención de Internet, la mejora ha sido muy notable, entre otras razones, por la cantidad de información y datos disponibles alrededor del mundo, pero también debido a la creación de nuevas formas de tecnología como la IA. Es en este punto de convergencia entre la inteligencia artificial y la medicina, donde se está produciendo un rotundo desarrollo en el sistema sanitario.

1.2. ¿Qué es la Inteligencia Artificial?

El término Inteligencia Artificial se adoptó por primera vez en el año 1955 por John McCarthy, quien organizó la Conferencia de Darthmouth en 1956. En esta Conferencia se plantó la semilla de lo que se ha considerado como el evento científico en el que se cimentó el origen de la Inteligencia Artificial como disciplina científica. Existen numerosas definiciones de IA, no obstante, todas incorporan conceptos relativos a la

forma de actuar y razonar como si se tratara de un ser humano, cuyo fin es buscar y resolver problemas a partir de una base de datos.[1]

En última instancia, se trata de conseguir una inteligencia artificial distributiva para que los programas software tomen decisiones autónomamente e interaccionen unos con otros.[2]

1.3. El software "e*B2MC*". Características generales.[3]

Se trata de una solución e-Health diseñada por y para los pacientes, cuidadores y profesionales de asistencia sanitaria. El Software recoge la información de la actividad del paciente de manera automática y continua, a través de teléfonos inteligentes, "wereables" y redes sociales.

El Software está caracterizado por su capacidad de aportar información objetiva del comportamiento del usuario, posibilita la decisión de intercambio de información con el médico o cuidador, recoge datos tanto pasiva como activamente, posibilita un control de la medicación y es capaz de integrarse con la historia clínica del paciente. A su vez, desarrolla indicadores de comportamiento basados en IA con módulos específicos relativos a la depresión, el bienestar emocional, la ansiedad, el trastorno bipolar, la hiperactividad, el autismo, el estrés laboral o los trastornos alimentarios.

Mediante este informe, pretendo ofrecer un planteamiento objetivo de las oportunidades reales que tiene este software de constituirse como un producto sanitario y su implantación en el SERMAS. Al margen del rendimiento económico que pueda extraerse de esta circunstancia, la implantación del software *eB2MC* en el SERMAS supondría una oportunidad única para explorar el rendimiento y la eficacia del Software.

Así pues, parece conveniente comenzar aportando una visión panorámica del espectro de posibilidades en el ámbito sanitario y las previsiones futuras en relación a la implementación de programas informáticos para el diagnóstico de enfermedades.

---

[1] De las Heras Rodríguez, T. (Julio 2019). Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact. Oxford Academic, *Uniform Law Review*, 24, pp. 302–314.

[2] Torra, V. (Diciembre 2011). La Inteligencia Artificia, *Instituto de Investigación en Inteligencia Artificial (CSIC)*. Recuperado de: www.fgcsic.es/lychnos/es_es/articulos/inteligencia_artificial

[3] Recuperado de: https://eb2.tech/es/eb2-mindcare-producto/

II. ANTECEDENTES Y EVOLUCIÓN DE LA SALUD ELECTRÓNICA.

2.1. Salud Electrónica y Estrategia Europea.

Las primeras manifestaciones de interés de las instituciones europeas por la puesta en marcha de la aplicación de las tecnologías informáticas en la salud electrónica podemos encontrarlas en los programas ESPRIT,[4] y posteriormente en la Acción Exploratoria de Informática Avanzada de Medicina.[5]

Los últimos hitos en materia de e-Salud vienen determinados por los trabajos de la red de salud electrónica, (Multiannual Work Programme (2018-2021) y el Plan Horizonte 2020.[6] A nivel nacional, cabe destacar la Estrategia Española de I+D+I en Inteligencia Artificial que analizaremos más adelante.

2.2. Plan de acción sobre la salud electrónica 2012-2020.[7]

Del Plan de acción sobre salud electrónica 2012-2020 se puede extraer que "*la salud electrónica consiste en el uso de las TIC en los productos, servicios y procesos sanitarios, combinado con cambios organizativos y nuevas capacidades en los sistemas de atención sanitaria, a fin de mejorar la salud de los ciudadanos, la eficacia y la productividad de la prestación de dicha atención, así como el valor social y económico de la salud* ".[8]

---

[4] Comunidad Europea, (1984-1988). Programa Europeo de investigación y desarrollo en el campo de las tecnologías de la información (ESPRIT). Recuperado de https://cordis.europa.eu/programme/id/FP1-ESPRIT-1/es

[5] Monteagudo Peña, J.L. (2019). La e-Salud en el marco de la Unión Europea. Aspectos organizativos, legislativos y operacionales. *Club Gurterch*, pp. 14-16. Recuperado de: https://www.clubgertech.com/ "Esta iniciativa marcó el origen de una serie de programas ininterrumpidos de investigación, desarrollo tecnológico e innovación dentro de los sucesivos programas marco hasta el Horizonte 2020 actualmente en vigor".

[6] Comisión Europea, (2014). El Programa Marco de Investigación e Innovación Dirección General de Investigación e Innovación. HORIZONTE 2020. "Con una dotación de 80.000 millones de euros, el programa Horizonte pretende ser el programa de investigación puesto en marcha por la UE. Permitirá que las ideas lleguen más rápidamente al mercado y puedan aplicarse en hospitales, fábricas, tiendas y hogares lo antes posible". Recuperado de : www.ec.europa.eu/horizon2020

[7] Comisión Europea. (2012). Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las Regiones.

[8] Ibid, p. 4.

Según las proyecciones extraídas de este Plan de acción para la salud electrónica se estima que en 2060, se alcanzará un 8,5% del PIB en gasto dirigido a la sanidad pública.[9] Parece esencial por lo tanto, poner todos los esfuerzos necesarios en reforzar el interés en la IA. Tengamos en cuenta que según datos de la OMS, entre el 30% y el 50% de los casos de cáncer pueden ser evitados si se toman medidas de prevención y de diagnóstico temprano.[10]

2.3. Multiannual Work Programme (Red de eHealth).[11]

En este documento se estableció una guía sobre la estrategia a seguir en la Unión Europea en materia de e-Health y se concluyó que existen cuatro prioridades a tener en cuenta:

a) El empoderamiento de la gente: mediante la habilitación a los ciudadanos a tomar un rol activo en el manejo de su salud;
b) Uso innovador de los datos relativos a la salud: explorando los datos relativos a la salud para desarrollar una política de atención sanitaria;
c) Potenciar la continuidad de la asistencia: mejorando la aceptación de los servicios de salud transfronterizo;
d) Superando los retos de implementación: aceptando y propiciando la transversalidad en el resto de los campos mencionados.

En lo concerniente al desarrollo de este trabajo, el punto A es en el que debemos de hacer hincapié ya que el *"empoderamiento de la gente"* es un factor esencial en el desarrollo apropiado de la salud digital y está íntimamente relacionado con la aplicación *eB2MC*.

Concretamente se establecen 4 áreas de interés prioritario en este sentido:

a) **La fiabilidad de las aplicaciones sanitarias:** será necesario desarrollar un marco común y principios que faciliten un ecosistema seguro y fiable.
b) **Acceso a la información por parte del paciente:** se pretende establecer una

[9]Renita, D. (2019). Top Predictions That will Disrupt Healthcare in 2020. *Forbes*. Recuperado de: https://www.forbes.com/sites/reenitadas/2019/12/04/top-8-predictions-that-will-disrupt-healthcare-in-2020/#5319179b7f1e
[10]OMS,. (2018). Cáncer. Recuperado de: https://www.who.int/news-room/fact-sheets/detail/cancer
[11] Comisión Europea. (2017). eHealth Network. Multiannual Work Programme 2018-2021, eHealth in support for better health.

orientación coherente en lo relativo al acceso, intercambio, y reutilización de los datos personales en la UE por parte del paciente.

c) **Alfabetización digital de los pacientes:** se espera que se implemente la alfabetización digital en el ámbito sanitario de los ciudadanos europeos.

d) **La Telemedicina:** existe el objetivo de que se tenga en consideración las evidencias y pruebas provenientes o derivadas de la salud telemática.

2.4. Integración de la e-Health en el Sistema Nacional de Salud.

Al margen de un posterior análisis normativo más exhaustivo sobre la salud digital, conviene detenerse a estudiar el despliegue digital en nuestra administración sanitaria tanto a nivel nacional como autonómico. Existen varios hitos en este sentido:

El primero fue, el **Informe de 2014 del COP** "*E-Salud: prioridad estratégica para el sistema sanitario*".[12] El segundo fue el **Plan de Telemedicina 2014-2018** en el ámbito de la Comunidad de Madrid.[13] Este Plan supuso una primera aproximación hacia el mundo de la salud digital, tenía objetivos puestos en la continuidad asistencial y en la reducción de barreras a los servicios, sin embargo, es importante destacar que no existe constancia de que se haya puesto en marcha nunca.[14]

Además, conviene destacar los efectos del Plan de Transformación digital de la Administración General del Estado[15] y el nuevo Plan de acción de transformación digital, en el que se incluyen Planes sectoriales para transformar los ministerios y un catálogo de servicios de administración electrónica para entes nacionales, regionales y locales. Su plena aplicación, "*podría preparar el camino para mejoras aún más significativas en el ámbito de la administración público- digital*."[16] Por último, es necesario hacer mención a **la Estrategia Española de I+D+I en Inteligencia Artificial,** ya que se trata de una estrategia en línea con Horizonte 2020 que incorpora

[12] Consejo Asesor de Sanidad. (2014). E-Salud: prioridad estratégica para el sistema sanitario. Recuperado de: http://www.infocop.es/view_article.asp?id=5071&cat=9

[13] Consejo Asesor de Sanidad. (2014). Es por Madrid. Plan estratégico de Telemedicina 2014-2020.. Recuperado de: https://www.espormadrid.es/2014/04/plan-estrategico-de-telemedicina-2014.html

[14] De Lima, D, (2018). Informe sobre Trasformación Digital en Salud en España Compromisos vs Realidad. *Asociación Salud Digital,* pp 135. Recuperado de: www.salud-digital.es

[15] Comisión Europea. (2018). Índice de la Economía y la Sociedad Digitales (DESI), Informe de país para España. Plan de Transformación digital de la Administración General del Estado y sus Organismos Públicos 2015-2020. Recuperado de https://ec.europa.eu/digital-single-market/en/desi. "El ahorro estimado en relación con el uso de los servicios digitales para el período de2012 a 2017 supero los 4.000 millones de EUR"

[16] Ibid, p 12.

elementos innovadores como la "*MedicinaP4"* basada en la predicción personalizada, preventiva, participativa y plenamente fundamentada en la IA.[17]

2.5. Perspectiva empresarial.

Para analizar esta perspectiva, nos hemos apoyado en una encuesta realizada a 180 directivos del sector empresarial de países de Europa y Asía, para evaluar los retos que plantea la adopción de IA en el sector sanitario, cuyos resultados se muestran en la siguiente gráfica.[18] Podemos concluir que más de un 90% de los encuestados cuentan con proyectos de IA en su agenda y solamente un 6% muestran desinterés por este tipo de soluciones, así pues, el IA parece tener el futuro asegurado en este sector.

Figura I: IA en el Sector Sanitario: encuesta a Directivos, realizada en varios países.[19]

Por otro lado, resulta necesario insistir en la importancia de la colaboración público-privada impulsada desde la Unión Europea.[20] La agenda de innovación y desarrollo fomentada desde las instituciones europeas incluye al sector privado como parte de su estrategia, siendo la estrategia de Horizonte Europa un ejemplo paradigmático de dicha agenda.[21]

---

[17] Ministerio de Ciencia, Innovación y Universidades. (2019). *Estrategia Española de I+D+I en Inteligencia Artificial*, pp 30. La dotación económica prevista por el Gobierno español para políticas de sanidad durante el año 2018 ascendió a 4.251 millones de euros, un incremento del 3,9% respecto del ejercicio anterior, lo que suponer un 6,3% del PIB nacional. Es de esperar que este incremento siga produciéndose en los próximos años, ya que, los españoles tendrán mayor esperanza de vida en 2040.

[18] Ibid, 25, página 5.

[19] Cassinello, Sánchez Pablo. (2019). Inyección de inteligencia artificial para el sector sanitario. IA en el sector sanitario: encuesta a directivos. *Accenture Consulting*, pp 6-9.

[20] Comisión Europea. (2020). Libro blanco de la Inteligencia Artificial, *Sobre la inteligencia artificial-un enfoque europeo orientado a la excelencia y la confianza*, pp 9.

[21] Horizonte Europa es el futuro Programa Marco de Investigación e Innovación de la Unión Europea para el periodo 2021-2027. Se trata de la iniciativa principal de la Unión Europea para el fomento de la investigación y la innovación desde la fase conceptual hasta la introducción en el mercado, y sirve de

Con esta vista panorámica y las implicaciones económicas derivadas de la implantación de un software de diagnóstico de IA, conviene exponer las tipologías, modalidades y algunos de los obstáculos a los que nos podemos enfrentar en la implantación del Software *eB2MC*.

2.6. La Salud Digital, Inteligencia Artificial y Big Data. Factores relevantes.

La IA aplicada a la Salud Digital abarca todo tipo de tecnologías de personalización de medicamentos, tecnologías de información y comunicación, soluciones software, herramientas de mejora de eficiencia y el desarrollo de sistemas de salud permanentemente interconectados.[22]

La criticidad actual relativa a la implementación de herramientas de IA reside en una suma de factores que han de ser tratados con un alto grado de pulcritud jurídica. Independientemente de que las cuestiones relativas a la protección intelectual, o la protección de datos personales sean tratadas posteriormente, existen una serie de recomendaciones sobre el uso del Big Data en la salud.

Tales recomendaciones pueden concretarse en cuestiones relacionadas con la legalidad, la ética y la ciencia, y que deben tenerse en cuenta a la hora de desarrollar e implementar un software de diagnóstico médico basado en inteligencia artificial.[23]

El siguiente cuadro establece un esquema de las directrices éticas y jurídicas que han de tenerse en cuenta a la hora de implementar herramientas basadas en IA, siempre teniendo como eje central, el bienestar del paciente y de los ciudadanos. A lo largo de este informe, se van a tratar el resto de cuestiones que afectan directa y transversalmente a la implementación de IA en el SERMAS, como son los aspectos legales, la gobernanza de los datos o las medidas de seguridad.

---

complemento a la financiación nacional y regional. Horizonte Europa constituye la prolongación del programa Horizonte 2020 de la UE.

[22] Malonda, V. (2020). Qué es la Salud Digital y e-Salud. *Principio Activa*, Recuperado de: https://principioactiva.com/salud-digital-e-salud/

[23] Comisión Europea. (2016). Study on Big Data in Public Health, Telemedicine and Healthcare Executive summary, p. 9.

