DATOS DE SALUD, DATOS ESPECIALMENTE PROTEGIDOS: EL CASO DE LOS DATOS BIOMÉTRICOS Y SU COMERCIALIZACIÓN*

Francisca Ramón Fernández

Catedrática de Derecho civil
Universitat Politècnica de València

SUMARIO

RESUMEN

La reciente noticia sobre el escaneo del iris a cambio de criptomonedas plantea un intenso debate sobre los datos de salud, los datos biométricos y su comercialización. El desconocimiento sobre las consecuencias que puede tener en el ámbito de la privacidad y la suplantación de identidad de una información única de la persona determina que se realicen transacciones comerciales con una falta de información al respecto. La inteligencia artificial puede ayudar al control del riesgo por lo que nos encontramos ante una oportunidad de futuro. La necesidad de protección de datos sensibles debe priorizarse en todo caso y evitar casos tan peligrosos como el analizado en el futuro.

PALABRAS CLAVE

Salud; datos, comercio; inteligencia artificial; protección.

ABSTRACT

The recent news about iris scanning in exchange for cryptocurrency raises an intense debate about health data, biometric data and their commercialization. Ignorance about the consequences that it can have in the field of privacy and identity theft of unique information of the person determines that commercial transactions are carried out with a lack of information in this regard. Artificial intelligence can help control risk, which is why we are faced with an opportunity for the future. The need to protect sensitive data must be prioritized in any case and avoid cases as dangerous as the one analyzed in the future.

KEYWORDS

Health; data, commerce; artificial intelligence; protection.

** Trabajo postulado al Premio Derecho y Salud 2024.*
*** Trabajo realizado en el marco del Grupo de Investigación de Excelencia Generalitat Valenciana "Algorithmical Law" (Proyecto Prometeu 2021/009, 2021-2024), y Proyecto "Derechos y garantías públicas frente a las decisiones automatizadas y el sesgo y discriminación algorítmicas" 2023-2025 (PID2022-136439OB-I00) financiado por MCIN/AEI/10.13039/501100011033/ FEDER, UE.*

I. INTRODUCCIÓN

La aparición en distintos medios de comunicación de una noticia en la que se pagaba una cantidad económica por la compra del iris hizo saltar la alarma en relación a la comercialización de datos personales, y en especial de datos especialmente sensibles

En la presente propuesta nos vamos a centrar en la mercantilización de los datos biométricos en relación con la noticia mencionada. Nuestro objetivo es analizar sobre dicha práctica y las consecuencias que puede tener en el ámbito jurídico especialmente en relación con la privacidad y la suplantación de identidad. Hay que tener en cuenta que muchas personas, desde el desconocimiento, y a cambio de una cantidad de moneda virtual les resulta atractivo escanear su iris sin pararse a pensar en las consecuencias.

Para estudiar en profundidad el tema que nos ocupa debemos hacer mención a los datos de salud, y también a la intrínseca relación que tiene con la inteligencia artificial y su regulación actual para, posteriormente ahondar en el comercio de los datos biométricos y la necesidad de una protección que dilucidaremos si la legislación aplicable otorga y es suficiente o es preciso establecer medidas coadyuvantes para ello[1].

Es cierto que en el ámbito de la salud y de la medicina las tecnologías de la información y comunicación están produciendo un cambio de gran calado en la forma de enfocar la asistencia médica al paciente. El tratamiento de los datos de salud es una realidad y avanzamos cada vez más rápidamente hacia la denominada medicina personalizada en atención a esos datos sensibles que nos proporcionan una información de gran interés para los avances en los tratamientos ajustados a las necesidades individuales de cada persona, a diseñar tratamientos cada vez más eficaces, a controlar los parámetros en la evolución de una enfermedad e incluso a asistir a los especialistas por medio de máquinas para perfeccionar y hacer más precisas las intervenciones quirúrgicas, o el diseño de fármacos más avanzados y efectivos, mediante la inteligencia artificial.

No siempre el derecho tiene respuesta para todas las cuestiones, y más aún cuando el continuo avance de la ciencia deriva en la utilización de inteligencia artificial para mejorar la salud, entre otros fines.[2] Aspectos como la responsabilidad por daños, la ética, la prestación del consentimiento y la vinculación con la investigación difícilmente encuentran un equilibrio en la normativa aplicable que se debate entre lo humano y lo ético, entre la investigación y el control.[3]

La metodología que vamos a utilizar es la habitual en los estudios de ámbito jurídico, y más en un tema especialmente reciente, donde los estudios doctrinales están en fase de desarrollo, y a pesar de ello nos centraremos en la principal doctrina especializada que se ha pronunciado sobre los datos de salud y su protección. Junto a ello, analizaremos con sumo detalle la normativa aplicable tanto a nivel comunitario como nacional, así como las propuestas legislativas existentes con la finalidad de arrojar un poco de luz en aspectos oscuros relacionados con los datos sensibles.

Con todo ello podremos obtener unas conclusiones, y también formular propuestas de *lege data* sobre algunos de los temas objeto de estudio para que puedan resultar de interés a la comunidad científica.

II. LOS DATOS DE SALUD: SU PROTECCIÓN A LA LUZ DE LA LEGISLACIÓN APLICABLE

1. Los datos de salud como datos especialmente protegidos

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[4] hace referencia a los datos relativos a la salud como datos personales[5] que se

1 La doctrina se plantea si debe acometerse cambios en el ámbito de los datos de salud: SALAZAR ROSADO, C. (2023): «Los desafíos del "datalake" sanitario: ¿cambio de paradigma en el control de los individuos sobre sus datos personales». *Comunicaciones en propiedad industrial y derecho de la competencia,* (100), págs. 43 y sigs.

2 COBAS COBIELLA, Mª. E. y PÉREZ COBAS. A. E. (2023): «Medicina personalizada. Retos para el derecho». En C. Gil Membrado (Dir.), *Derecho y medicina: desafíos tecnológicos y científicos*, Dykinson, págs. 129 y sigs.

3 RAMÓN FERNÁNDEZ, F. (2022c): «Nuevos retos de la inteligencia artificial: ética y responsabilidad», En L. Martínez Velencoso y M. Sancho López (Dir.), *Protección jurídica de la privacidad. Inteligencia Artificial, Salud y Contratación*, Thomson Reuters Aranzadi, págs. 123 y sigs.