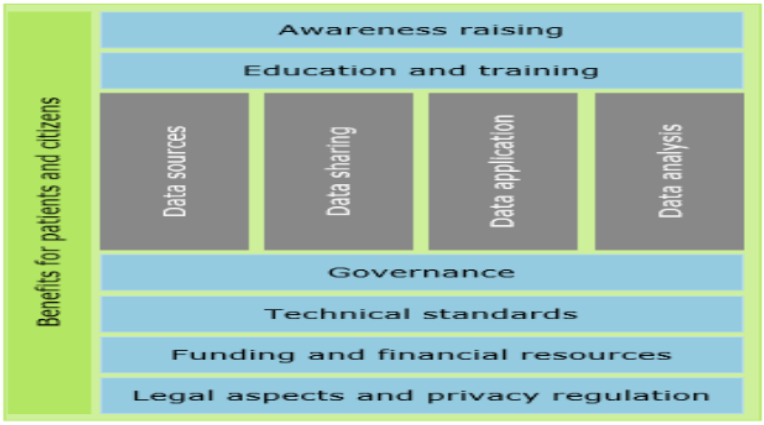

Figura 2: Overview of fields of policy recommendations[24]

[24] Ibid, p, 10.

III. ANÁLISIS JURÍDICO

Antes de abordar los principales retos a los que nos vamos a enfrentar en relación a la protección de datos, la propiedad intelectual, la vinculación contractual con la administración pública, o la responsabilidad civil derivada del uso del software, hemos de hacer mención al impacto de la IA y qué lugar ocupa dentro de la legislación nacional y europea.

A pesar de la existencia de un cuerpo normativo europeo sobre derecho informático, protección de datos, o productos sanitarios, no existe una regulación armonizada sobre la IA, y tampoco sobre la aplicación y uso de los algoritmos. Así pues, en la medida que aceptamos que el uso de algoritmos aplicados en cualquier ámbito profesional está transformando el mundo laboral de manera exponencial, debemos asumir que dicho cambio va producirse de manera global y deviene necesaria una mayor concreción regulatoria.

El fundamento de esta reflexión descansa en el efecto de las consecuencias jurídicas derivadas de la consideración del Software *eB2MC* como producto sanitario. Además, la obtención del marcado CE posibilitaría la comercialización del Software en la UE y supondría un importante impacto en el prestigio de EBB y de la UC3M.

1. El software *eB2MC* como producto sanitario.

Para determinar si *eB2MC* puede calificarse como producto sanitario, debemos analizar con detenimiento los requisitos necesarios para que un software sea calificado como tal y así poder optar con garantías suficientes a la obtención del certificado CE.[25] Esta certificación puede ser difícil de obtener pero es perfectamente factible, de hecho, existe algún precedente que puede servirnos como punto de referencia.[26]

[25] El marcado CE de un producto sanitario certifica el cumplimiento del fabricante de dicho producto de los requisitos establecidos en el Reglamento (UE) 2017/745 sobre productos sanitarios y el marco normativo que le aplica, permitiendo su comercialización en cualquier país de la UE.

[26] La solución digital para la salud mental "Monsenso", obtuvo en 2016 el Marcado CE, siendo una aplicación basada en la recogida de datos para la ayuda del diagnóstico y comportamiento del paciente, así como permitiendo consultas personales en persona o a través de videollamada. Recuperado de: https://www.monsenso.com/ .

En primer lugar, debemos identificar si el software puede definirse como un "*programa informático autónomo"* o como un "*software incorporado en un dispositivo médico".*[27]

Para incorporarlo a la categoría de "*Programa informático autónomo"*[28], el software tiene que cumplir los requisitos establecidos en la guía MDCG 2020-1.[29] Si bien este documento tan solo es una guía, debemos ser conscientes de la enorme importancia de su contenido.[30]

Así pues, debemos conocer la definición de producto sanitario que se desprende del artículo 2 del Reglamento (UE) 2017/475 UE:

> *"El* ***producto sanitario****: todo instrumento , dispositivo, equipo* ***, programa informático****, implante, reactivo, material y otro artículo destinado por el fabricante a ser utilizado en personas, por separado o en combinación , con alguno de los siguientes fines médicos específicos:*
>
> - ***Diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad.***
> - ***Diagnóstico, seguimiento, tratamiento, alivio o compensación de una lesión o de una discapacidad.***
> - ***Investigación, sustitución*** *o modificación de la anatomía o de un proceso o estado fisiológico o patológico,*
> - *Obtención de información mediante el examen in vitro de muestras procedentes del cuerpo humano, incluyendo donaciones de órganos, sangre y tejidos,*

[27] Traducción propia de "Software as a medical device".
[28] Traducción propia de "Stand Alone Software". Software como producto sanitario.
[29] Comisión Europea. (2016). Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices. (2016). Este documento sólo trata las categorías de programa informático autónomo. La Directiva 93/42/CEE del Consejo relativa a los productos sanitarios prevé lo siguiente: "*Es necesario precisar que los programas informáticos como tales, cuando están destinados específicamente por el fabricante a una o varias de las finalidades médicas establecidas en la definición de un producto sanitario, son productos sanitarios. Los programas informáticos para usos generales que son utilizados en el marco de la asistencia sanitaria no son productos sanitarios."*
[30] Grupo de coordinación de Productos Sanitarios. (2020). MDCG 2020-1 "*Guidance on Clinical Evaluation (MDR)/Performance Evaluatios (IVDR) of Medical Device Software*", (2020). Este documento está respaldado y aprobado por un grupo creado en el Reglamento 2017/475 UE en su artículo 103, (MDCG) Grupo de Coordinación de Productos Sanitarios. Esta guía trata de aportar un marco legal para la determinación de un nivel apropiado de pruebas clínicas requeridas para la consideración de un software como un producto sanitario según los criterios establecidos en el propio Reglamento.

> *Y que no ejerce su acción principal prevista en el interior o en la superficie del cuerpo humano por mecanismos farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales mecanismos".*[31]

A la luz de esta definición, considero que *eB2MC*, **puede ser categorizado como producto sanitario,** ya que encaja con la definición del Reglamento 2017/745/UE. En este sentido, es posible establecer un criterio análogo al aplicado con el programa "Monsenso", y en consecuencia, alcanzar dicha categorización.

En segundo lugar, debemos tener en cuenta la definición de "*fabricante"* establecida en el artículo 2.20 del Reglamento. A saber, *"Una persona física o jurídica que fabrica, renueva totalmente o manda diseñar, fabricar o renovar totalmente un producto, y lo comercializa con su nombre o marca comercial*." En este contexto, con carácter previo, necesitamos obtener la **licencia previa de fabricación de producto sanitario o licencia de funcionamiento de instalaciones.**

Los requisitos de fabricación de un producto sanitario están previstos en el artículo 9 de RD 1591/2009, por el que se regulan los productos sanitarios.[32] La solicitud de licencia se presentará ante la AEMPS, debiéndose aportar las instrucciones de fabricación y nombrar a un responsable técnico.[33] Conviene hacer mención a la importancia de la documentación relativa al sistema de gestión de la organización y las instrucciones de fabricación requeridas por la AEMPS, ya que son la principal causa de retraso en la solicitud de licencia, y por ello, es importante ser exhaustivos con su preparación.

Por último, una vez obtenida dicha licencia, es necesario cumplir con un último requisito para poder fabricar un producto sanitario. Se trata de la elaboración del expediente técnico para obtener el marcado CE, cuyo procedimiento explico a continuación.

---

[31] Esta definición de producto sanitario es prácticamente idéntica a la prevista en el artículo 2 del Real Decreto 1591/2009.

[32] Dicho artículo hace referencia al artículo 100 de la ley 14/1986, de 25 de abril general de sanidad, donde se establece la obligación de obtener licencia de fabricación de productos sanitarios.

[33] El responsable técnico es el responsable en verificar que el producto cumple con las exigencias del reglamento y en autorizar su comercialización. Sin embargo, el artículo 15.2 Reglamento (UE) 2017/745 prevé que en el caso de que el fabricante sea una microempresa o una empresa pequeña, basta con que puedan disponer de tal persona de forma permanente y continua.

1.1. Marcado CE. Clasificación y procedimiento de obtención.

Existen varias clases de producto sanitario en función de las características del producto, (I, IIa, IIb y III). La clasificación de eB2MC sería **clase I.**[34]

Una vez determinada la clase de producto, hay que elaborar la denominada **evaluación de conformidad**, en la que el fabricante debe acreditar que el producto sanitario satisface las exigencias del Reglamento, siguiendo el procedimiento determinado en el anexo IV correspondiente a los productos de clase I.

El marcado CE de los productos sanitarios de clase I se obtiene a través de un procedimiento **de autodeclaración,** y la posterior emisión de la **declaración UE de conformidad.**

El marcado expedido por la Comisión Europea aporta no sólo prestigio al Software y a la compañía sino que además, impide que otros estados miembros exijan controles o condiciones adicionales al producto. En este sentido, merece la pena hacer mención a la STJ C-329/16, 2017,[35] en la que se establece los siguiente:

> "*El artículo 1, apartado 1, y el artículo 1, apartado 2, letra a), de la Directiva 93/42/CEE del Consejo, de 14 de junio de 1993, relativa a los productos sanitarios, en su versión modificada por la Directiva 2007/47/CE del Parlamento Europeo y del Consejo, de 5 de septiembre de 2007, establece que el programa informático debe interpretarse en el sentido de que tenga* ***una funcionalidad que permite la explotación de datos propios de un paciente, con el fin, en particular, de detectar las contraindicaciones, las interacciones de medicamentos y las posologías excesivas constituye, por lo que respecta a esa funcionalidad, un producto sanitario en el sentido de tales disposiciones, aun cuando ese programa informático no actúe directamente en el interior o en la superficie del cuerpo humano****."*

[34] En el Anexo VIII del Reglamento 2017/745/UE se encuentran las definiciones necesarias para poder clasificar el producto en virtud de su finalidad. A su vez, el artículo 11 del RD 1591/2009 establece la misma clasificación y en su anexo IX prevé los criterios de clasificación. Al ser un producto no invasivo, hemos de clasificarlo conforme a la regla 1.1, Regla 1 de productos no invasivos: "*Todos los productos no invasivos se incluirán en la clase I.*"

[35] Tribunal de Justicia en sentencia de 7 de diciembre del 2017, en el asunto C-329/16. (2017). Syndicat National de lìndustrie des technologies m´wdecales (Sniterm, Philips France y Premier ministre, Ministre des Affaires sociales e de la Santé.

Existen por lo tanto dos requisitos acumulativos para considerar al Software como producto sanitario. Primero, que **la única finalidad sea específicamente médica**, **y segundo, que debe tener una determinada acción que condicione al usuario**.

Así mismo, cabe la posibilidad de que algún módulo concreto del software alcance la condición de producto sanitario, en cuyo caso se incorporaría el marcado CE a los módulos correspondientes. De todo ello se puede concluir que el Tribunal de Justicia ha efectuado una interpretación amplia del programa de ordenador como programa sanitario.[36]

En este sentido, existen razones para ser optimistas en la obtención del marcado CE ya que existen otros casos similares en los que se haya otorgado. Ahora bien, la mejora técnica en la toma de decisiones del Software y la incorporación de nuevas posibilidades y opciones en el programa, ayudarán a que pueda considerarse un producto sanitario. A continuación, voy a exponer las principales particularidades jurídicas de un software de estas características.

2. Protección de Datos Personales.

Con carácter previo a la exposición de todas las cuestiones relativas a la correcta utilización de los datos personales, conviene hacer mención en primer lugar, a los principios generales entorno a los cuales, han de ser tratados:

- Licitud, lealtad y trasparencia.
- Limitación de la finalidad.
- Minimización de datos.
- Exactitud.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.

En segundo lugar, debemos aportar varios conceptos para comprender el informe en su integridad. En este sentido, la definición que de los datos personales hace el RGPD es la siguiente: "*Son **datos personales** toda aquella información sobre una persona física identificada o identificable*".

[36] García Vidal, A. (2017). Los programas informáticos como productos sanitarios. Gómez-Acebedo y Pombo, *Revista CESCO*, (22) pp. 6.-8.

Del mismo modo, resulta imprescindible señalar el concepto de **tratamiento de datos personales**: "*Cualquier operación o conjunto de operaciones realizadas sobre datos personales ya sea por procedimientos automatizados o no*". Al tratarse de un software con fines sanitarios, debemos ser conscientes de que los datos que vamos a manejar son datos sensibles.

Dicha consideración implica una especial protección sobre los mismos y por lo tanto, deviene necesario un análisis pormenorizado y sistemático de todas las cuestiones y circunstancias relacionadas con el tratamiento de los datos sensibles relativos a la salud.

2.1. Datos relativos a la salud.

Como ya hemos mencionado, los datos relativos a la salud son considerados **sensibles**, el RGPD los define como: "*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 sus estado de salud***".[37] En esta misma línea, el Considerando 35 del mismo Reglamento *incluye como dato sanitario "la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria (....)* ***o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro hospital sanitario, un hospital, un dispositivo médico o una prueba diagnóstica invitro***." Por su parte, la LOPDGDD en su artículo 9, nos remite a la definición prevista en el RGPD sobre datos sensibles.

Atendiendo a lo dispuesto, debemos proceder a establecer la base de legitimación adecuada para el tratamiento de datos personales.

2.2. Bases de Legitimación.

En Europa rige el **Principio de Autodeterminación Informativa**, es decir, la potestad individual de disponer de los datos personales. En este contexto, cualquier tratamiento de un dato personal requiere una base de legitimación.[38] Las bases de legitimación más adecuadas en este tipo de aplicaciones y programas software son, la **ejecución**

[37] Artículo 4.15 del Reglamento (UE) 2016/679, (RGPD).
[38] Artículo 6 RGPD: consentimiento, interés legítimo, interés público, protección de intereses vitales, responsabilidad contractual, obligaciones legales.

contractual, el interés legítimo[39] y sobre todo el consentimiento. En particular, **consentimiento del usuario,** es la base más idónea y en muchas ocasiones, será la única base legitimadora posible. Concretamente **un consentimiento expreso**, ya que se están tratando datos de salud y por lo tanto especialmente sensibles.

2.3. Roles y Responsabilidades.

La transparencia en el tratamiento de los datos personales es capital de cara a poder demostrar un nivel de responsabilidad y buen uso de los mismos, lo que comúnmente se denomina como *"accountability o responsabilidad proactiva"*. Por lo tanto, hemos de saber distinguir **quién es el responsable del tratamiento de los datos.** Con carácter general, el Responsable del tratamiento es la persona física o jurídica que marca las pautas sobre las decisiones del tratamiento de datos, "*quien determina los fines y los medios."* Sin embargo, el RGPD en su artículo 26 introduce la figura de la *corresponsabilidad*. Para poder determinar esta responsabilidad compartida, debemos tener en cuenta la etapa o el ciclo de vida del dato.

Por otro lado, el **Encargado de tratamiento** será aquella persona física o jurídica que realice las tareas encargadas según las instrucciones del responsable. Si establecemos una relación contractual con el SERMAS y la utilización del software se limita a las condiciones y finalidades establecidas por la administración, EBB será el encargado de tratamiento.

Los datos que obtenga EBB para prestar el servicio de *eB2MC* pueden provenir de **una cesión de datos personales o del acceso a los datos personales de una base de datos.** Esta diferenciación es importante ya que si EBB tiene acceso a los datos, no será necesario el consentimiento expreso del afectado, mientras que si se acuerda la cesión de datos, EBB será responsable de los datos y necesitará el consentimiento del usuario. Si un hospital contrata los servicios de EBB para la finalidad que el hospital determine,

[39] Grupo de Trabajo del artículo 29. (2014). Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud el artículo 7 de la Directiva 95/46/CE. El interés legítimo como base de legitimación tiene ciertas particularidades y exige un alto grado de responsabilidad por parte del responsable. Pp. 30-33. "*El interés legítimo debe ser lícito, estar articulado con claridad suficiente para permitir que la prueba de sopesamiento se lleva a cabo en contraposición a los interés y los derechos fundamentes del interesado, es decir, suficientemente específico y representar un interés real y actual, no especulativo.*

en el contrato de servicios debe especificarse el objeto de la prestación, así como la necesidad del acceso a los datos por parte de EBB para el cumplimiento de dichos fines.

Lo mismo ocurrirá si se toman decisiones automatizadas o cuando se elaboren perfilados con fines propios, en cuyo caso, ambas entidades serán corresponsables del tratamiento. En este sentido es importante destacar que, "*Si el usuario realiza un perfilado sobre sus propios datos en su entorno para una actividad exclusivamente personal, se aplicará la* ***excepción doméstica***".[40] En este caso, EBB no tendrá la condición de responsable de tratamiento.

El responsable del tratamiento siempre debe comprobar la legitimidad de la fuente de los datos, ya sea por parte del SERMAS, o de un proveedor de sanidad privado. Por lo tanto, con carácter general, en la medida que un hospital **no ceda los datos sino que otorgue el acceso a los datos** con las finalidades exigidas, EBB será el Encargado de tratamiento.

2.4. Incidencias con la Historia Clínica.

Una vez analizada la legitimación del tratamiento de datos personales, debemos abordar los problemas relacionados con la "historia clínica". La denominada *historia clínica,* constituye toda la información y documentación relativa a la evolución clínica del paciente, incluyendo valoraciones e informaciones a lo largo del proceso asistencial. En este sentido, toda información tratada sobre el diagnóstico médico psiquiátrico acumulada en el programa informático formará parte de la historia clínica del paciente.

En cualquier caso, es importante haber fijado las condiciones y los fines conforme a los cuales se va a tener acceso a los datos del usuario, ya que en el ámbito de la asistencia sanitaria, los facultativos y el personal cualificado, son los únicos que deben tener acceso a dichos datos y siempre respetando el principio de proporcionalidad. Por lo tanto, será necesario para el tratamiento de cualquier dato del paciente, su consentimiento.[41] Los responsables del tratamiento de datos deben, una vez más,

[40] AEPD. (2020). Adecuación al RGPD de tratamientos que incorporan IA, pp18. Excepción doméstica: Considerando 18 del RGPD. "*El Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y por tanto, sin conexión alguna con una actividad profesional o comercial."*

[41] *Aguirre Beltrán, J.L.* (2017). Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD." *SESPAS,* Página, 53-55. Por ejemplo, "*no está permitido modificar los datos de una prescripción médica de manera automática por medio del software*

establecer las medidas de seguridad correspondientes, siendo estos, los que deben acreditar que cuentan con el consentimiento del paciente.[42]

2.5. Los menores de edad y el dato sanitario.

Al margen de las numerosas medidas de seguridad disponibles para tutores y padres en el uso de las aplicaciones de internet y el control que estos pueden ejercer sobre sus hijos, conviene centrar la atención en la relación entre datos de salud y los menores. El artículo 8 RGPD establece la edad a partir de la cual estos pueden prestar su consentimiento en relación con los servicios de la sociedad de la información. En concreto, la legislación española establece la edad de 14 años de edad, sin embargo, existen excepciones en la legislación española. En este sentido, la legislación española prevé situaciones en las que los padres pueden acceder a la documentación clínica de sus hijos.[43]

2.6. El ejercicio de los derechos ARCO.

Los derechos ARCO hacen referencia a los derechos que tiene el titular sobre sus datos personales. A saber:

El derecho de acceso garantiza el acceso a toda la documentación que constituye su historia clínica por parte de sus usuarios ante el responsable del tratamiento, ya sea un hospital privado o público.[44] Este derecho no solo está contemplado en los artículos 12 y 15 del RGPD y en el 13 LOPDGDD, sino que también en el artículo 18 de la ley 41/2002 de la Autonomía del Paciente.

Las solicitudes de acceso obligan al responsable *a "dar respuesta expresa, siempre y en todo caso, empleando para ello cualquier medio que acredite dicho deber, incluso en*

---

sin el consentimiento del paciente y sin la intervención del médico competente. Así está previsto en la Sentencia del Tribunal Superior del País Vasco de febrero de 2017, de 21 de febrero de 2017, JUR/2017/116575.".

[42] AEPD. (2019). Guía para pacientes y usuarios de la sanidad, pp. 10. Recuperado de: www.AEPD.es La guía de la AEPD para pacientes y usuarios de la sanidad especifica que con carácter general, no se sanciona al profesional ya que se considera un usuario del sistema. Se sanciona al empleador del médico.

[43] Artículo 7.2d, Ley 21/2000, de 29 de diciembre, sobre los derechos de información concernientes a la salud y al autonomía del paciente, y la documentación clínica.

[44] Ibid, 42, p. 13.

aquellos supuestos en los que tales solicitudes no reúnan los requisitos previstos."[45] El tiempo establecido por el RGPD para dar respuesta a la solicitud de acceso es de 1 mes desde la recepción aunque es prorrogable por 2 meses más, dependiendo de la complejidad y el número de solicitudes.

Por último, debemos tener en cuenta que el derecho de acceso no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos, ni en perjuicio de facultativos o profesionales que participen en su elaboración.

Derecho de rectificación está previsto en el artículo 16 RGPD y supone la inmediata rectificación de los datos personales inexactos que conciernan al usuario y a que se completen los que sean incompletos, además, la rectificación del responsable del fichero, debe incluir la documentación acreditativa del error.

No obstante, en el caso de que se trate de un dato de salud, es el profesional sanitario el que tiene que determinar si debe rectificarse el dato o no, siempre basándose en un criterio médico de acuerdo con su código deontológico y sin poner en peligro la salud del paciente, en cuyo caso, no procederá la rectificación de dichos datos.[46]

El derecho de supresión supone la supresión de los datos personales de su titular sin dilación indebida. Este derecho tiene ciertas particularidades, especialmente en el ámbito sanitario. En este sentido, la AEPD determina que los datos correspondientes a la historia clínica debe ser limitado, sobre todo si se tratan datos "*para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador,* ***diagnóstico médico****, prestación de asistencia o tratamiento de tipo sanitario o social, o* ***gestión de los sistemas y servicios de la asistencia sanitaria y social."***[47]

Por último, hay que destacar la obligación del responsable de tratamiento del **bloqueo de datos personales** con el propósito de dar respuesta a una posible reclamación judicial. Así pues, se deberán tomar las medidas de seguridad necesarias para garantizar que dicha información pueda estar disponible para la autoridad competente, ya sea judicial o administrativa.

[45] AEPD. Expediente TD/00194/2019. Resolución R/00492/2019.
[46] AEPD. Expediente TD/0091/2018. Resolución N: R7001455/2018.
[47] Ibid, p. 34.

El derecho de oposición permite al interesado oponerse a que se produzca un tratamiento determinado de sus datos personales, funciona de manera similar al resto de derechos mencionados.

Por último, cabe destacar el **derecho a la portabilidad**, mediante el cual, el usuario del a tendrá derecho a recibir los datos que le hubiera facilitado a EBB de forma estructurada, con el fin de transmitírselos a otra empresa o a otro responsable o de tratamiento.[48]

2.7. Decisiones basadas en un tratamiento automatizado.

El RGPD protege a los interesados a no ser objeto de decisiones automatizadas, incluyendo la elaboración de perfiles, no obstante, si el usuario presta su consentimiento explícito, será perfectamente legal. Ahora bien, deben tomarse estrictas medidas desde el diseño de tal manera que se pueda proteger la libertad de elección del usuario. En este sentido, es muy importante ofrecer al usuario otras alternativas viables o equivalente a la decisión automatizada.[49]

2.8. La gobernanza de datos, gestión de riesgos y medidas de seguridad.

Los principales problemas relativos a la protección de datos y al uso del software *eB2MC* vienen determinados por el grado de injerencia del algoritmo en los datos personales de los usuarios. Por lo tanto, será necesario implementar medidas adecuadas de seguridad en aras de garantizar la transparencia y la responsabilidad proactiva. En definitiva, es altamente recomendable implementar una estrategia de gobernanza de datos en la que se establezcan guías y normas según las cuales se gestione la calidad, arquitectura, trazabilidad e integración de datos.[50]

---

[48] Conviene destacar que el RGPD en su artículo 20.2, contempla la posibilidad de que se transmitan los datos de responsable a responsable, como si de una compañía de telecomunicaciones se tratara.
[49] AEPD. (2020). Adecuación al RGPD de tratamientos que incorporan IA, pp18.
[50] Barrios, J, (2019). Gobernanza de datos en el sector salud. *Health and Big Data*. Disponible en https://www.juanbarrios.com/el-gobierno-del-dato-data-governance/ En un modelo de gobernanza de dato, los usuarios tienen un rol activo en la estrategia del dato. En este modelo se estandarizan herramientas de calidad e integración del dato y el monitoreo y corrección de desviaciones del mismo. Todo ello ayuda a reducir los riesgos.

2.8.1. La privacidad como requisito primordial.

La privacidad es el factor entorno al cual gravitan todos los peligros potenciales, ya que todas las acciones preventivas y reactivas deben tener como objetivo preservarla en todas sus dimensiones y por lo tanto ha de tenerse en cuenta durante todo el **ciclo de vida** de los mismos.

Figura 3: Representa la metodología para mantener el dato seguro.

Desde esta perspectiva, es fundamental ocuparse de la calidad y la seguridad de los datos en todas las etapas de creación y desarrollo del Software, ya sea en la concepción, en el desarrollo, explotación y retirada.

La implementación de medidas desde el diseño para una aplicación de este tipo es parte de la responsabilidad proactiva esperada de un Responsable de tratamiento, sobre todo teniendo en cuenta el alto grado de confidencialidad que exige el dato sanitario. Pero esta responsabilidad no acaba aquí, el Responsable tiene el deber de contar con Encargados de tratamiento con un alto grado de diligencia, por lo tanto, la implementación de una estrategia específica desde el comienzo y a lo largo del ciclo de vida de los datos, es primordial.

La administración del estado aplica a toda su organización administrativa digital, el ENS previsto en el RD 3/2010, de 8 de enero. Su contenido, estructura y desarrollo puede servir de referente para implementar todo tipo de medidas de seguridad y políticas de privacidad, siempre con el riesgo en el punto de mira.[51]

Armados con estos criterios podemos establecer un sistema de información adecuado que goce de una robustez suficiente que permita un flujo de información con el nivel alto de seguridad necesario para el tratamiento de este tipo de datos. Desde la óptica del cumplimiento normativo, no debemos obviar el respeto por la transparencia, ni a la hora de la recogida de datos e introducida en el sistema del software y ni una vez se haya puesto en funcionamiento. Esta garantía es especialmente relevante cuando obtenemos los datos directamente del usuario, no obstante, en el caso de que no se pueda garantizar

[51] Comisión Europea. (2020). The impact of GDPR on IA. Pp. 80-82.

la transparencia porque suponga un esfuerzo desproporcionado, este principio no será de aplicación.[52]

2.8.2. Medidas de seguridad y Evaluaciones de impacto.

La constante adaptación a las nuevas amenazas obliga a las instituciones investigadoras y sanitarias a imponer medidas de seguridad más estrictas en los sistemas de información. Atendiendo a lo dispuesto, es importante hacer hincapié en la incorporación de medidas de ciberseguridad actualizadas, así como en la concienciación del personal al servicio de la plataforma, la definición y racionalización del liderazgo, el desarrollo de estrategia desde la dirección y la implementación de mecanismos que protejan los esfuerzos de investigación y la propiedad intelectual, ante los ataques o la difusión indebida.[53] Todas estas medidas deben de incorporarse con la vista puesta en la calidad, confidencialidad y legitimación de los datos tratados.

En este sentido, la EIPD es una herramienta que tiene por objetivo prever o visualizar los riesgos potenciales a los que estamos expuestos en función del tipo de tratamiento de datos que se estén produciendo. Así pues, y teniendo en cuenta que los datos personales tratados son de categoría sensible, los análisis de riesgos, las EIPD y las auditorías internas cobran un protagonismo esencial y obligatorio.

En relación con las EIPD en el tratamiento de datos con fines de investigación, la LOPDGDD en su disposición final novena obliga a que se adopten este tipo de medidas con el fin de garantizar que no se pueda acceder a los datos identificativos por parte de los investigadores. En dicha disposición se distingue entre el tratamiento de datos por autoridades sanitarias, la reutilización de datos con fines de investigación y la seudonimización de datos con fines de investigación.

Para garantizar que la gestión se esté produciendo conforme a derecho, los usuarios deben tener control sobre sus datos, y además estar plenamente convencidos de que sus datos no van a perjudicarles, ni van a sufrir ningún tipo de discriminación.

Por su parte, el artículo 16.3 de La ley 41/2002, de 14 de noviembre establece que …"*el acceso a la historia clínica con fines de investigación personal del paciente, separados*

[52] Artículo 14.5 b RGPD.
[53] García Díaz, J. (2019). Un Nuevo Marco en la Ciberseguridad y la Protección de Datos. *Revista de la Sociedad Española de la Informática y Salud*, (134), pp 19-20.

de los de carácter clínicoasistencial, de manera que, como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos".

Esto significa que si los datos de los pacientes se obtienen voluntariamente desde la aplicación móvil, EBB será el Responsable de los datos, mientras que si los obtiene por parte del hospital, los datos han de ser previamente anonimizados. De hecho, resultará de aplicación obligatoria cualquier mecanismo técnico como registros secretos o los códigos de acceso, que impidan el acceso a dicho historial por personal no autorizado.

En segundo lugar, debemos hacer hincapié en la manera en la que se recogerán los datos, si los datos son proporcionados por los proveedores sanitarios o si son recopilados de modo individual por cualquier usuario. En este contexto, la Comisión Europea ha determinado que la privacidad y gestión de datos son requisitos esenciales.[54] En cualquier caso, el Responsable debe mantener un Registro de actividad de tratamiento, en el que se pueda apreciar el ciclo de vida del dato desde el origen y permita tener un control sobre los mismos.

Para mayor abundamiento, es altamente recomendable acudir a documentación especializada en la materia como por ejemplo, la guía sobre copias de seguridad de INCIBE, en la que se ofrecen soluciones como la estrategia 3-2-1 de copias de seguridad o soluciones mixtas como Disk 2 Disk 2 o Disk 2 Cloud.[55]

2.8.3. Conservación y custodia de los datos de salud.

La LAP fija un plazo de 5 años desde el alta del paciente de conservación de los datos, sin embargo, con fines de investigación, el plazo puede incrementarse de manera ilimitada siempre y cuando los datos sean debidamente seudonimizados.