4 Diario Oficial de la Unión Europea L 119/1, de 4 de mayo de 2016.

5 El artículo 4 del Reglamento (UE) 2016/679, define los datos personales como «toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular

refieren a la salud física o mental de una persona física, y se incluye dentro de dicho concepto la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

Todo ello de conformidad con lo que indica la Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza[6] todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de la fuente que se haya obtenido, ya sea un facultativo, profesional sanitario, un establecimiento hospitalario, un dispositivo médico, o una prueba diagnóstica que se haya realizado in vitro.

Uno de los principales problemas que nos encontramos es que estos datos especialmente sensibles como son los datos de salud deben adoptarse las medidas adecuadas para su privacidad y evitar sesgos discriminatorios en los sujetos.[7] También es objeto de preocupación que exista una transparencia y un control de los datos en el ámbito de la sanidad digital para su protección.[8]

El tratamiento de los datos personales debe realizarse con el consentimiento de la persona interesada, pero también es posible ese tratamiento sin el consentimiento en los supuestos de razones de interés público en el ámbito de la salud pública. Es por ello, que debe ordenarse siempre bajo la protección de los derechos y libertades de las personas físicas, y hay que determinar de forma precisa qué se entiende por una situación de salud pública. Por poner un ejemplo, podemos hacer referencia a la pandemia por la Covid-19 en la que se planteó si la disposición de datos sensibles por parte de aplicaciones era conforme o no a dicha situación excepcional.[9]

El Reglamento (CE) núm. 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo[10] dicho contexto debe ser entendido en relación al estado de salud, incluyendo la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, también los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad.

El tratamiento de los datos de salud por razón de interés público no incluye que terceros puedan tratar los datos personales con otra finalidad. Se refiere con terceros a las empresas, compañías de seguro o entidades bancarias, por ejemplo.

La Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales[11], categoriza como especiales los datos en el artículo 9, y se refiere al artículo 9.2, a) del Reglamento (UE) 2016/579 al establecer que para evitar situaciones que produzcan una discriminación, el mero consentimiento de la persona afectada no será suficiente para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Los tratamientos de datos a los que se refiere el artículo 9.2, en las letra g) que se refiere al tratamiento necesario por razones de un interés público

mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

6 Diario Oficial de la Unión Europea L 88/45, de 4 de abril de 2011.

7 Véase: RAMÓN FERNÁNDEZ, F. (2022a): «Inteligencia artificial y protección de la salud: La necesidad de establecer unos límites en la carta de derechos digitales». En M. J. Blanco Sánchez (Coord.), A. Madrid Parra y L. Alvarado Herrera (Dir.), *Derecho digital y nuevas tecnologías*, Aranzadi, págs. 1027 y sigs.

8 VIVAS TESÓN, I. (2023): «Transparencia, protección y control de los datos de salud en la sanidad digital». En Mª. É. Cobas Cobiella y R. Guillén Catalán (Dir.), *Equidad y transparencia en la prestación de servicios*, Dykinson, págs. 223 y sigs. Véase también: PLAZA PENADÉS, J. (2022): «Cuestiones actuales de la inteligencia artificial y el BIG DATA». En L. Martínez Velencoso y M. Sancho López (Dir.), *Protección jurídica de la privacidad. Inteligencia Artificial, Salud y Contratación*, Thomson Reuters Aranzadi, págs. 45 y sigs.; (2023): «Cuestiones básicas del derecho de protección de datos de carácter personal y su seguridad». *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 63.

9 Así, RAMÓN FERNÁNDEZ, F. (2020a): «El derecho a la vida y a la protección de la salud en las medidas adoptadas en España como consecuencia de la covid-19. Una reflexión sobre su oportunidad». *Estudios Constitucionales*, volumen 18 (2), págs. 51 y sigs. Disponible en la URL: http://www.estudiosconstitucionales.cl/index.php/econstitucionales/article/view/701/420 [Con acceso el 10.4.2024]. Véase también: DE LECUONA RAMÍREZ, I. (2020). "Aspectos ético, legales y sociales del uso de la inteligencia artificial y el Big Data en salud en un contexto de pandemia". *Revista internacional de pensamiento político*, (15), págs. 139 y sigs. Disponible en la URL: https://www.upo.es/revistas/index.php/ripp/article/view/5599 [Con acceso el 13.4.2024].

10 Diario Oficial L 354, de 31 de diciembre de 2008.

11 BOE núm. 294, de 6 de diciembre de 2018.

esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado; letra h) se centra en el caso de que el tratamiento de los datos es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías que se indican en el artículo 9.3, y letra i) que trata sobre el tratamiento que es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional, deberán estar amparados el tratamiento en una norma con rango de ley, que podrá establecer requisitos adicionales referentes a la seguridad y confidencialidad.

Dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

La disposición adicional decimoséptima de la Ley Orgánica 3/2018 se refiere al tratamiento de los datos de salud y se remite a lo que hemos indicado del artículo 9.2, letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 en los que se ampara el tratamiento de los mismos y también de datos genéticos que se regulan en un listado de normas que precisa el precepto. Estás normas son: Ley 14/1986, de 25 de abril, General de Sanidad[12]; Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales[13]; 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[14]; Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud[15]; Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias[16]; Ley 14/2007, de 3 de julio, de Investigación biomédica[17]; Ley 33/2011, de 4 de octubre, General de Salud Pública[18]; Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras[19]; Real Decreto Legislativo 1/2015, de 24 de julio, que aprueba el texto refundido de la Ley general de derechos de las personas con discapacidad y de su inclusión social.

El tratamiento de estos datos en la investigación en salud sigue una serie de criterios señalados por la norma que pasamos a indicar a continuación:

La persona interesada o su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. La finalidad podrá abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

Se permite en situaciones de excepcional relevancia y gravedad para la salud pública que las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud puedan llevar a cabo estudios científicos sin el consentimiento de los afectados.

Se considera que es lícito y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, en el caso de obtenerse el consentimiento para una finalidad concreta, se utilicen para finalidades o áreas de investigación que estén relacionadas con el área en la que se integrase científicamente el estudio inicial.