Debido al enorme riesgo al que están expuestos los datos, es necesario tomar medidas enfocadas a velar por la seguridad y protección de los mismos. La interconexión digital expone los datos a la interrupción en la cadena de suministros o el robo de la

[54] Comisión Europea. (2019). Comunicación de la Comisión al Parlamento Europea y al Consejo y al Comité económico y social Europea y al comité de las Regiones. Pp 168. "Los otros 6 requisitos son: la Intervención y supervisión humanas, la solidez y seguridad técnicas, la transparencia, la Diversidad, no discriminación y equidad, el bienestar social y medioambiental y la rendición de cuentas".
[55] INCIBE. (2018). Copias de seguridad: Una guía de aproximación para el empresario. Páginas 14-16.

investigación por lo que estaremos a lo expuesto en el epígrafe anterior sobre medida de seguridad.

2.8.4. Deber de secreto profesional.

En la LAP[56] está previsto "el deber de secreto" en relación con los datos en la historia clínica en el ejercicio profesión. Por su parte, el Código Penal también establece multas y sanciones en relación a la revelación de secretos. En este sentido, el personal de EBB deben cumplir con un código deontológico y conocer la Política de Privacidad y de Protección de datos que se imponga como parte de la garantía de responsabilidad proactiva por parte dela dirección de EBB.

Por su parte, el RGPD establece como una excepción a esta regla, que es el denominado, **secreto compartido.**[57] Esta particularidad está sujeta a la investigación médica para fines de medicina preventiva o para evaluar a un trabajador, pero ha de estar justificada en un contrato o sobre el Derecho de la Unión o de los Estados miembros.

2.8.5. El Delegado de Protección de Datos.

Esta figura incorporada por el RGPD es obligatoria en los supuestos designados en el artículo 37.1 de la LOPDGDD. Esta figura será obligatoria tanto en el hospital, ya sea público o privado como para EBB. Dicha obligación responde a la gran cantidad de datos que se manejan y a la complejidad de la estructura sanitaria en todas sus capas, pero más específicamente debido a la categoría de datos que se tratan.

2.8.6. Productos y seguros de ciberseguridad.

La ciberseguridad ha de plantearse como un desafío cuya implementación ha de ser abordada desde una perspectiva garantista que reduzca el riesgo al mínimo posible y siempre como un proceso continuo y continuado en el tiempo. El análisis de riesgos, la identificación de las amenazas contra la información y contra las infraestructuras son

[56] Artículo 16.6 de la LAP.
[57] Artículo 9.2h del RGPD

algunas de las actividades fundamentales para garantizar la seguridad del sistema y de la organización.

De las numerosas herramientas y soluciones en el mercado me parece esencial hacer mención a las **Certificaciones normativas.** Se trata de herramientas que facilitan el cumplimiento normativo y posibilitan la implementación de políticas de seguridad, la realización de análisis de riesgos y la valoración de activos. Por otro lado, su implementación afecta de manera positiva a la organización en todos sus ámbitos, ya sea al personal, a las infraestructuras, a la información o al negocio.

En esta misma línea, la implantación de un Sistema de Gestión de Seguridad bajo la norma ISO/IEC 27001 en combinación con la ISO/IEC 27018 generará confianza para usuarios y proveedores del Software y protegerá la reputación de EBB. Con carácter adicional, la certificación de EBB de la norma ISO 13485, asegurará que el Software cumpla con los requisitos regulatorios aplicados a los productos sanitarios.

Por su parte, tanto el RGPD como la LOPDPGDD también recomiendan e incluyen los **Códigos de Conducta** como herramientas que sirven para adecuar y facilitar la legislación relativa a la protección de datos. La adhesión a un código de conducta puede servir para demostrar el cumplimiento normativo sobre las medidas de seguridad de los responsables y encargados y se tendrán en cuenta para evaluar el impacto del tratamiento de datos que se lleve a cabo por EBB. En definitiva, son herramientas destinadas a probar la proactividad empresarial y el procedimiento transparente en el tratamiento de datos.[58]

Por último, conviene plantearse la contratación de **un seguro de ciberseguridad.** Toda organización debe estar preparada para detectar y poder recuperarse ante una amenaza o un ciberataque, lo que hoy se denomina como *ciberesiliencia.* A la hora de hacer un análisis de riesgo debemos tener en cuenta la importancias de adquirir este tipo de productos nuevos en el mercado que entre otras circunstancias, cubren los riesgos ocasionados por la privacidad, la pérdida de beneficios, los datos alojados en nube o la violación de derechos de propiedad intelectual.

[58] Comité Europeo de Protección de Datos. (2019). Directrices 1/2019. Pp. 3-5. Recuperado de: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_es

3. Régimen contractual.

3.1. Contratación pública con el SERMAS.

A continuación, vamos a analizar la delimitación contractual correspondiente a un software como *eB2MC*, las diferentes opciones de contratación pública, los criterios de adjudicación y la responsabilidad civil derivada de dicha contratación.

3.1.2 Delimitación contractual.

Para saber qué tipo de contrato corresponde al Software *eB2MC,* debemos acudir al criterio establecido en artículo 16.3b) de la LCSP. En este precepto legal se establece la definición de contrato de suministros, con una matización sobre dicha tipología referida a la "*adquisición de programas de ordenador desarrollados a medida".* En este caso, se tratará de un contrato de servicios . Es decir, si nos encontramos ante un software diseñado y desarrollado a medida de las especificaciones establecidas por el SERMAS, estaríamos ante un **contrato de servicio**. De lo contrario, si se trata de una adquisición y una cesión de derechos de uso sobre el programa informático, será un **contrato de suministro**.

Por lo tanto, en principio estaríamos ante un **contrato de suministro**, a no ser que EBB desarrolle la estructura, funciones y arquitectura del Software conforme a unas exigencias previas determinadas por el SERMAS.

Por otro lado, es conveniente señalar, que en los contratos de servicio, existen subtipos de contrato: de informática, telecomunicaciones, investigación y desarrollo, e.t.c… En este sentido, considero que el tipo de contratos correspondiente a un software de estas características puede considerarse como un **contrato de servicios.**

Una vez delimitado el tipo contractual, vamos a tratar de ofrecer una visión panorámica del espectro de posibilidades de la contratación pública de tecnologías.

3.1.3. La Compra Pública de Innovación.

La Compra Pública de Innovación, (CPI), es un instrumento implementado a nivel europeo que fomenta la innovación, con objeto de satisfacer una necesidad tecnológica

de las administraciones públicas y potenciar el desarrollo de nuevos mercados a través de la contratación pública.

Existen varios tipos de procedimientos de compra pública en materia de nuevas tecnologías. Dependiendo de las necesidades de la administración, el SERMAS podrá optar por un procedimiento ordinario, (abierto o restringido) o uno especial, en el que los operadores tengan un mayor protagonismo a la hora de negociar las condiciones.

El factor que va a determinar una u otra opción, tendrá causa en el hecho de que el programa informático que demande la administración no esté disponible en el mercado, o no se tenga constancia de que exista un programa informático que se adapte adecuadamente a las exigencias de la administración correspondiente.

Teniendo en cuenta la solución novedosa que ofrece el programa informático en cuestión, el complejo desarrollo de su arquitectura y el carácter evolutivo de las tecnología de IA aplicable en el mismo, podemos concluir, que el SERMAS debería acudir a un procedimiento de **Compra por Innovación.**

En definitiva, la CPI sirve de apoyo a la actividad innovadora del sector privado para colmar necesidades de una administración pública necesitada de productos tecnológicos innovadores, además de fomentar la dinamización del sector empresarial y la inversión pública en I + D.

Existen tres tipos de Compra pública de Innovación:

- La Compra Pública Pre-comercial, (CPP): se constituye como un procedimiento de contratación de servicios de Investigación y Desarrollo, que adopta la forma de contrato privado.[59] Esta modalidad pretende abarcar las necesidades y el diseño de soluciones originales para probarlo en sus instalaciones antes de que se haya puesto el producto en el mercado. De esta manera, la administración se adelanta competitivamente a otros operadores y ayuda al desarrollo del producto. Lo relevante en esta modalidad es establecer en el contrato, las cláusulas de gestión de la propiedad intelectual que garanticen al comprador la plena utilización del software y la realización de modificaciones por sí mismos o

[59] Agencia Valenciana de la Innovación. (2019). Guía Práctica del Proceso de Compra Pública de Innovación para Organismos Públicos de la Comunidad Valenciana. Pp, 33-35.

por terceros.[60]. En cualquier caso, este tipo de contrato no está incluido en la LCSP y por tanto, el poder adjudicador del órgano contratante puede configurar libremente el procedimiento de adjudicación.

- La Compra Pública de Tecnología Innovadora. (CPTI): este procedimiento se pone en marcha para soluciones que ya están desarrolladas a un nivel de mercado moderado pero que ya se han probado moderadamente en un entorno real. Esta modalidad, aporta aspectos innovadores a los servicios públicos. En mi opinión se ajusta con bastante precisión a las características de *eB2MC*.
- La Compra Pública Regular de Innovación. (CPRi): Se trata de un contrato a que busca soluciones existentes en el mercado pero con un grado de innovación superior a las ya implantadas.

Una parte del proceso de CPI implica la consulta previa del mercado y del estado del arte por parte del SERMAS y por lo tanto, es necesario mantener un nivel de comunicación fluida y generar un nivel de confianza propicio para asegurar la opción de compra o contratación. Tras un diálogo técnico sobre las exigencias propuestas por el SERMAS, se cerrará el plazo de recepción de propuestas y posteriormente, se procederá por parte de la administración a seleccionar la que mejor se ajuste a sus necesidades.

Téngase en cuenta, que la Directiva 2014/24/UE establece que "*los poderes públicos deben hacer la mejor utilización estratégica posible para la contratación pública para fomentar la innovación…*"[61]. En este sentido, resulta imprescindible prestar atención a todas las actualizaciones tecnológicas y publicaciones sobre los procesos de contratación.

En cuanto a la metodología para determinar qué tipo de CPI se adecúa a cada situación, se acudirá al grado de madurez tecnológica existente (TRL).[62] En tanto en cuanto se trata de contratos desarrolladas en varias fases, los TRL se medirán en función del momento en el que se inicia la contratación y en la finalización de la ejecución del contrato. Estas tablas ilustran la metodología de manera más esquemática.

---

[60] Vázquez Matilla, F.J. (2019). Desde España: La Compra Pública por Innovación. *IDOM Consulting*. Recuperado de: https://idomcpi.com/desde-espana-la-compra-publica-de-innovacion/

[61] Directiva 2014/24/UE, sobre contratación pública. Considerando 47.

Este concepto surge de la NASA y tiene su origen en proyectos aeroespaciales. Se trata de una escala de 9 niveles. Del 1-4 investigación, del 5-6, desarrollo (nivel deseable para los CPP), del 7-9, innovación (nivel deseable para los CPTI).

<table>
<tr><th>NIVEL</th><th colspan="2">CATALOGACIÓN</th></tr>
<tr><td>TRL 1</td><td colspan="2" rowspan="3">Investigación fundamental</td></tr>
<tr><td>TRL 2</td></tr>
<tr><td>TRL 3</td></tr>
<tr><td>TRL 4</td><td rowspan="2">Investigación Industrial</td><td rowspan="4">Investigación aplicada</td></tr>
<tr><td>TRL 5</td></tr>
<tr><td>TRL 6</td><td rowspan="2">Desarrollo experimental</td></tr>
<tr><td>TRL 7</td></tr>
<tr><td>TRL 8</td><td colspan="2">Producto preparado para fabricación</td></tr>
<tr><td>TRL 9</td><td colspan="2">Producto preparado para su comercialización</td></tr>
</table>

Figura 4: Niveles de madurez de la Tecnología.[63]

	TRL Al inicio de la Contratación	TFL A la finalización de la ejecución
CPP	5-6	7-8
CPTi	7-8	9
CPRi	9	9

Figura 5: TRL deseable.

Existen casos paradigmáticos de éxito en CPI en el ámbito sanitario a nivel europeo. Entre ellos, podemos mencionar el Proyecto THALEA, en el que varias entidades españolas han estado involucradas, y el proyecto HAPPI.[64]

Una vez definidas las modalidades y la metodología para elegir una opción de compra u otra, vamos a detallar los diferentes procedimientos de adjudicación para la CPI.

3.1.4. Procedimientos especiales de adjudicación.

3.1.4.1. Procedimientos con negociación.

Se trata del procedimiento típico de adjudicación para el caso que la administración requiera el desarrollo de un software con el fin de adaptarlo a sus necesidades. Consta de 3 fases, (selección, negociación y adjudicación). El proceso de negociación tendrá el foco puesto en las especificaciones técnicas y económicas establecidas en los pliegos correspondientes. En este procedimiento, la administración tendrá que especificar las características del servicio desde el principio del proceso, para posteriormente negociar

[63] Guía de contratación pública de innovación. (2019). Ayuntamiento de Madrid. Pp, 29-32.
[64] Comisión Europea. (2016). Casos de éxito CPI en Europa-Eafip.. Recuperado de: https://www.youtube.com/watch?v=Ni6w9raLwYU https://www.youtube.com/watch?v=U5vAcFt3K_s

las particularidades del mismo y por último, adjudicar el contrato de acuerdo con las condiciones negociadas. Existen dos modalidades:

- Procedimiento negociado con publicidad: se trata de los contratos en los que el órgano de contratación exija un trabajo previo de diseño o adaptación de los licitadores, o cuando el órgano no pueda especificar las prestaciones necesarias del software o cuando se hubiera producido un procedimiento abierto o restringido previo, cuyas propuestas de oferta fueran irregulares o inaceptables.
- Procedimiento negociado sin publicidad: este procedimiento permite la negociación de las condiciones técnicas del Software con el SERMAS pero respetando las características exclusivas del programa. A pesar de ser eB2MC un software único en el mercado, el órgano de contratación establecerá unos criterios de evaluación de la oferta, generalmente basándose en el precio propuesto. Por ello, es necesario justificar con enorme rigurosidad en el expediente de contratación, el carácter único del Software.[65] La solución eB2MC tiene un encaje idóneo en este procedimiento ya que se trata de un programa previamente desarrollado para un problema concreto.

3.1.4.2. Diálogo competitivo con publicidad:

Este procedimiento se pondrá en marcha cuando el SERMAS necesite desarrollar alguna aplicación software, o cuando por la naturaleza o la complejidad del programa así lo exija, o cuando no está del todo definido el objeto del contrato.[66] El procedimiento tiene una fase de selección, otra de diálogo y la fase final de adjudicación. En esta última fase se pueden negociar aspectos adicionales.

También está previsto en los casos en los que la autoridad contratante no puede establecer las prescripciones técnicas conforme a un estándar. La principal diferencia entre estos dos primeros procedimientos radica en el grado de convencimiento y confianza del comprador público con respecto al proyecto.

3.1.4.3. Asociación para la innovación.

[65] Collado Gallego, J. (2019). Contratación de Software y de bases de datos en el sector público. Pp. 32. La Junta Consultiva de Contratación Administrativa de la Generalidad de Cataluña establece que el procedimiento negociado debe estar sujeta a dos requisitos acumulativos, razones técnicas y derechos de exclusividad y que dichas razones hagan absolutamente necesaria la adjudicación del contrato a una empresa determinada.

[66] Guía para autoridades Europea de Compra Pública en Innovación. (2016), pp 44. Recuperado de: www.innovation-procuremente.org

Este proceso se introdujo en la LCSP a raíz del Programa Horizonte Europa 2020. Se configura como un procedimiento de adjudicación derivado de la transposición de la Directiva 2014/24/UE pero puede considerarse como un procedimiento de contratación paralelo al CPP y CPTI ya que está previsto para soluciones que no se encuentran en el mercado. Se trata de un proceso constitutivo de 2 fases, una de innovación tecnológica y otra de compra. En esta segunda fase solamente continuarán los licitadores que sean exitosos al finalizar la primera fase. Este proceso se llevará a cabo en casos en los que exista una necesidad de un producto o servicio que no se pueda conseguir con otras soluciones o programas.

Este procedimiento obedece a la necesidad de proporcionar un servicio inexistente en el mercado, con la característica fundamental de que la innovación tiene que tener lugar durante la ejecución del contrato. El contratista tendrá que aportar una solución a los objetivos planteados desde el punto de vista tecnológico. Es un procedimiento en el que la negociación juega un papel importante y pueden estar involucrados uno o varios operadores.

Este procedimiento guarda evidentes semejanzas con los otros procedimientos mencionados en lo referente a las fases, sin embargo este procedimiento es más complejo ya que en la fase de desarrollo del producto se fijan objetivos intermedios y al final de cada fase, la autoridad contratante puede decidir no contar con alguno de los operadores.[67] A pesar de que este procedimiento puede ajustarse a las características de *eB2MC*, se dilata bastante en el tiempo y su ejecución acaba siendo compleja y costosa.

3.1.5. Criterios de adjudicación.

La última fase de todos los procedimientos viene determinada por el criterio según el cual, el órgano contratante conceda la adjudicación del contrato. Son los criterios objetivos a los que se atiende para valorar las ofertas. Deben establecerse en el pliego de cláusulas administrativas particulares y figurar en el anuncio de licitación. Existen tres criterios comunes a todos los estados de la Unión que son:

[67] Guía para autoridades Europea de Compra Pública en Innovación. Pp 27. Recuperado de: www.innovation-procuremente.org

- *El precio:* se refiere al valor de compra. Es un criterio que no ofrece muchas posibilidades para la innovación salvo que esté en combinación con otras exigencias funcionales o variantes.
- *Coste:* el coste por lo general se refiere al valor monetario, la combinación de ambos criterios fomenta la innovación ya que estimularía la venta del software a posteriori.
- *Calidad:* El criterio de la calidad puede consistir en aspectos relacionados con el carácter evolutivo del servicio, (inteligencia artificial) y también su utilidad y eficacia.

3.1.6. Responsabilidad del SERMAS.

Una vez adjudicado el contrato, la ejecución del mismo genera una responsabilidad a la que EBB debe hacer frente. En principio, salvo que el SERMAS haya impuesto alguna cláusula al licitador cuyo contenido produzca un daño a un tercero, la empresa adjudicataria responderá de los daños producidos en su actividad. En este sentido, el artículo 312 b) de la LCSP prevé que con carácter general, el contratista es el responsable por los daños y perjuicio causados a terceros.

Por otro lado, parece conveniente incluir cláusulas contractuales en las que se establezca **el flujo de información directo** con EBB relativo a los usuarios, más allá de una clausula estandarizada que obliga al proveedor a solucionar los defectos del sistema. Todo ello sin dejar de lado lo relativo a los incentivos, la propiedad intelectual, las prórrogas o las cláusulas de resolución.

3.2. Contratación con un proveedor de atención médica.

La implantación del software *eB2MC* es un proceso de diversa complejidad que requiere una planificación determinada. Como en el caso del SERMAS, la implementación del software va llevar consigo riesgos desde el punto de vista del protección de datos y del complimiento normativo en general.

Las primeras consideraciones a tener en cuenta sobre la posible contratación relativa a la protección de datos, es que EBB será el **Encargado de tratamiento.**

No obstante, por lo que a EBB afecta, tendrá que acreditar su responsabilidad proactiva de la misma manera que si se tratara con un hospital público. En este sentido, debe ofrecer las garantías necesarias antes mencionadas con el objetivo de poder demostrar garantías de seguridad en caso de algún incidente.

Por otro lado, en la medida que se hagan tratamientos de datos relativos a la salud mental del paciente, se ha de respetar el **principio de calidad,** es decir, los datos han de ser adecuados, pertinentes y no excesivos para la finalidad del tratamiento. También han de ser exactos y se conservarán durante el plazo legalmente establecido. Los datos sensibles relativos a la salud exigen implican un nivel de seguridad alto, así como la implantación de todas las medidas de seguridad y herramientas previamente mencionadas.

Como es lógico, a EBB se le va a exigir garantías de seudonimización, anonimización, encriptación de datos y su mantenimiento, de modo que EBB ofrezca garantías a cualquier entidad privada del cumplimiento de las normas adecuadas.[68]

Cualquier hospital privado debe exigir un alto grado de transparencia e información relativa al lugar o programa Paas donde albergamos la información, o la copia de seguridad, así como certificados, portabilidad y la finalización de la relación jurídica. Toda esa información ha de estar detallada en el contrato de licencia.

En relación a la configuración contractual entre un proveedor privado de sanidad y EBB, he incluido dos anexos con un modelo de contrato de licencia de uso del software eB2MC en un Hospital Privado. En el ANEXO B aparecen detalladas todas las condiciones esenciales de un posible contrato de licencia con un hospital privado, al margen de las particularidades que se puedan negociar según el caso. En el ANEXO C, he incluido los términos y condiciones que desde la perspectiva de la protección de datos y de la sociedad de la información, EBB ha de cumplir.

3.2.1. La Responsabilidad civil derivada del uso del Software eB2MC.

[68] AEPD. (2016). Listado de cumplimiento normativo. Este documento es un complemento a las guías sobre EIPD y Análisis de riesgo de la AEPD. Contiene un listado muy completo sobre las obligaciones a las que ha de hacer frente cualquier organización en lo relativo al cumplimiento del RGPD.

La complejidad derivada del uso de los datos personales, la conectividad, la multiplicidad de componentes y los servicios que eB2MC ofrece, hacen de este tipo de herramientas, elementos de difícil encaje en el ordenamiento jurídico.

El problema más inmediato derivado del uso del software proviene de **las ciberamenazas**. A pesar de que no existan requisitos esenciales obligatorios específicos frente a las ciberamenzas que afecten a los usuarios, sí que existen disposiciones en materia de seguridad en el Reglamento 2017/475/UE.[69]

Otro de los problemas que podemos encontrarnos como consecuencia del mal funcionamiento del software es el planteado por la **opacidad** de los sistemas basados en algoritmos. Será pues, necesario, contemplar la posibilidad de introducir requisitos de transparencia de los algoritmos, solidez, rendición de cuentas y cuando sea posible, supervisión humana y resultados imparciales.[70]

En este sentido, la adhesión a códigos de conducta o la incorporación de mecanismos de certificación antes mencionado serán esenciales para la exoneración de responsabilidad civil. En cualquier caso es importante señalar que, en materia digital y más concretamente en el ámbito de la IA, el nexo entre la causa y el resultado es complicado de demostrar ya que al gozar la IA de un alto grado de ubicuidad, existen muchos agentes involucrados, desde el proveedor de internet, el tipo de dispositivo, la plataforma en nube, e.t.c…[71]

En este contexto, la responsabilidad civil por mal funcionamiento del programa informático basado en IA va a sufrir un enorme cambio en los próximos años ya que además de todo lo mencionado, los programas informáticos también interactúan con otro tipo de tecnologías más rutinarias de tal manera que la responsabilidad se puede llegar a dividir entre muchos agentes y será más difícil de determinar a los responsables.

Como ya hemos mencionado en el apartado 2.8.2, con motivo de la evolución exponencial de las aplicaciones y programas derivados de la IA se están incorporando muchas normas relativas al cumplimiento, certificaciones y recomendaciones generales provenientes de entidades de certificación privadas.

---

[69] Comisión Europea. (2020). Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica. Pp 8.
[70] Ibid, p 9.
[71] Ibid, p. 16. "*Si bien el programa informático que dirige las operaciones de un producto físico puede considerarse una parte o componente de este, algunos tipos de programas informáticos autónomos podrían ser más difíciles de clasificar.*"

Al margen de las acciones de responsabilidad civil por vulneración al derecho al honor previstas en el Código Civil,[72] vamos a centrar nuestro análisis en las acciones orientadas a obtener una indemnización por daños y perjuicios previstas en el RGPD.[73]

Para que un usuario pueda reclamar una indemnización por medio de la acción derivada del RGPD, tendrá que acreditar que concurren los elementos siguientes:[74]

- La condición de responsable o encargado del tratamiento del reclamado:
  En este sentido, ambos pueden ser responsables ante el interesado, razón por la cual, se ha insistido en otros epígrafes en tratar de delimitar con el mayor grado de exactitud la posición que ostenta cada parte. Una de las novedades del RGPD es incluir al encargado de tratamiento como sujeto pasivo de la responsabilidad derivada de sus actuaciones.
- Una infracción de la normativa RGPD sobre la protección de datos personales:
  En la mayor parte de los casos, la infracción es consecuencia de la falta de diligencia del responsable o del encargado. De ahí que se hiciera especial hincapié en la responsabilidad proactiva a la hora de crear diseñar el sistema de información.
- Los daños y perjuicios sufridos:
  Abarca tanto daños morales como patrimoniales. Las infracciones derivadas de la elaboración de perfiles son bastante comunes, aunque a estas hay que sumarles las causadas por fallos de seguridad de la información en línea.
- Una relación de causalidad entre la infracción y el resultado dañoso:
  Hay que destacar que los daños derivados de datos sensibles no sólo pueden reclamarse por parte del usuario directamente, hay personas físicas que de modo indirecto pueden verse afectados por el mal funcionamiento del programa,[75] sin embargo, cada uno de ellos responderá únicamente por el daño causado.

En lo que se refiere a la exclusión de la responsabilidad, en los casos de fuerza mayor o culpa exclusiva del usuario, tanto el responsable como el encargado, quedarán

[72] Artículo 1902 del Código Civil.
[73] Artículo 82 RGPD.
[74] Rubí Puig, A. (2018). Daños por infracciones del derecho a la protección de datos personales. *Revista de Derecho Civil* (5), pp. 53-87.
[75] En los casos de que se divulgue alguna enfermedad hereditaria psicopática, afectará no solamente al titular sino también al heredero.

exonerados de una infracción de una norma. En el contrato de licencia, incluiremos una cláusula con esta circunstancia.

Por otro lado, cabe destacar que a nivel europeo, existen normas como la Directiva 85/374/CEE, de responsabilidad de daños causados por productos defectuosos. Por lo tanto, parece conveniente la suscripción a un seguro de responsabilidad civil adecuado ya que en caso de un perjuicio causado a un tercero, estén cubiertos los gastos derivados de la indemnización.

4. La Propiedad Intelectual del Software.

El Convenio de Berna, la Directiva 2004/48/CE, relativa al respeto de los derechos de propiedad intelectual, la Directiva 2009/24/CE, sobre protección jurídica de programas de ordenador y la legislación nacional, a través del TRLPI, otorgan una protección jurídica a los programas de ordenador semejante al de una obra literaria, esto significa que un software es susceptible de albergar y generar derechos de autor.

Estos derechos se generan una vez se hayan creado, y por lo tanto, para poder demostrar su autoría con mayor éxito, conviene registrar la creación del mismo en un depósito notarial o en un registro público de propiedad intelectual. A través de este tipo de mecanismos conseguiremos alcanzar la plena validez probatoria. En este contexto, es muy importante destacar la importancia del código fuente sobre el Software ya que será el elemento principal sobre el cual se articule el derecho de autor.

A pesar de la importancia de esta consideración, hay dos cuestiones cuyo planteamiento jurídico genera ciertas dudas debido a su transversalidad. Por un lado, la protección relativa al algoritmo y por otro, la Inteligencia Artificial.

4.1 Tratamiento jurídico del algoritmo.

La aparición del algoritmo en el mundo jurídico plantea no pocos problemas de diferente calado, cuyas posibles soluciones no seríamos capaces de abarcar en este informe. No obstante, es necesario tener una aproximación básica al reto jurídico que plantea un elemento matemático de este tipo, para poder afrontar cualquier incidencia desde el punto de vista de la propiedad intelectual. Un algoritmo se puede definir como ”*el conjunto de reglas que, aplicada sistemáticamente a unos datos de entrada*

apropiados, resuelven un problema en un número finito de pasos elementales".[76] Al tener la misma consideración que una fórmula matemática, no puede ser objeto de registro de la propiedad intelectual.

Sin embargo, existen mecanismos mediante los cuales un algoritmo puede estar protegido jurídicamente. En este sentido, un algoritmo puede percibirse como un secreto profesional debido a que la aplicación de un algoritmo en combinación con más elementos suponen la capacidad o "Know-how" de una organización para llevar a cabo una tarea específica. Desde esta perspectiva, el algoritmo está protegido bajo el paraguas de la Ley de Competencia Desleal y la Directica 2016/943/UE, relativa a la protección de los secretos comerciales, transpuesta en nuestra legislación nacional por la Ley 1/2019, de 20 de febrero de secretos empresariales.[77]

En este contexto, la protección que ofrece este marco normativo, depende de la actitud de la empresa para mantener en secreto el algoritmo. Por lo tanto, las medidas a las que hemos hecho referencia con anterioridad, como la encriptación de archivos o la limitación de acceso, son perfectamente homologables a este ámbito. Por este motivo, es muy importante especificar todos los extremos relativos al secreto profesional y a la confidencialidad a través de un NDA.

Con arreglo a esta consideración, no solo tendrán cabida acciones civiles propias del derecho de marcas, sino que a las acciones derivadas de la competencia desleal hay que sumar acciones penales como la violación de secreto profesional o el uso ilícito de información privilegiada.

Situación parecida puede deducirse de las *bases de datos sui generís.*[78] De la misma manera que un software tiene la consideración de una obra literaria, una base de datos cuya originalidad[79] quedara fuera de toda duda, es susceptible de ser registrada. No obstante, si EBB tiene una base de datos y logra demostrar el esfuerzo y la inversión

[76] Peña Marí, R. (2020). ¿Qué es exactamente un algorimo?, *Retina, El País*. Recuperado de: https://retina.elpais.com/retina/2018/03/22/tendencias/1521745909_941081.html

[77] González Royo, I. (2016). Blog, Protección de activos intangibles en el contexto del Fintech, *Garrigues*. Recuperado de: http://blog.garrigues.com/proteccion-de-activos-intangibles-en-el-contexto-del-fintech-finance-technology/

[78] Artículo 12 de la ley de Propiedad Intelectual.

[79] Esta originalidad quedará determinada en función de la ordenación de los datos, el almacenamiento, los criterios de selección…

realizada para conseguirla, puede y debe inscribir dicha base con el objetivo de alcanzar toda la protección que la ley le confiere.[80]

4.2. Tipos de contratos de Propiedad Intelectual.

4.2.1. La licencia de uso o concesión de licencia de uso.

Este tipo de contrato permite a EBB, otorgar una licencia para que el SERMAS o un proveedor independiente, use el programa durante un periodo de tiempo determinado. O dicho de otro modo, es como si EBB prestase el software para que lo utilice un licenciatario bajo los términos y condiciones que ambos negocien.