En estos casos, los responsables deberán publicar la información que se indica en el artículo 13 del Reglamento (UE) 2016/679, que se refiere a la Información que deberá facilitarse cuando los datos personales se obtengan del interesado en un lugar accesible de la web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de dicha información por medios electrónicos a las personas interesadas. Se requerirá el informe favorable del comité de ética de la investigación.

Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud, y en particular, biomédica.

12 BOE núm. 102, de 29 de abril de 1986.

13 BOE núm. 269, de 10 de noviembre de 1995.

14 BOE núm. 274, de 15 de noviembre de 2002.

15 BOE núm. 128, de 29 de mayo de 2003.

16 BOE núm. 280, de 22 de noviembre de 2003.

17 BOE núm. 159, de 04 de julio de 2007.

18 BOE núm. 240, de 05 de octubre de 2011.

19 BOE núm. 168, de 15 de julio de 2015.

El uso de estos datos requerirá una serie de requisitos: que exista una separación técnica y funcional entre el equipo de investigación y las personas que realicen la seudonimización y conserven la información que posibilite la reidentificación, y que los datos sudonimizados únicamente sean accesibles al equipo de investigación en unos supuestos muy específicos: por un lado, exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación; y por otro, que se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Se podrá proceder a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de ellas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

Cuando se traten de datos personales con finalidad de investigación en salud, y particularmente en el ámbito de la biomedicina, a los efectos de lo indicado en el artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15 (derecho de acceso de los interesados), 16 (derecho de rectificación), 18 (derecho a la limitación del tratamiento) y 21 (derecho de oposición) del Reglamento (UE) 2016/679 en estos casos:

- Los indicados derechos se ejerzan directamente ante los investigadores o centro de investigación que utilicen datos anonimizados o seudonimizados.

- El ejercicio de dichos derechos se refiera a los resultados de la investigación.

- La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

En los casos en que conforme a lo indicado en el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, particularmente, en la biomedicina, se procederá a realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los casos indicados en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos; someter la investigación científica a las directrices internacionales sobre buena práctica clínica; adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados, y designar un representante legal establecido en la Unión Europea, de acuerdo con lo indicado en el artículo 74 del Reglamento (UE) núm. 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE[20], si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

El uso de datos personales seudonimizados con fines de investigación en salud pública, y en particular, en la biomedicina deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679, que establece que el delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39 del Reglamento (UE) 2016/679.

En el plazo máximo de un año desde la entrada en vigor del Reglamento (UE) 2016/679, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos, o en su defecto, un experto con conocimiento suficientes de esta norma cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Según la disposición transitoria sexta de la Ley Orgánica 3/2018 referente a la reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de la misma, se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada

20 Diario Oficial de la Unión Europea núm. 158, de 27 de mayo de 2014.

en vigor de la norma siempre que concurra alguna de estas circunstancias: que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento, y que habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

La Ley 3/2028, en su disposición final quinta, modifica la Ley 14/1986 en la que se añade un nuevo capítulo II sobre el tratamiento de datos de la investigación en salud en el que se indica que se regirá por lo indicado en la disposición adicional decimoséptima de la Ley Orgánica 3/2018 (artículo 105 bis).

También la disposición final novena de la Ley Orgánica 3/2018 modifica la Ley 41/2022, en su artículo 16.3. En la nueva redacción se indica que el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia se rige por lo dispuesto en la normativa vigente en protección de datos personales, y en la Ley 14/1986, y demás normas que sean aplicables.

El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico asistencial, de forma que, como regla general, quede asegurado el anonimato, excepto que el paciente haya prestado su consentimiento para no separarlos.

Se exceptúan los casos de investigación que contempla la disposición adicional decimoséptima, apartado 2, de la Ley Orgánica 3/2018.

También se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.

Interesa en este punto destacar la Estrategia Europea de Datos[21] en la que el acceso de datos en este caso de salud y la capacidad para utilizarlos forman parte de un futuro para la innovación y el crecimiento en el ámbito de la medicina personalizada[22].

La pretensión es la circulación de datos por todo el espacio de la Unión, para beneficiar a todos, con respeto a las normas de privacidad y protección, y establecer las normas para el acceso a los datos y que su utilización sea justa, práctica y clara.

Así, podemos mencionar el Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, sobre la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Ley de Gobernanza de Datos) (Texto pertinente a efectos del EEE)[23], y el Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos)[24].

Por último podemos mencionar 121/000110 Proyecto de Ley por la que se modifican diversas normas para consolidar la equidad, universalidad y cohesión del Sistema Nacional de Salud[25], aunque actualmente caducado debido al calendario político con el adelanto de las elecciones generales, el apartado 3 de la Disposición Adicional segunda de dicho Proyecto establecía criterios para aplicar al tratamiento de los datos. Se incluían los datos biométricos, personales socioeconómicos y laborales, por lo que se atendía a otros factores que puedan tener incidencia en la salud de la persona.

21 COMISIÓN EUROPEA (2020): *Estrategia Europea de Datos*. Disponible en la URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es [Con acceso el 18.4.2024].

22 ANDREU MARTÍNEZ, B. (2023): «Datos de salud y bien común: hacia la construcción de un mercado europeo de datos sanitarios». En B. Andreu Martínez y A. Espinosa de los Monteros Rodríguez (Coord.), *Tecnología para la salud: una visión humanista desde el biodererecho*, Plaza y Valdés, págs. 209 y sigs.

23 Diario Oficial de la Unión Europea, L 152/1, de 3 de junio de 2022.

24 Diario Oficial Unión Europea, núm. 2854, de 22 de diciembre de 2023.

25 BOGG. Serie A. Proyectos de Ley, núm. 110-1, de 24 de junio de 2022. Mencionado por ANDREU MARTÍNEZ, B. (2023): «La necesaria actualización de la Ley de Autonomía del Paciente frente a los retos en la gestión de los datos de salud». En B. Andreu Martínez (Coord.), *Los datos de salud como eje de la transformación digital de la Sanidad*. Comares, págs. 139 y sigs. Disponible en la URL: https://accesoabiertocomares.com/index.php/coa/catalog/book/51 [Con acceso el 25.4.2024].