Normalmente, para este tipo de contratos, se establece un régimen de no exclusividad y de carácter intransferible.[81] Es decir, que el licenciatario no tiene por qué ser el único beneficiario de la licencia y que no puede distribuir el software sin la autorización del licenciante. En este sentido, se puede otorgar al licenciatario la facultad de "sublicenciar" el programa. Esto significa que EBB autoriza al licenciatario para que desarrolle, modifique o distribuya el software, dentro del alcance de los límites establecidos en el contrato. Este tipo de acuerdo permite al licenciante la oportunidad de ampliar el volumen de negocio ya que permite a los interesados ajustar el programa a sus necesidades.

Este cláusula de sublicencia, puede establecerse con carácter exclusivo sobre un derecho de explotación en concreto, por ejemplo, se puede otorgar el derecho exclusivamente de desarrollo o exclusivamente de distribución. En ocasiones, será recomendable elaborar un acuerdo única y exclusivamente para cada autorización de licencia concreta.

4.2.2. La licencia de obra derivada.

---

[80] STJUE, asunto C-388/02, (petición de decisión prejudicial planteada por leHogsta domstolen): Fixtures Marketin Ltd contra Svenska Spel. "*El concepto de inversión destinada a la obtención del contenido de una base de datos(...) debe entenderse en el sentido de que designa los recursos dedicados a la búsqueda de datos ya existentes y a su recopilación en dicha base*".

[81] El artículo 99 del TRLPI prevé que salvo prueba en contrario, *"la cesión del derecho de uso tiene carácter no exclusivo e intransferible y la primera venta del producto en la Unión Europea de una copia de un programa por el titular de los* ***derechos o con su consentimiento, agotará el derecho de distribución*** *de dicha copia, salvo el derecho de controlar el subsiguiente alquiler del programa o de una copia del mismo."*

Mediante este acuerdo, se autoriza al licenciante a que desarrolle un software similar a *Eb2MC*. Esta modalidad contractual permite crear una *"marca blanca"* del software primigenio. No obstante, no se llega a ceder el código fuente, simplemente se ciñe a cuestiones concretas del programa que puedan interesar al licenciatario, pasando a ser el licenciante de la obra derivada y obteniendo todos los derechos de propiedad intelectual derivados de la obra resultante.

4.2.3. Acuerdo de cesión de los derechos de propiedad intelectual sobre desarrollo informático.

Con este acuerdo, EBB actúa como cedente de los derechos de propiedad intelectual patrimoniales, también en régimen de exclusividad, con carácter intransferible y durante un periodo de tiempo pactado. En los casos en los que algún operador de telecomunicaciones, o un laboratorio con su propio equipo de desarrolladores estén interesados en el programa, puede ser más frecuente este tipo de contratos, ya que es posible que les interese algún módulo del programa y quieran optar por cambiar alguna prestación o adaptarla a sus necesidades.

Este tipo de acuerdo, le puede permitir a EBB obtener rentabilidad sin ceder el código fuente, además de favorece el desarrollo de la aplicación.

4.2.4. Acuerdo de Investigación y Desarrollo.

Este tipo de acuerdos pueden llevarse a cabo cuando haya una empresa que subcontrate actividades de investigación o en el caso de que EBB considere oportuno colaborar con otras empresas, incluso con competidores.[82]

4.2.5. Acuerdo de licencia con el SERMAS.

La relación contractual con la administración implicará, como hemos analizado en el capítulo tercero, una voluntad de negociación por ambas partes. En el caso de la CPI, es posible que desde la administración se exijan ciertas condiciones para la adjudicación, como por ejemplo, la concesión de derechos de uso, y desarrollo de

[82] European IPR Helpdesk. (2016). Su Guía sobre la Comercialización de la PI y Contratos. pp, 44. Recuperado de: www.iprhelpdesck.edu

software, de distribución o incluso de exclusividad. En este sentido, la administración establecerá en los pliegos las reservas que consideren exigir, incluso llegando a tener acceso al código fuente.[83]

4.2.6. Acuerdo de Confidencialidad.

En los casos en los que se ceden derechos de propiedad intelectual, es bastante corriente que los licenciatarios abusen de su posición debido a que en ocasiones, el límite de la licencia es confuso y el licenciatario puede tender a abusar de la confianza depositada por el licenciante. En este contexto, es muy importante defenderse de una eventualidad de este tipo por medio de un Non-Disclosure agreement o NDA.

Uno de los elementos más importante del acuerdo de confidencialidad es el relativo al **registro de la información.**[84]. En este sentido, el registro previo de cierta información cobra especial importancia ya que dicho registro ofrecerá garantías suficientes para que la información en cuestión no pueda ser refutada, con independencia del acuerdo de licencia de uso, la autoría de dicha información, un código fuente, u otro aspecto relevante del software.

Por la propia naturaleza del producto software, será necesario que los empleados o estudiantes tengan acceso a información confidencial y no pueda evitarse la divulgación de cierta información, para lo cual, es conveniente establecer una cláusula de permiso de divulgación de información confidencial en la que se especifique la **"necesidad de conocer".** Ahora bien, se hará especial hincapié de las condiciones concretas en las que se puede divulgar y se concienciará a cada uno de los firmantes sobre la importancia de dicha cláusula.

En el ANEXO B, he incluido una cláusula de confidencialidad que puede servir como ejemplo, aunque variará en función del caso y de cada situación en particular.[85]

4.3. Responsabilidad civil por infracción de derechos de la propiedad intelectual.

[83] MINHAFP. (2015). Guía 2.0 para la compra pública de innovación. Pp, 67.
[84] European IPR Helpdesk. (2015). *"Acuerdo de no divulgación: una herramienta comercial.* Recuperado de: http://www.iprhelpdesk.eu/
[85] OMPI. (2010). Intercambiar Valor. Negociación de acuerdos de licencia de Tecnología. Manual de capacitación, pp 40.

La protección intelectual de un programa de ordenador está prevista en el Título VII del TRLPI. Conviene destacar que los derechos de protección intelectual no protegen las ideas sobre este software o la función que se logra con la implementación de dicho software.[86] En este contexto, conviene detenerse a estudiar los elementos generadores de derechos de protección intelectual según el artículo 96 del TRFLPI, a saber:

- El código fuente y objeto;
- La documentación preparatoria, técnica y manual de uso;
- Cualquier forma de expresión del programa de ordenador;
- Cualesquiera versiones sucesivas y derivadas;

Es importante tener claro este punto a la hora de elaborar los contratos de licencia de uso con un licenciatario, especialmente si se optase por un contrato de sublicencia o de obra derivada.

En lo que atañe a las posibles acciones previstas en la ley para reclamar la responsabilidad civil correspondiente, debe tenerse presente la existencia de dos acciones no excluyentes. Por un lado, podría acudirse a la responsabilidad contractual del derecho común civil previamente analizada, y por otro lado, la vía prevista en la legislación sobre propiedad intelectual.

En este sentido, parece conveniente destacar una reciente Sentencia del TJUE.[87] De esta decisión, podemos extraer la perfecta convivencia de la acción civil por daños y perjuicios, derivada del derecho nacional, y infracción de los derechos del titular frente al licenciatario previstos en la Directiva 2004/48/CE, sobre la protección jurídica de programas de ordenador. Es decir, que ambas acciones pueden invocarse para reclamar una posible indemnización por daños y perjuicios ya que son compatibles entre sí.

[86] STJUE, asunto C-406/10, 2 de mayo de 2012. SAS Institute vs. World Programming Ltd. Conclusión 61. "No puede haber infracción del derecho de autor sobre el programa de ordenador cuando, (…), el adquirente legítimo de la licencia no ha tenido acceso al código fuente del programa de ordenador correspondiente a esa licencia, sino que se limitó a estudias, observar y verificar ese programa con el fin de reproducir su funcionalidad en un segundo programa."

[87] Sentencia TJUE, asunto C-666/18, iT Development contra Free Mobile, de 18 de diciembre de 2019, conclusión 49.

IV. CONCLUSIONES

I. El impacto producido por la Inteligencia Artificial en el ámbito sanitario está suponiendo una nueva revolución científica a nivel global**.** La implementación del software eB2MC supondría no sólo una oportunidad única para explorar el rendimiento y la eficacia del Software, sino que también sería un gran aporte para el propio Servicio Madrileño de salud. Así mismo, la agenda de innovación y desarrollo fomentada desde las instituciones europeas incluye al sector privado como parte de su estrategia, por lo tanto, estamos ante una gran oportunidad para colaborar con otras entidades sanitarias, hospitales privados y laboratorios de biotecnología.

II. Existen razones para ser optimistas en la obtención del marcado CE. Ahora bien, la mejora técnica en la toma de decisiones del Software y la incorporación de nuevas posibilidades y opciones en el programa, ayudarán a la obtención de dicho marcado. La documentación relativa al sistema de gestión de la organización y las instrucciones de fabricación requeridas por la AEMPS, son la principal razón de retraso en la solicitud de licencia de fabricación de productos sanitarios, y por ello, es importante ser exhaustivos con su preparación.

III. La privacidad es el factor entorno al cual gravitan todos los peligros y riesgos potenciales, por lo tanto, todas las acciones preventivas y reactivas deben tener como objetivo preservar la privacidad en todas sus dimensiones. Desde esta perspectiva, es fundamental ocuparse de la calidad y la seguridad de los datos en todas las etapas de creación y desarrollo del Software, ya sea en la concepción, en el desarrollo, explotación y retirada. La ciberseguridad ha de plantearse como un desafío cuya implementación ha de ser abordada desde una perspectiva garantista que reduzca el riesgo al mínimo posible y siempre como un proceso continuo y continuado en el tiempo.

El análisis de riesgos, la identificación de las amenazas contra la información y contra las infraestructuras son algunas de las actividades fundamentales para garantizar la seguridad del sistema y de la organización. Así pues, todas las precauciones son pocas y por lo tanto, la implementación de un Sistema de Gestión de la Información bajo el parámetro de la norma ISO 27001 o del ENS es fundamental para probar la capacidad de reacción y el carácter proactivo de la empresa.

IV. Una parte del proceso de la CPI implica la consulta previa del mercado y del estado del arte por parte del SERMAS y por lo tanto, es necesario mantener un nivel de comunicación fluida y generar un nivel de confianza propicio para asegurar la opción de compra o contratación. En este sentido, resulta imprescindible prestar atención a todas las actualizaciones tecnológicas y publicaciones sobre los procesos de contratación. El órgano de contratación establecerá unos criterios de evaluación de la oferta, generalmente basándose en el precio propuesto. Por ello, es necesario justificar con enorme rigurosidad en el expediente de contratación, el carácter único del Software.

V. Un software informático goza del mismo régimen de protección intelectual que una obra literaria. Es muy importante destacar la importancia del código fuente sobre el Software ya que será el elemento principal sobre el cual se articule el derecho de autor. Sin embargo, el algoritmo tiene un tratamiento diferente, a pesar de lo cual, existen mecanismos para garantizar su protección. En este sentido, un algoritmo puede percibirse como un secreto profesional y por lo tanto está protegido bajo el paraguas de la Ley de Competencia Desleal y la Directica 2016/943/UE, relativa a la protección de los secretos comerciales, y por la Ley 1/2019, de 20 de febrero de secretos empresariales

VI. Existen varias modalidades de contrato de licencia pero el contrato de licencia de uso es el más común. Para este tipo de contratos, se establece un régimen de no exclusividad y de carácter intransferible. Es decir, que el licenciatario no tiene por qué ser el único beneficiario de la licencia y que no puede distribuir el software sin la autorización del licenciante.

En el caso de la CPI, es posible que desde el SERMAS se exijan ciertas condiciones para la adjudicación, como por ejemplo, la concesión de derechos de uso, y desarrollo de software, de distribución o incluso de exclusividad. En este sentido, el SERMAS establecerá en los pliegos, las reservas que consideren exigir, incluso llegando a tener acceso al código fuente. En los casos en los que se ceden derechos de propiedad intelectual, es bastante corriente que los licenciatarios abusen de su posición debido a que en ocasiones, el límite de la licencia es confuso y el licenciatario puede tender a abusar de la confianza depositada por el licenciante. En este contexto, es muy importante defenderse de una eventualidad de este tipo por medio de un NDA.

V. BIBLIOGRAFÍA

- Asociación Española de Protección de Datos. Expediente TD/0091/2018. Resolución N: R7001455/2018.
- Asociación Española de Protección de Datos.. Expediente TD/00194/2019. Resolución R/00492/2019.
- Asociación Española de Protección de Datos.. (2019). Guía para pacientes y usuarios de la sanidad. Pp. 10. Recuperado de: www.AEPD.es
- Asociación Española de Protección de Datos.. (2020). Adecuación al RGPD de tratamientos que incorporan IA. pp18. Excepción doméstica: Considerando 18 del RGPD.
- Aguirre Beltrán, *J.L.* (2017). Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*." SESPAS,* Página, 53-55.
- Agencia Valenciana de la Innovación. (2019). Guía Práctica del Proceso de Compra Pública de Innovación para Organismos Públicos de la Comunidad Valenciana. Pp, 33-35.
- Barrios, J. (2019). Gobernanza de datos en el sector salud. *Health and Big Data*. Disponible en https://www.juanbarrios.com/el-gobierno-del-dato-data-governance/
- Cassinello, Sánchez Pablo. (2019). Inyección de inteligencia artificial para el sector sanitario. IA en el sector sanitario: encuesta a directivos. *Accenture Consulting*, pp 6-9.
- Cotino Hueso, Lorenzo. (2019). Ética en el diseño para el desarrollo de una inteligencia artificial, robótica y big data confiables y su utilidad desde el derecho. *Revista Catalana De Dret Públic*. N: 58, pp. 13-15.
- Comunidad Europea, (1984-1988). Programa Europeo de investigación y desarrollo en el campo de las tecnologías de la información (ESPRIT)**.** Recuperado de https://cordis.europa.eu/programme/id/FP1-ESPRIT-1/es
- Comisión Europea. (2012). Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las Regiones.

- Comisión Europea, (2014). El Programa Marco de Investigación e Innovación Dirección General de Investigación e Innovación. HORIZONTE 2020. "Con una dotación de 80.000 millones de euros, el programa Horizonte pretende ser el programa de investigación puesto en marcha por la UE. Recuperado de : www.ec.europa.eu/horizon2020
- Comisión Europea. (2016). Study on Big Data in Public Health, Telemedicine and Healthcare Executive summary, pp 9.
- Comisión Europea. (2016). Guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices. (2016).
- Comisión Europea. (2016) Casos de éxito CPI en Europa-Eafip.. Recuperado de: https://www.youtube.com/watch?v=Ni6w9raLwYU
- Comisión Europea. (2017). eHealth Network. Multiannual Work Programme 2018-2021, eHealth in support for better health.
- Comisión Europea. (2018). Índice de la Economía y la Sociedad Digitales (DESI), Informe de país para España. Plan de Transformación digital de la Administración General del Estado y sus Organismos Públicos 2015-2020
- Comisión Europea. (2019). Comunicación de la comisión al Parlamento Europea y al Consejo y al Comité económico y social Europea y al comité de las Regiones. Pp 168.
- Comisión Europea. (2020). The impacto of GDPR on IA., pp. 80-82.
- Comisión Europea. (2020). Libro blanco de la Inteligencia Artificial, *Sobre la inteligencia artificail- un enfoque europeo orientado a la excelencia y la confianza*, pp 9.
- Comité Europeo de Protección de Datos. (2019). Directrices 1/2019. Pp. 3-5. Recuperado de: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_es
- Consejo Asesor de Sanidad. (2014). E-Salud: prioridad estratégica para el sistema sanitario. Recuperado de: http://www.infocop.es/view_article.asp?id=5071&cat=9
- Consejo Asesor de Sanidad. (2014). Es por Madrid. Plan estratégico de Telemedicina 2014-2020. Recuperado de:

https://www.espormadrid.es/2014/04/plan-estrategico-de-telemedicina-2014.html

- Cotino Hueso, Lorenzo. (2019). Ética en el diseño para el desarrollo de una inteligencia artificial, robótica y big data confiables y su utilidad desde el derecho. *Revista Catalana De Dret Públic*. N: 58, pp. 13-15.
- De las Heras Rodríguez, T. (Julio 2019). *Legal challenges of artificial intelligence: modelling the disruptive features of emerging technologies and assessing their possible legal impact. Oxford Academic*, *Uniform Law Review*, 24, pp. 302–314. Recuperado de https://academic-oup-
- De Lima, D (2018). Informe sobre Trasformación Digital en Salud en España Compromisos vs Realidad. *Asociación Salud Digital,* pp 135. Recuperado de: www.salud-digital.es
- European IPR Helpdesk. (2015). Acuerdo de no divulgación: una herramienta comercial. Recuperado de: http://www.iprhelpdesk.eu/
- European IPR Helpdesk. (2016). Su Guía sobre la Comercialización de la PI y Contratos. Pág 44. Recuperado de: www.iprhelpdesck.edu
- García Díaz, J. (2019). Un Nuevo Marco en la Ciberseguridad y la Protección de Datos. *Revista de la Sociedad Española de la Informática y Salud*, (134), pp 19-20.
- García Vidal, A. (2017). Los programas informáticos como productos sanitarios. *Revista CESCO*, (22), p. 6.
- Grupo de Trabajo del artículo 29. (2014). Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud el artículo 7 de la Directiva 95/46/CE. El interés legítimo como base de legitimación tiene ciertas particularidades y exige un alto grado de responsabilidad por parte del responsable. Pp. 30-33.
- Grupo de coordinación de Productos Sanitarios. (2020). MDCG 2020-1 "*Guidance on Clinical Evaluation (MDR)/Performance Evaluatios (IVDR) of Medical Device Software*". Este documento está respaldado y aprobado por un grupo creado en el Reglamento 2017/475 UE en su artículo 103, (MDCG). Grupo de Coordinación de Productos Sanitarios.

- González Royo, I. (2016). Blog, Protección de activos intangibles en el contexto del Fintech, *Garrigues*, Recuperado de: http://blog.garrigues.com/proteccion-de-activos-intangibles-en-el-contexto-del-fintech-finance-technology/
- Guía para autoridades Europea de Compra Pública en Innovación. (2016). Pp 27. Recuperado de: www.innovation-procuremente.org
- Guía de contratación pública de innovación. (2019). Ayuntamiento de Madrid. Pp, 29-32.
- Guillén, Raúl. "Retos a la Hora de Proteger la Ciberseguridad de los Hospitales Conectados". *Revista de la Sociedad Española de la Informática y de la salud*. Num. 134, páginas 37-40.
- INCIBE. (2018). Copias de seguridad: Una guía de aproximación para el empresario. Páginas 14-16.
- Malonda, V. (2020). Que es la Salud Digital y e-Salud. *Principio Activa*, Recuperado de: https://principioactiva.com/salud-digital-e-salud/
- Ministerio de Ciencia, Innovación y Universidades. (2019). *Estrategia Española de I+D+I en Inteligencia Artificial*. pp 30.
- Moisés Barrio, Andrés. Robots, inteligencia artificial y persona electrónica. *Sociedad Digital y Derecho*, Capítulo 4. 2018.
- Monteagudo Peña, J.L. (2019). La e- Salud en el marco de la Unión Europea. Aspectos organizativos, legislativos y operacionales. *Club Gurterch*, pp. 14-16. Recuperado de https://www.clubgertech.com/
- Organización Mundial de la Propiedad Intelectual. (2010). Intercambiar Valor. Negociación de acuerdos de licencia de Tecnología. Manual de capacitación. WipoPI.Pdf. Pp 40.
- Organización Mundial de la Salud. CANCER. (2018). Recuperado de: https://www.who.int/news-room/fact-sheets/detail/cancer
- Renita, D. (2019). Top Predictions That will DisruptHealthcare in 2020. *Forbes*. Recuperado de: https://www.forbes.com/sites/reenitadas/2019/12/04/top-8-predictions-that-will-disrupt-healthcare-in-2020/#5319179b7f1e
- Rubí Puig, A. (2018). Daños por infracciones del derecho a la protección de datos personales. *Revista de Derecho Civil,* (5), pp. 53-87.

- Torra, V. (Diciembre 2011). La Inteligencia Artificia, *Instituto de Investigación en Inteligencia Artificial (CSIC)* . Recuperado de: www.fgcsic.es/lychnos/es_es/articulos/inteligencia_artificial
- Peña, Marí, R. (2020).¿Qué es exactamente un algorimo?,*Retina, El País.* Recuperado de*:* https://retina.elpais.com/retina/2018/03/22/tendencias/1521745909_941081.html
- Vázquez Matilla, F.J. (2019). Desde España: La Compra Pública por Innovación. *IDOM Consulting.* Recuperado de: https://idomcpi.com/desde-espana-la-compra-publica-de-innovacion/

VI. ANEXOS

ANEXO A

LEGISLACIÓN Y JURISPRUDENCIA

- Constitución Española. Boletín Oficial del Estado N311, de 29 de diciembre de 1978.
- Ley 14/1986, de 25 de abril, General de sanidad.
- Ley 21/2000, de 29 de diciembre, sobre los derechos de información concernientes a la salud y la autonomía del paciente.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal;
- Real Decreto 1591/2009, de 16 de octubre, por el que se regulan los productos sanitarios.
- La Ley33/2011, de 4 de octubre, General de la Salud Pública.
- Real Decreto Legislativo1/2015, de 24 de julio por el que se aprueba el texto refundido de la Ley de Garantías y uso racional de los medicamentos y productos sanitarios.
- Ley 39/2015, de 1 de octubre del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 9/2017, de 8 de noviembre de Contratos del Sector Público, por la que se trasponen al ordenamiento jurídico española Directivas del Parlamento Europeo y del consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de 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 (RGPD).

- Reglamento (UE) 2017/745 sobre Productos del Parlamento Europeo y del Consejo, de 5 de abril del 2017, sobre los productos sanitarios.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales.
- Ley 1/2019, de 20 de febrero de secretos empresariales.

Jurisprudencia

- Sentencia del Tribunal de Justicia de la Unión Europea, asunto C-388/02 (petición de decisión prejudicial planteada por leHogsta domstolen): Fixtures Marketin Ltd contra Svenska Spel.
- Sentencia del Tribunal de Justicia de la Unión Europea, asunto C-406/10, 2 de mayo de 2012SAS Institute vs. World Programming Ltd.
- Sentencia del Juzgado Contencioso-Administrativo núm 2 de Tarragona, núm 55/2014 de 4 de marzo.
- Tribunal de Justicia en sentencia de 7 de diciembre del 2017, en el asunto C-329/16 Syndicat National de lìndustrie des technologies m´wdecales.
- Sentencia del Tribunal de Justicia de la Unión Europea, asunto C-666/18, iT Development contra Free Mobile, de 18 de diciembre de 2019

ANEXO B

MODELO DE CONTRATO DE LICENCIA DE USO DEL SOFTWARE EB2MC[88]

En Madrid, a 25 de septiembre de 2020

REUNIDOS

De una parte el Hospital Privado, en adelante HP, LICENCIATARIO Y RESPONSABLE DEL TRATAMIENTO, quien tendrá acceso al software *EB2MC*, únicamente previa aceptación de todas y cada una de las cláusulas y condiciones del siguiente contrato.

De otra parte EVIDENCED-BASED BEHAVIOR S.L, LICENCIANTE Y ENCARGADO DE TRATAMIENTO, en adelante *EBB,* con NIF: 6565666565-l y domicilio en la Avenida Gregorio Peces-Barba, N1, Leganés 2919 MADRID.

MANIFIESTAN

I. Que, con motivo de la prestación de servicio contratado que ofrece *EBB* y que constituye el objeto del contrato principal, a saber, el Contrato de Licencia de uso del software *EB2MC*, ambas partes se comprometen a cumplir cada una de las cláusulas, incluyendo el acuerdo de confidencialidad y el uso que se haga de los datos de carácter personal.

II. Que, El ENCARGADO DEL TRATAMIENTO, tratará los datos de carácter personal por cuenta del RESPONSABLE, por lo que en cumplimiento del artículo 28 del RGPD y los artículos 28 y 33 de la LOPDGDD, ambas parte, de forma libre, acuerdan regular el tratamiento de los datos de carácter persona de acuerdo a las estipulaciones de este contrato.

III. Que, se reconocen mutua y legal capacidad para obligarse a cumplir los términos y condiciones del Contrato, de conformidad con las siguientes:

CLÁUSULAS

1- OBJETO. Es objeto del presente contrato otorgar la licencia de uso intransferible y no exclusiva, por parte del LICENCIANTE, propietario del Software, al LICENCIATARIO para utilizar el programa por parte del EBB al HP, del programa

[88] Este modelo de contrato está basado en un hipotético entre EBB y un hospital privado interesado en la implantación del software eB2MC.

denominado *EB2MC*, para la gestión de una evaluación objetiva y funcional del estado de los pacientes psiquiátricos mediante técnicas de machine learning e Inteligencia Artificial, analizando la información a partir de la información y datos del paciente aportada por HP. Que podrá utilizar por medio de las claves de acceso que el HP previo abono de la cuota mensual/anual y aceptación de las presentes CONDICIONES GENERALES, se le entregará.

EL HP manifiesta haber examinado y comprobado, las características, contenidos, capacidad y alcance específico del objeto de este Contrato, según se establece en la Oferta Comercial y en la información suministrada sobre éste, todo lo cual es plenamente aceptado en señal de conformidad por parte de HP. El pago de la licencia otorgada bajo el presente contrato, no constituye la compra de los programas ni de los títulos, ni derechos de autor correspondientes.

2- CONDICIONES ECONÓMICAS Y FORMA DE PAGO. La forma de pago será mediante suscripción mensual o anual. En el momento de realizar el primer pago mensual y la empresa EBB tenga constancia, se procederá dar acceso al software mediante las contraseñas que se facilitaran en el momento. La conexión on line al software a través de la plataforma EB2MC, estará activa mientras se procedan realizar los pagos. Los datos serán destruidos si el cliente comunica que no continuará con los servicios. En ningún caso, el HP tiene derecho a la devolución o restitución de las cantidades entregadas de otro importe derivado de cualquier servicio o suscripción.

El HP acepta que el EBB podrá emitir facturas electrónicas con relación a los servicios contratados y/o prestados a través de Internet, correo electrónico o cualquier otro medio electrónico o telemático, y acepta cumplir las obligaciones de pago derivadas de las mismas como si éstas hubiesen sido emitidas por escrito.

I. CONDICIONES Y VARIACIONES. El HP manifiesta que el servicio contratado, objeto de este Contrato, son conformes y aptos para los fines por los que los contrata. En ningún caso, HP podrá ceder, sublicenciar, distribuir, alquilar o transmitir de cualquier otra forma los accesos de referido programa o realizar explotaciones por cuenta de terceros.

II. VIGENCIA. El presente contrato estará vigente en tanto en cuanto esté vigente el contrato de prestación de servicios, por lo que en el momento en que se incumpla con la misma se suspenderá el servicio.

III. PROPIEDAD DE LOS PROGRAMAS Y DERECHOS DE AUTOR. El acceso al programa amparado por este contrato, las reproducciones originales de los mismos, cualquier copia parcial o total, realizada por el HP o por cualquier otra persona, los derechos legales de copia, los secretos comerciales, y de cualquier otro derecho intelectual o de propiedad, pertenecen al EBB, por lo que cuenta con las autorizaciones suficientes para otorgar a su vez licencias de uso sobre dicho programa. HP acepta y reconoce que el acceso on line al programa son secretos comerciales de EBB, así como toda la información o documentación que le sea proporcionada y que haya sido identificada por este como confidencial.

IV. ALCANCE DEL USO AUTORIZADO DE LOS PROGRAMAS. EBB proporciona al HP el acceso al programa mediante la web, a través de unas claves de acceso (password) de carácter confidencial y que tienen el carácter de intransferibles. Las contraseñas que se otorgan podrán ser modificadas por HP, pero en cualquier caso es de responsabilidad del HP el deber de secreto de las mismas, eximiendo de cualquier responsabilidad de pérdida o transferencia EBB. HP **no tendrá derecho de comercializar o sublicenciar en ninguna forma el acceso al programa de acceso on line**.

VI. DESISTIMIENTO DEL CONTRATO. Es causa esencial del presente Contrato, y por ello es aceptado por el HP que, una vez aceptado el mismo, se procederá cobro mensual/anual a EBB a la tarjeta/cuenta bancaria proporcionada. Para el caso de dejar pagar el mismo, se procederá suspender el servicio. El presente contrato también quedará resuelto y el HP perderá el acceso al software en los siguientes casos:

a) Mutuo acuerdo entre el HP y EBB que deberá tramitarse por medio de correo electrónico a EBB. Por transcurso del plazo de duración siempre que medie el preaviso antes indicado.

b) Por falta de pago de los Servicios por parte del HP.

c) Almacenamiento de información no relacionada con la salud y gestión medica.

d) Conducta agresiva, amenazas y actuaciones legales que puedan poner en peligro el uso de la plataforma o servicios prestados a los usuarios.

e) Por incumplimiento por parte de alguna de las partes de sus obligaciones. En este caso, la parte cumplidora deberá comunicar por escrito a la parte incumplidora el supuesto incumplimiento. El incumplidor tendrá un plazo de 15 días para corregir la

cuestión denunciada. En caso contrario la parte denunciante podrá declarar resuelto el presente contrato.

VII. PROTECCION DE DATOS. Atendiendo a la LOPDGDD, HP es el titular de la base de datos de sus pacientes y por tanto es el Responsable del Fichero, del tratamiento y gestión de referidos datos.

a) Protección de Datos. El HP consiente expresamente la incorporación de todos sus datos de carácter personal/ empresarial en un repositorio de información donde obran los datos de los usuarios de eB2MC, para que sean tratados por EBB con las finalidades descritas en los Módulos del software eBMC que HP, también acepta expresamente. El Delegado de Protección de Datos es Ramón Pérez (Ficticio).

Los datos incorporados se cancelarán y eliminarán cuando el HP lo solicite expresamente en su EJERCICIO DE DERECHO DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN. El USUARIO podrá ejercitar los derechos de acceso, rectificación y cancelación de datos, así como oponerse a su tratamiento de acuerdo con la LOPDGDD.