2. Datos de salud e inteligencia artificial: un binomio a proteger

La regulación que hemos analizado en los puntos anteriores respecto a los datos de salud y su protección tanto en el Reglamento (UE) 2016/679 como en la Ley Orgánica 3/2018 no se puede desligar de la futura regulación relativa a la inteligencia artificial.

Se afirma por parte de la doctrina[26] que la conexión entre ambas normas es que el Reglamento Europeo de Inteligencia Artificial regula la comercialización y puesta en servicio de la inteligencia artificial, y el Reglamento (UE) 2016/679 el uso de los datos y de una inteligencia artificial para su entrenamiento, perfilación de personas y toma de decisiones automatizadas como se indica en el artículo 22 del citado texto, y que veremos en un punto siguiente de la exposición.

Por su parte la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios, de 3 de mayo de 2022, COM(2022) 197 final[27] indica dicha relación con los sistemas de inteligencia artificial de alto riesgo, ya que deberán de estar certificados de acuerdo con lo indicado en el Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) n.º 178/2002 y el Reglamento (CE) n.º 1223/2009 y por el que se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo[28], y los requisitos esenciales de interoperabilidad solamente deben aplicarse en la medida en que el fabricante de un producto sanitario o de un sistema de inteligencia artificial de alto riesgo facilite datos sanitarios electrónicos que vayan a ser tratados como parte del sistema de historiales médicos electrónicos (HME) alegue interoperabilidad con dicho sistema. En este caso, las disposiciones sobre especificaciones comunes para estos sistemas HME deben ser aplicables a dichos productos sanitarios y sistemas de inteligencia artificial de alto riesgo.

III. LOS DATOS BIOMÉTRICOS COMO DATOS SENSIBLES: ASPECTOS JURÍDICOS RESPECTO A SU COMERCIALIZACIÓN

1. Los datos biométricos: concepto y características

El Reglamento (UE) 2016/679 diferencia entre datos genéticos, datos biométricos y datos de salud. Todos ellos son datos personales, pero tienen alguna diferenciación que resulta de interés.

Los datos genéticos son datos personales que se refieren a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona y que se han obtenido en particular del análisis de una muestra biológica de dicha persona.

Los datos biométricos son datos personales que se obtienen a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos

Los datos relativos a la salud son datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

El Real Decreto 311/2022, de 3 de mayo, por el

26 Sigo la exposición de TODOLÍ, A. (2024): «Reglamento europeo de IA y su coordinación con el Reglamento de protección de datos (Iniciativa interblogs)». *Argumentos en Derecho Laboral*. Disponible en la URL: https://adriantodoli.com/2024/04/18/reglamento-europeo-de-ia-y-su-coordinacion-con-el-reglamento-de-proteccion-de-datos-iniciativa-interblogs/ [Con acceso el 18.4.2024]. Véase también: RAMÓN FERNÁNDEZ, F. (2020b): «La sanidad móvil: la protección de datos referentes a la salud y la genética». En F. Ramón Fernández, (Coord.), *Marco Jurídico de la Ciencia de Datos*, Tirant lo Blanch, págs. 197 y sigs.; (2022b): «Protección de datos de salud en el ámbito laboral: una perspectiva española». En *Estudos sobre LGPD – Lei geral de proteção de dados. Doutrina e aplicabilidade no* âmbito *laboral*, Editorial Diadorim, págs. 99 y sigs.

27 Disponible en la URL: https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0005.02/DOC_1&format=PDF [Con acceso el 17.4.2024]. Véase: MORTE FERRER, R. (2023): «Crítica de la Conferencia de Autoridades de Protección de Datos Alemana a la Propuesta de Reglamento para la regulación del Espacio Europeo de Datos de Salud». *La Ley privacidad* (16); CASANOVA ASENCIO, A. S. (2023): «Espacio Europeo de datos sanitarios, uso primario y autonomía del paciente». En B. Andreu Martínez (Coord.), *Los datos de salud como eje de la transformación digital de la Sanidad*. Comares, págs. 107 y sigs. Disponible en la URL: https://accesoabiertocomares.com/index.php/coa/catalog/book/51 [Con acceso el 14.4.2024]; DE MIGUEL BERIAIN, I. (2023): «El uso de datos de salud para investigación biomédica a la luz de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios». *Revista jurídica de Castilla y León*, (60), págs. 7 y sigs. Disponible en la URL: https://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1131978346397/Publicacion/1285279043799/Redaccion [Con acceso el 11.4.2024].

28 Diario Oficial de la Unión Europea L 117 de 5 de mayo de 2017.

que se regula el Esquema Nacional de Seguridad[29] define la biometría como factor de autenticación al reconocimiento de los individuos en base a sus características biológicas o de comportamiento.

La referencia a datos biométricos se indica también en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[30], modificada por la Ley Orgánica 3/2018. Se modifica el artículo 15, apartado 1, y se establece que si la información incluye datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos, el acceso solamente se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.

También encontramos referencias a pruebas biométricas[31] en la ya mencionada Ley 41/2002, en su artículo 17, respecto a la conservación de la documentación clínica. Los datos de la historia clínica que se relacionen con el nacimiento del paciente, incluidos los resultados de pruebas biométricas que resulten necesarias para determinar el vínculo de filiación con la madre, no se destruirán, trasladándose una vez conocido el fallecimiento del paciente, a los archivos definitivos de la Administración, donde se conservarán con las medidas de seguridad a efectos de la normativa de protección de datos. Los datos de la historia clínica relacionados con las pruebas biométricas anteriormente indicados, solamente se podrán comunicar a petición judicial, dentro del correspondiente proceso penal o en caso de reclamación o impugnación judicial de la filiación materna.

La Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[32], en su artículo 5, define los datos biométricos como datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos. Reproduce la definición contenida en el artículo 4 del Reglamento (UE) 2016/679.

La Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM(2021)0206 – C9-0146/2021 –2021/0106(COD))[33] hacía referencia a qué se consideraba como identificación biométrica, considerando como tal el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos. Lo diferencia de la verificación biométrica entendida como la verificación automatizadas y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente.

Hay que tener en cuenta que después de la elaboración de este trabajo se ha aprobado el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial),[34] por lo que se entenderán las referencias indicadas al mismo.