Para ejercitar estos derechos podrá dirigirse por correo electrónico a eB2.DPD.com. También podrá acceder a su información, rectificarla, solicitar su cancelación u oponerse a tratamientos mediante las opciones destinadas al efecto.

b) Obligaciones del HP. El HP, respecto el/los fichero/s que contiene/n datos de carácter personal de sus pacientes, expresa que cumple con todos los requisitos exigidos legalmente para su recogida y tratamiento. Asimismo, manifiesta que ha adoptado las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal incluidos en los ficheros, establecidas en la normativa vigente en materia de protección de datos personales.

c) Obligaciones de EBB. El acceso a el/los fichero/s facilitado/s por el USUARIO, será única y exclusivamente con el fin de realizar el traspaso y adaptación de base/s de datos, y prestar el servicio de mantenimiento técnico. EBB se compromete a tratarlo/s conforme a las instrucciones del HP, y a no aplicarlo/s o utilizarlo/s con fin distinto al estipulado en este contrato, ni comunicarlo/s, ni siquiera para su conservación a otras personas. Asimismo, el EBB implementará las medidas técnicas y organizativas necesarias, que garanticen la seguridad e integridad de los datos de carácter personal incluidos en el/los fichero/s y que eviten su alteración, pérdida, tratamiento o acceso no

autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana, del medio físico o natural. Las medidas de seguridad mencionadas son las determinadas en la normativa vigente sobre protección de datos personales.

d) Deber de secreto. EBB se compromete al secreto profesional respecto a los datos incluidos en el/losfichero/s, obligación que subsistirá aún después de finalizar sus relaciones con el HP. Dicho deber de secreto afecta a todo el personal de eB2 que pueda tratar datos personales de los ficheros facilitados por el HP.

e) Subcontratación. El HP, será quien se encargará de prestar y resolver cualquier incidencia con el programa objeto del presente contrato así como de las futuras actualizaciones o versiones del mismo y así como también consiente la subcontratación del almacenamiento de la información contratado con los servidores que se ha previsto con la empresa Microsoft (por Ejemplo), la cual proporciona todas las garantías de seguridad y confidencialidad que se exige en materia de protección de datos dotándolos de una seguridad de nivel alto.

La empresa Microsoft.(EJEMPLO FICTICIO DE PAAS), goza de la solvencia nacional e internacional en la prestación del servicio contratado, asegurando un servicio seguro realizando las copias de seguridad de forma automática. La empresa Microsoft con la que se tiene contratado el servicio de servidores, no tendrá acceso a los datos del HP por estar estos encriptados, pero para el caso de que por causas de mantenimiento tuviera que acceder a datos, procederá actuar con las instrucciones que en el presente contrato se han establecido, en materia de seguridad y protección de datos.

La empresa con la que se tiene contratado el servicio de mantenimiento y actualización del programa, no tendrá acceso a los datos del HP por estar estos encriptados, pero para el caso de que por causas de mantenimiento tuviera que acceder a datos, procederá actuar con las instrucciones que en el presente contrato se han establecido, en materia de seguridad y protección de datos.

f) Destrucción o devolución de la información. Tras la solicitud por parte del cliente en el apartado anterior, EBB deberá cancelar el/ los fichero/s con datos de carácter personal facilitado/s por parte del HP. Este fichero tendrá que ser destruido o devuelto al HP, igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento.

f) *Descripción técnica.* El presente software destinado al tratamiento de datos personales cumple con las medidas de seguridad de Nivel Alto de acuerdo con lo establecido en la legislación vigente a la fecha del presente acuerdo. Por lo tanto el presente programa está dotado de todas las prestaciones necesarias de seguridad pertinentes para cumplir con la legislación actual.

VI. SUBCONTRATACIÓN. EBB no podrá subcontratar con un tercero la realización de ningún tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del ENCARGADO. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de ***1 mes*** indicando los tratamientos que se pretende subcontratar e identificando, de forma clara e inequívoca, la empresa Subcontratista y sus datos de contacto. **La subcontratación sólo podrá llevarse a cabo si el responsable da su autorización expresa en el plazo establecido**.

IV.RESPONSABILIDAD. El responsable de los datos y su tratamiento es del HP, como responsable del fichero. El HP es el responsable como titular, de los datos contenidos en la base de datos y de sus pacientes y de tener debidamente inscrito ante la Agencia de Protección de Datos, el fichero correspondiente para su tratamiento. El HP es responsable de verificar por si mismo y asegurarse de que el software, las condiciones de almacenamiento de datos y seguridad, cumplen con la legislación española.

El ENCARGADO DEL TRATAMIENTO queda exonerado de cualquier responsabilidad que se pudiera generar por el incumplimiento por parte del RESPONSABLE DEL TRATAMIENTO de las estipulaciones del presente documento, así como de lo previsto en el RGPD, en cuyo caso será el Responsable del Tratamiento, respondiendo de las infracciones en que pudiera incurrir, quien deba ocuparse de cualquier reclamación de indemnización que los interesados pudieran interponer ante la Autoridad de Control o ante los Tribunales.

En concreto, El RESPONSABLE DEL TRATAMIENTO será directamente responsable frente a los consumidores, Agencia Española de Protección de Datos, Administraciones Públicas y cualesquiera Juzgado o Tribunal, del sistema de obtención de datos utilizado y la propia obtención de los mismos, exonerando expresamente al ENCARGADO de cualquier responsabilidad a este respecto y debiendo reintegrar a éste cualquier sanción

o indemnización a la que tenga que hacer frente por el incumplimiento del RESPONSABLE, así como los daños y perjuicios que dicho incumplimiento pudiera ocasionarle.

EBB no será responsable por cualquier daño y/o perjuicio:

a) Cuando el HP o las personas de las que deba responder sean las culpables de tales daños y perjuicios.

b) Causado a terceros.

c) Por pérdida de datos, dado que el HP no tiene acceso a los mismos, simplemente proporciona el servicio del programa on line a través de Internet por medio de las claves de acceso.

d) Por lucro cesante o ganancias dejadas de obtener por el HP y/o terceros en caso de pérdida de datos o caída del sistema.

e) Por cualquier circunstancia de fuerza mayor, caso fortuito, fallo o error de las líneas de comunicación, o de la prestación defectuosa o fallo de la red Internet o de la plataforma de Cloud que albergue toda la información y los datos (Microsoft Cloud/Azure).

f) Por la utilización y/o acceso y/o conexión a su página web y/o a páginas a ella enlazadas, a causa del funcionamiento incorrecto, defectos y/o fallos causando daños, totales y/o parciales, a todo hardware, software y/o programas informáticos, así como de la pérdida, alteración y/o daños, totales y/o parciales sobre información contenida en el dispositivo electrónico que albergue la aplicación.

EBB no garantiza que el sitio web vaya a funcionar constante, fiable y permanentemente, sin retrasos o interrupciones por lo que EBB no se responsabiliza por cualquier daño y/o perjuicio y/o beneficios dejados de obtener por el HP/Usuarios y/o cualquier otro tercero que se vea perjudicado como consecuencia de tales circunstancias.

En cualquier caso, EBB en cuanto tenga conocimiento de referida incidencia procederá lo antes posible proceder restablecer el servicio, sin que en tal caso puedan derivarse responsabilidades al EBB.

HP, no se hará responsable de en el caso de realizar la migración de datos del sistema actual del HP al nuevo que se que contrata mediante la presente, de la perdida de cualquier dato que no estuviera indicado en los campos de datos del nuevo software. El

Servicio Técnico de EBB o el personal debidamente subcontratado por éste, son los únicos autorizados para realizar y resolver las incidencias que puedan surgir en los servidores instalados en Microsoft.

VIII. CONFIDENCIALIDAD. El personal y el servicio técnico de EBB guardarán la más absoluta reserva, seguridad e integridad de los procesos, datos e información perteneciente facilitada por el HP. EBB se compromete a no divulgar la información de HP a la que tenga acceso, a no utilizarla ni copiarla.

IX. INTERLOCUTOR. El interlocutor habitual que, por parte del HP, intervenga en cualquiera de los servicios o transacción entre las partes, es designado por éste como persona plenamente autorizada y con plenas facultades para adoptar cualquier decisión.

X. MODIFICACIONES. Ninguna cláusula del presente contrato podrá ser modificada, suprimida o agregada por una de las partes unilateralmente. Toda proposición de cambio deber ser comunicada y aceptada por escrito un mes antes de la fecha de realización.

XI. COMPETENCIA. Las partes renuncian expresamente al fuero de sus domicilios y se someten a la competencia de los Jueces y Tribunales de la ciudad de Madrid, así mismo, declaran expresamente que en todo lo no previsto en el presente contrato se rigen por lo dispuesto en el Código Civil en lo que fuera pertinente.

ANEXO C

TÉRMINOS Y CONDICIONES DE USO DE LA APLICACIÓN

PARA USUARIOS[89]

Estos Términos y Condiciones regulan la descarga, acceso y utilización de la aplicación móvil eB2, para usuarios y pacientes (en adelante, la "APLICACIÓN"), que eB2MC ponen a disposición de los usuarios. Esta versión de la APLICACIÓN está disponible de forma gratuita. El acceso a la APLICACIÓN supone que el usuario reconoce ha aceptado y consentido sin reservas de las presentes condiciones de uso.

1. OBJETO. La APLICACIÓN tiene el objetivo de acceder a un área del software eB2MC para permitir el acceso y transmitir datos médicos de forma privada y con seguridad. En el diseño y desarrollo de esta APLICACIÓN han intervenido profesionales especialistas así como un grupo de usuarios que participaron en el periodo de prueba. Funciona en un teléfono móvil, tablets o cualquier dispositivo Wereable.

2. DERECHOS DE PROPIEDAD INTELECTUAL E INDUSTRIAL. Los derechos de propiedad intelectual e industrial sobre la APLICACIÓN son titularidad de eB2MC, correspondiéndole el ejercicio exclusivo de los derechos de explotación de los mismos en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación.

Los textos, imágenes, sonidos, animaciones, software y Software y el resto de contenidos incluidos en el Sitio Web, así como el propio Sitio Web, susceptibles de ser objeto de protección a través de la normativa de propiedad intelectual e industrial están sujetos a los derechos de propiedad intelectual e industrial y, son titularidad exclusiva de eB2MC o de las personas físicas o jurídicas autoras o licenciantes, en su caso y consecuentemente el Usuario declara conocer que no tiene ningún tipo de derecho sobre los mismos y que el hecho de visitar el sitio no le otorga ningún derecho en este sentido.

En relación al Software y por el periodo de vigencia del presente contrato eB2MC ofrece al Usuario una licencia de uso de carácter no exclusivo y no transferible. El usuario reconoce que la reproducción, modificación, distribución, comercialización,

[89] Este modelo de contrato está ideado en base al establecimiento de las condiciones de uso de la aplicación del teléfono móvil. En este caso EBB es el Responsable del tratamiento de datos, ya que eB2MC recoge los datos de los usuarios autónomamente y de manera directa , sin intermediarios. He obviado incluir los avisos de privacidad, políticas de cookies y demás cuestiones adicionales.

descompilación, desensamblado, utilización de técnicas de ingeniería inversa o de cualquier otro medio para obtener el código fuente, transformación o publicación de cualquier resultado de pruebas de referencias no autorizadas de cualquiera de los elementos y utilidades integradas dentro del desarrollo constituye una infracción de los derechos de propiedad intelectual de EBB, obligándose, en consecuencia, a no realizar ninguna de las acciones mencionadas.

3. POLITICA DE PRIVACIDAD. La APLICACIÓN utilizará Google Analytics como herramienta para conocer uso y las tendencias de interacción de la misma. eB2MC podrán utilizar la información de carácter personal que nos facilite de forma disociada (sin identificación personal) para fines internos, tales como la elaboración de estadísticas.

La APLICACIÓN podrá recabar, almacenar o acumular determinada información de carácter no personal referente a su uso. De conformidad con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril de 2016, se informa que los datos de carácter personal proporcionados mediante la aceptación de estos Términos y Condiciones, formarán parte de un fichero responsabilidad de eB2MC y que estos serán tratados con la finalidad descrita en el apartado "1. OBJETO" de este documento y serán conservados mientras dure la relación contractual objeto del uso de la APLICACIÓN, con el único objetivo de facilitar la introducción de mejoras en futuras versiones de la APLICACIÓN, también podrá realizarse el tratamiento de la información de las instalaciones, accesos de usuarios, datos demográficos, pantallas e interacción del usuario y bloqueos y excepciones.

Así mismo, se informa que podrá retirar el consentimiento en cualquier momento y ejercer los derechos de acceso, rectificación, supresión, portabilidad, limitación y oposición escribiendo un correo electrónico a eB2.DPDUc3m.es.

eB2MC se reserva la facultad de efectuar, en cualquier momento y sin necesidad de previo aviso, modificaciones y actualizaciones en la APLICACIÓN. Asimismo, también se reserva el derecho a modificar los presentes Términos y Condiciones con el objetivo de adaptarlos a las posibles novedades legislativas y cambios en la propia APLICACIÓN, así como a las que se puedan derivar de los códigos tipos existentes en la materia o por motivos estratégicos o corporativos.

4. EXCLUSIÓN DE RESPONSABILIDAD. EBB se reserva el derecho de editar,

actualizar, modificar, suspender, eliminar o finalizar los servicios ofrecidos por la Aplicación, incluyendo todo o parte de su contenido, sin necesidad de previo aviso, así como de modificar la forma o tipo de acceso a esta.

Las posibles causas de modificación pueden tener lugar, por motivos tales, como su adaptación a las posibles novedades legislativas y cambios en la propia Aplicación, así como a las que se puedan derivar de los códigos tipos existentes en la materia o por motivos estratégicos o corporativos. EBB no será responsable del uso de la APLICACIÓN por un menor de edad, siendo la descarga y uso de la APLICACIÓN de la exclusiva responsabilidad del usuario.

EBB no se hace responsable de la calidad final de la APLICACIÓN ni de que ésta sirva y cumpla con todos los objetivos de la misma. No obstante lo anterior, EBB se compromete en la medida de sus posibilidades a contribuir a mejorar la calidad de la APLICACIÓN , pero no puede garantizar la precisión ni la actualidad del contenido de la misma.

La responsabilidad de uso de la APLICACIÓN corresponde solo al usuario. Salvo lo establecido en estos Términos y Condiciones, EBB no es responsable de ninguna pérdida o daño que se produzca en relación con la descarga o el uso de la APLICACIÓN, tales como los producidos como consecuencia de fallos, averías o bloqueos en el funcionamiento de la APLICACIÓN (por ejemplo, y sin carácter limitativo: error en las líneas de comunicaciones, defectos en el software de la APLICACIÓN o fallos en la red de Internet).

Igualmente, EBB tampoco será responsable de los daños producidos como consecuencia de un uso indebido o inadecuado de la APLICACIÓN por parte de los usuarios.

5. JURISDCIÓN Y COMPETENCIA. Las partes renuncian expresamente al fuero de sus domicilios y se someten a la competencia de los Jueces y Tribunales de la ciudad de Madrid, así mismo, declaran expresamente que en todo lo no previsto en el presente contrato se rigen por lo dispuesto en el Código Civil en lo que fuera pertinente.