El concepto de datos biométricos que se indicaba en la Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024 se interpretará según lo indicado en el artículo 4, punto 14, del Reglamento (UE) 2016/679, del artículo 3, punto 18, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) núm. 45/2001 y la Decisión núm. 1247/2002/CE[35], y en el artículo 3, punto 13, de la

29 BOE núm. 106, de 04 de mayo de 2022.

30 BOE núm. 295, de 10 de diciembre de 2013.

31 Véase: GÓMEZ PIQUERAS, C. (2009): «Disociación/anonimización de los datos de salud». *Revista Derecho y Salud*, volumen 18 (1), págs. 43 y sigs. Disponible en la URL: https://www.ajs.es/sites/default/files/2020-05/DyS-Vol18-01-estudio_03.pdf [Con acceso el 10.4.2024]; GONZÁLEZ REVUELTA, Mª. E. (2023): *Evolución de la historia clínica digital, retos y dificultades: Avances y desafíos en la seguridad de la historia clínica y el acceso a los datos de salud.* Almería. Universidad de Almería, págs. 95 y sigs. Disponible en la URL: https://repositorio.ual.es/bitstream/handle/10835/14572/01.Tesis.pdf?sequence=1&isAllowed=y [Con acceso el 12.4.2024].

32 BOE núm. 126, de 27 de mayo de 2021.

33 Disponible en la URL: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf [Con acceso el 17.4.2024].

34 Diario Oficial de la Unión Europea núm. 1689, de 12 de julio de 2024.

35 Diario Oficial de la Unión Europea, núm. 295, de 21 de noviembre de 2018.

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.[36]

Dentro del concepto de identificación biométrica se considera el reconocimiento automatizado de características humanas de tipo físico, fisiológico o conductual, como la cara, el movimiento ocular, la forma corporal, la presión arterial, el olor, o las características de las pulsaciones de tecla, con la finalidad de identificar a una persona comparando sus datos biométricos con los datos biométricos de otras personas almacenados en una base de datos independientemente de que haya o no una prestación del consentimiento.

La categorización biométrica es la inclusión de personas físicas en categorías específicas en función de los datos biométricos de cada una de ellas. Estas categorías específicas se pueden referir al color de los ojos, por ejemplo, entre otros aspectos como podría ser el sexo, la edad, el color del pelo, los tatuajes, rasgos conductuales o de la personalidad, lengua, religión, la pertenencia a una minoría nacional o la orientación sexual o política.

No se incluyen los sistemas de categorización biométrica que sean una característica meramente accesoria intrínsecamente vinculada a otro servicio comercial, por lo que la característica no puede utilizar, por razones técnicas objetivas, sin el servicio principal, y que la integración de dicha característica o funcionalidad no es un medio para eludir la aplicabilidad de las normas. Por ejemplo, los filtros que clasifican las características faciales o corporales utilizados en los mercados en línea podrían constituir una característica accesoria de este tipo, ya que solamente se pueden utilizar en relación con el servicio principal, que consiste en vender un producto permitiendo al consumidor una previsualización de cómo le quedaría y ayudarlo en su decisión de compra.

También los filtros que se usan en redes sociales que clasifican las características faciales o corporales con la finalidad de que el usuario pueda añadir o modificar imágenes o vídeos, también se podrían considerar una característica accesoria, ya que no se utilizan separadamente de las redes sociales y de compartir contenidos en línea.

La exclusión de los sistemas de inteligencia artificial destinados a la verificación biométrica que comprenden la autenticación, cuyo único propósito es confirmar que una persona física concreta es la persona que dice ser, o también la identificación que tiene como finalidad acceder a un servicio o desbloquear un dispositivo se justifica porque tales sistemas tengan una repercusión menor en los derechos fundamentales, que los demás sistemas de identificación biométrica remota que se puedan utilizar para el tratamiento de los datos biométricos de un gran número de personas sin su participación activa.

Como sigue precisando La Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, los sistemas en tiempo real implican el uso de materiales en directo como grabaciones de vídeo, generados por una cámara u otro dispositivo con una función similar, mientras que los sistemas en diferido recaban datos biométricos y la comparación e identificación se produce con una demora, y se utilizan materiales como imágenes o grabaciones de vídeos que captan cámaras de televisión con circuito cerrado o dispositivos privados, generados con anterioridad a la utilización del sistema en relación con las personas físicas.

Se deben prohibir los sistemas de categorización biométrica basados en datos biométricos de las personas físicas, como es la cara o las impresiones dactilares de una persona física, para deducir o inferir las opiniones políticas, la afiliación sindical, las convicciones religiosas o filosóficas, la raza, la vida sexual o la orientación sexual de una persona física. Esta prohibición no se debe aplicar al etiquetado, filtrado ni a la categorización lícitos de conjuntos de datos biométricos adquiridos de conformidad con el Derecho nacional o de la Unión en función de datos biométricos, como la clasificación de imágenes en función del color del pelo o del color de ojos, que se pueden utilizar en el ámbito de aplicación de la futura norma.

El tratamiento de datos biométricos y de datos personales de otra índole asociado al uso de sistemas de inteligencia artificial para la identificación biométrica, excepto el asociado al uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de aplicación de la norma debe seguir cumpliendo los requisitos derivados del artículo 10 de la Directiva (UE) 2016/680, el artículo 9, apartado 1, del Reglamento (UE) 2016/579, y el artículo 10, apartado 1, del Reglamento (UE) 2018/1725 prohíben el tratamiento de datos biométricos con fines distintos de la aplicación de la ley, con las excepciones limitadas que se contemplan en dichos preceptos. En la aplicación del artículo 9, apartado 1, del Reglamento (UE) 2016/679, el uso de la

36 Diario Oficial de la Unión Europea L 119/89, de 4 de mayo de 2016.

identificación biométrica remota para fines distintos de la aplicación de la ley ya ha sido objeto de decisiones de prohibición por parte de las autoridades nacionales de protección de datos.

La doctrina[36] se ha pronunciado sobre una futura regulación específica de condiciones adicionales para el tratamiento de datos genéticos, biométricos o de salud, que nos lleva a afirmar que estamos ante una nueva categoría de datos, cuya protección se refuerce con unas garantías específicas, con la finalidad de establecer y equilibrar la protección subjetiva de la persona, su privacidad y el avance tecnológico.

2. La sensibilidad de los datos biométricos como datos de salud. Aplicación de la inteligencia artificial

Los datos de salud como datos personales y datos que por su naturaleza son particularmente sensibles ya que están íntimamente relacionados con los derechos y libertades fundamentales de los sujetos, ya que un tratamiento no adecuado de los mismos afectaría a esos derechos y libertades fundamentales ya ha sido puesto de manifiesto no solamente en el ámbito legislativo, sino también en el doctrinal.[38]

El artículo 9 del Reglamento (UE) 2016/679, en sus apartados 1 y 4 establece la protección de los datos personales particularmente sensibles en relación con los derechos y las libertades fundamentales, por el tratamiento que se podría derivar un riesgos para los mismos. Se prohíbe el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física, los datos relativos a la salud, y los datos genéticos, entre otros. Por parte de los Estados miembros se podrán mantener o introducir condiciones adicionales, incluidas limitaciones, en relación al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. Sin embargo, estas limitaciones no pueden suponer un obstáculo para la libre circulación de datos personales dentro de la Unión Europea cuando estas condiciones se apliquen al tratamiento transfronterizo de esos datos.

En cuanto a los datos de salud, se indica que el tratamiento de categorías especiales de datos personales referentes a la salud, en relación con necesidades específicas, deben establecerse condiciones armonizadas y especialmente si el tratamiento de esos datos lo realizan personas que están obligadas al secreto profesional.

Se precisa una evaluación del impacto en relación a la protección de los datos que entrañan un alto riesgo para los derechos y libertades de los sujetos. Ello se tendrá en cuenta cuando se utilicen dispositivos optoelectrónicos o cuando el tratamiento entrañe ese alto riesgo para los sujetos.

Según indica la Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, a la que hemos hecho referencia anteriormente, los datos biométricos son una categoría especial de datos personales sensibles, y se pueden clasificar como de alto riesgo varios casos de uso críticos de sistemas biométricos, en la medida que se permita su utilización. Véase lo indicado en el Reglamento (UE) 2024/1689.

Las imprecisiones técnicas de los sistemas de inteligencia artificial destinados a la identificación biométrica remota de las personas físicas pueden dar lugar a resultados sesgados y producir un efecto discriminatorio.

Por tanto, de lo expuesto vemos que la inteligencia artificial en los datos de salud, y especialmente en los datos biométricos puede producir un efecto discriminatorio y especialmente en el caso de los sistemas de identificación biométrica remota se deben clasificar como de alto riesgo precisamente por el riesgo que entrañan para los derechos y libertades fundamentales de los sujetos.

Se excluirían los sistemas de inteligencia artificial que están destinados a la verificación biométrica para la autenticación cuya finalidad única es la confirmación de la identidad de una persona, y su confirmación respecto a quien dice es. Esto sería el caso para desbloquear un dispositivo, acceder a un espacio. Sin embargo, si el sistema de inteligencia artificial que utiliza datos biométricos para categorización biométrica sí que se deben calificar como de alto riesgo ya que se está refiriendo a atributos o características sensibles del sujeto que están protegidas por el artículo 9, apartado 1 del Reglamento (UE) 2016/679 sobre la base de datos biométricos,

37 GUILLÉN CATALÁN, R. (2020): «Sujetos responsables por vulneración de las normas de protección de datos. Especial referencia a los datos relativos a la salud». *Revista Boliviana de Derecho,* (30), pág. 71. Disponible en la URL: https://dialnet.unirioja.es/descarga/articulo/7521500.pdf [Con acceso el 12.4.2024]. Cfr. JAREÑO BUTRÓN, M. y ARRATIBEL ARRONDO, J. A. (2023): «Técnicas para el control del tratamiento masivo de datos personales en el sector público sanitario». *Auditoría pública: revista de los Órganos Autónomos de Control Externo,* (81), págs. 180 y sigs. Disponible en la URL: https://asocex.es/wp-content/uploads/2023/05/Articulo-13.pdf [Con acceso el 12.4.2024]; LATORRE LUNA, L. (2022): «El valor de los datos sanitarios de las Administraciones públicas: ¿Los futuros bienes de dominio público?». *Revista catalana de dret públic*, (65), págs. 46 y sigs. Disponible en la URL: http://revistes.eapc.gencat.cat/index.php/rcdp/article/view/10.2436-rcdp.i65.2022.3834 [Con acceso el 11.4.2024].

38 ABAD AMORÓS, Mª. R. (2003): «El carácter sensible de los datos biométricos». *Datospersonales. org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, págs. 1 y sigs.

en la medida en que no estén prohibidos por la regulación en el ámbito de la inteligencia artificial, así como los sistemas de reconocimientos de emociones que tampoco estén prohibidos.

Se consideran que los sistemas biométricos que están destinados a ser utilizados solamente a efectos de posibilitar la ciberseguridad y las medidas de protección de los datos personales no se consideran como sistemas de alto riesgo.

El tratamiento de datos biométricos que se realice dentro del marco de un sistema de inteligencia artificial para la identificación biométrica debe cumplir lo que se indica en el artículo 10 de la Directiva (UE) 2016/680. Se permite dicho tratamiento en los casos que sean estrictamente necesarios, salvaguardando los derechos y libertades del sujeto, y cuando se autorice por parte del Derecho de la Unión o de los Estados miembros.

Dicho uso, cuando se autorice, deberá respetar lo indicado en el artículo 4, apartado 1, de la Directiva (UE) 2016/680 que dispone respecto al tratamiento de los datos personales que sean tratados de manera lícita y legal, se hayan recogido con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines, sean adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados, sean exactos, y, si fuera necesario, actualizados. Se habrán de adoptar todas las medidas razonables para que se suprimen o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados. Los datos deberán ser conservados de forma que permita identificar al interesado durante un período no superior al necesario para los fines para los que son tratados, y los datos se tratarán de tal forma que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas.

3. El caso de la comercialización del iris como dato biométrico y la necesidad de protección

Si tomamos como ejemplo la película "I Origins" dirigida por Mike Cahill, en 2014, en el que se muestra el acceso completo a la base de datos de escaneo del iris y la reciente noticia sobre el escaneo del iris a cambio de criptomonedas, vemos cómo la realidad ya supera a la ficción.

Las cuestiones que se pueden plantear en el ámbito jurídico radican en que según Reglamento (UE) 2024/1689 respecto del concepto de datos biométricos. Estos pueden permitir la autenticación, identificación o categorización de las personas físicas y el reconocimiento. Junto a ello también hay que atender a lo indicado en el Reglamento (UE) 2023/2854 del Parlamento Europeo y del Consejo, de 13 de diciembre de 2023, sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos)[39].

El concepto de identificación biométrica que indica la Resolución de 2024 es el reconocimiento automatizado de características humanas físicas, fisiológicas o conductuales, entre las que se incluye el movimiento ocular con la finalidad de determinar la identidad de una persona comparando sus datos biométricos con los almacenados en una base de datos de referencia, independientemente de que haya o no prestado su consentimiento. Se diferencia del concepto de categorización biométrica que es la inclusión en categorías en función de sus datos biométricos, y se puede referir al color de los ojos, entre otros aspectos.

Las consecuencias del escaneado del iris radica también en el desconocimiento de lo que realmente se realiza, y la contraprestación que la persona obtiene a cambio de dicho escaneado. Los datos obtenidos del registro del iris que es único e intransferible y que son datos sensibles, y que se desconoce qué uso se va a realizar de esos datos obtenidos del escaneo del ojo. Llama la atención que en los medios de comunicación se realicen afirmaciones del tipo que no se obtienen datos biométricos delicados, que solamente se toman unas medidas de ojo para la creación de un código encriptado para navegar por internet de forma anónima, y que la finalidad es saber si se trata de una persona real o un bot.

Incluso consideramos ir más allá en relación con la elaboración de perfiles utilizando los datos del iris y las decisiones individuales automatizadas donde se aplica la inteligencia artificial, y al que se refiere el artículo 22 del Reglamento (UE) 2016/679. Este precepto indica que todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizada, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Se exceptúa el caso de la prestación de consentimiento explícito del interesado, pero en este caso el responsable del tratamiento deberá adoptar las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesados, como

39 Diario Oficial Unión Europea, núm. 2854, de 22 de diciembre de 2023.

el derecho a obtener intervención humana por parte del responsable, expresar su punto de vista e impugnar la decisión.

Pero lo más importante es que las decisiones no se basarán en las categorías especiales de datos que se indican en el artículo 9.1 (recordemos que se incluyen los datos de salud y datos genéticos), salvo que se aplique el artículo 9.2, letra a) o g) y se hayan adoptado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

El iris contiene datos genéticos (color, morfología, etc.) y también datos de salud (determinadas enfermedades tienen una característica que se puede apreciar en el iris, como por ejemplo la enfermedad de Wilson, con los anillos de color dorado o anillo de Kayser-Fleischer, el anillo de sodio, entre otras patologías que se podrían mencionar)[40].

La Declaración Internacional de Datos Genéticos Humanos de la UNESCO del año 2003, ya ofreció una definición como la información sobre las características hereditarias de los científicos, mientras que la Recomendación R (97) 5 del Consejo de Europa por su parte los define como : "todos los datos, con independencia de su tipo, que se refieren a las características hereditarias de una persona o al modelo de herencia de estas características de un grupo de personas de la misma familia", reflejados además en la Ley 14/2007, sobre Investigación Biomédica en su art. 3j).

4. La postura de la Agencia Española de Protección de Datos

Ante dicha situación, la Agencia Española de Protección de Datos, en el Acuerdo de adopción de medida provisional correspondiente al EXP202312448[41], en 2024, ha hecho uso de lo indicado en el artículo 66.1 del Reglamento (UE) 2016/679 respecto de la asistencia mutua adoptó medidas para asegurar una efectiva cooperación por lo que se ha suprimido la venta como medida cautelar para la protección de los derechos y libertades personales. La adopción de esta medida tendrá un periodo de validez no superior a los tres meses.

De esta forma, la Agencia mencionada ha señalado que el procesado de datos biométricos a través de la captura inicial de imágenes de los iris, ojos y rostro de miles de personas desde múltiples puntos de la geografía española, y haciendo uso de un dispositivo especial, denominado ORB, es capaz de almacenar esta información y generar patrones biométricos, afectando la práctica a diversas personas, incluidos menores de edad, sin constar acreditado el consentimiento y la información proporcionada acerca de dicho tratamiento.

El escaneo del iris, como hemos indicado, se procedía a cambio del pago de una cantidad económica mediante criptomonedas que se ingresaba en el "wallet" que estaba vinculado a una aplicación de móvil.

Según manifestaba la empresa, la finalidad no era otra que facilitar a las personas lo que ellos llamaban identidad digital para contrarrestar la condición de avatares de inteligencia artificial, y para su funcionamiento se precisaba la instalación de la aplicación móvil, el registro como usuario, y la recepción de un código QR.

Después, se verificaba la prueba de personalidad mediante la captura del iris mediante ORB y la aplicación se transforma en un pasaporte, que a su vez es también un monedero de una criptodivisa.

La denuncia a la Agencia también tenía como fundamento que se captaban datos de personas menores de edad, que no se les proporcionaba suficiente información, y que no resultaba claro que se captaban datos biométricos.

De igual modo, se denunciaba que no se facilitaba, a petición de los interesados, el formulario que habían rellenado prestando el consentimiento, y que no se permitía la retirada del mismo remitiendo al interesado al borrado de la aplicación. También la falta de funcionamiento de un supuesto procedimiento de supresión mediante un procedimiento en internet, en tanto que requiere que la empresa envíe un código por correo que se demora, de tal forma que cuando está en disposición del usuario ya no es válido.

Las Directrices 05/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de aplicación de la ley, Versión 2.0[42] «El tratamiento de datos biométricos en cualquier circunstancia constituye una interferencia grave en sí mismo».

40 Como señalan PÉREZ COBAS, A. E. y COBAS COBIELLA, Mª. E. (2020): «Datos genéticos y datos de salud. Una aproximación a su estudio». *Revista Boliviana de Derecho,* (30), págs. 440 y sigs. Disponible en la URL: https://dialnet.unirioja.es/descarga/articulo/7521512.pdf [Con acceso el 10.4.2024].

41 Disponible en la URL: https://www.aepd.es/documento/co-000297-2023-medida-provisional.pdf [Con acceso el 24.4.2024].

42 EUROPEAN DATA PROTECTION BOARD (2023): *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*. Disponible en la URL: https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf [Con acceso el 24.4.2024].

La Agencia Española de Protección de Datos, en su informe jurídico 0036/2020[43] señaló que: hay que adelantar que el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, ya que el artículo 9.1. se refiere a los "datos biométricos dirigidos a identificar de manera univoca a una persona física", por lo que, de una interpretación conjunta de ambos preceptos parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico especifico dirigido a identificar de manera univoca a una persona física. En este sentido, parece que igualmente se pronuncia el Considerando 51 al señalar que "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación univocas de una persona física"».

El Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de Trabajo del artículo 29, 00720/12/ES. WP193[44] expresa respecto de los datos biométricos que: «Los sistemas biométricos están estrechamente vinculados a una persona, dado que pueden utilizar una determinada propiedad única de un individuo para su identificación o autenticación. Mientras que los datos biométricos de una persona pueden suprimirse o alterarse, la fuente de la que se han extraído en general no puede ser modificada ni suprimida».

Si se recoge la información sin facilitar información suficiente no se realiza una puesta a disposición de los usuarios sobre los riesgos que implica el tratamiento de los datos, en este caso, los datos biométricos.

En el caso que nos ocupa esta información no ha sido facilitado de forma adecuada a los interesados, ya que no se les advierte de los riesgos que implica usar sus datos biométricos.

El tratamiento de los datos personales, y por ende, el de los datos biométricos, se basa en el consentimiento que se debe prestar sin vicios, de forma libre, un consentimiento específico, informado e inequívoco, y aquí ese consentimiento informado no se produce.

Tampoco se habilita un sistema para retirar el consentimiento, que siempre se puede revocar, y en este caso, no se admite la revocación.

De igual forma, no se acredita que se supere el análisis de idoneidad y necesidad que exige el tratamiento de los datos de alto riesgo, ni la existencia de otras alternativas para los fines objeto del tratamiento que se puedan realizar sin recabar datos biométricos.

La Agencia, por todo ello, considera que existen indicios racionales de que el tratamiento de los datos personales por medio del procesado de datos biométricos, puede constituir una vulneración de los artículos 5.1.a), 6.1, 7, 9, 12, 13 y 17 del Reglamento (UE) 2016/679.

La utilización de datos biométricos tiene unos riesgos muy elevados para los derechos de las personas. Teniendo en cuenta lo indicado como datos sensibles, y también en el caso de las personas vulnerables, como los menores, el tratamiento puede afectar a su bienestar y también a sus derechos y libertades fundamentales, como ya se ha puesto de manifiesto de forma reiterada.

También interesa destacar, y así lo pone de relieve la Agencia, la repercusión y alarma social que ha tenido la venta de los datos biométricos a cambio de criptomonedas. Es por todas las razones anteriormente aducidas que se ha adoptado atendiendo a las circunstancias de carácter excepcional y la urgencia para proteger los intereses de las personas, la adopción de medidas provisionales para el cese inmediato del tratamiento de los datos personales, la prevención de la cesión a terceros, y la salvaguarda del derecho fundamenta a la protección de datos personales atendiendo al mandato constitucional del artículo 18.4[45].

El artículo 57 del Reglamento (UE) 2016/679 determina que una serie de funciones de la autoridad de control, entre la que se encuentra la Agencia, y en particular lo indicado en el apartado 2, f), respecto a «tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control».

Esta intervención por parte de la Agencia es urgente para poder adoptar una medida cautelar de

43 Disponible en la URL: https://www.aepd.es/documento/2020-0036.pdf [Con acceso el 24.4.2024].

44 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2012). Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de Trabajo del artículo 29, 00720/12/ES. WP193. Disponible en la URL: https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf [Con acceso el 24.4.2024].

45 BOE núm. 311, de 29 de diciembre de 1978.

carácter excepcional, ya que se considera urgente la intervención para la protección de los derechos y libertades de los interesados, y podrá, como mecanismo de coherencia que se contempla en los artículo 63, 64, 65 y 66o al procedimiento que se indica en el artículo 60 del Reglamento (UE) 2016/679, la adopción de medidas provisionales de forma inmediata para que produzcan efectos jurídicos en su propio territorio, con un periodo de validez no superior a tres meses.

El tratamiento presuntamente ilícito, sigue indicando la Agencia, implica el procesamiento de datos personales sensibles a través de medios y formas altamente opacas e intrusivas, que podrían incluir operaciones de seguimiento y elaboración de perfiles, sin garantizar, además, el derecho de los interesados a la información adecuada. Se ponen en peligro también el derecho a la retirada del consentimiento o el derecho de supresión.

En el caso de que no se adopten medidas urgentes para garantizar el cumplimiento de la normativa de protección de datos estarían los interesados en un riesgo elevado, privándoles de las protecciones que le otorga el Reglamento (UE) 2016/679, y por tanto, la adopción de medidas urgentes de prohibición temporal de las actividades de tratamiento consideradas potencialmente irregulares está justificada para evitar daños potencialmente irreparables a sus derechos y libertades.

Como en este supuesto analizado, se da la circunstancia de intervención de menores, hay que atender al interés superior del menor tal y como está indicado en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil[46], así como indican también los Considerandos 38 y 75del Reglamento (UE) 2016/679, así como el artículo 84 de la Ley Orgánica 3/2018 respecto a la protección de los menores en internet, y los artículos 45 referente al uso seguro y responsable de internet y 52 sobre la Agencia Española de Protección de Datos, de la Ley Orgánica 8/2021.

Se acuerda por parte de la Agencia ordenar a la empresa en cuestión que, de forma inmediata, cese la recopilación y el tratamiento de datos personales en el territorio español que implica el escaneo de iris, ojos y rostro, y su posterior procesamiento; ordenar el bloqueo de los datos captados en territorio español, y ordenar a la empresa que comunique a la Agencia la efectiva ejecución de la medida dentro del plazo máximo de 72 horas desde la recepción del acuerdo.

46 BOE núm. 15, de 17 de enero de 1996.

El incumplimiento, según establece el artículo 83.6 del Reglamento (UE) 2016/679, de las resoluciones de la autoridad de control siguiente lo indicado en el apartado 58, apartado 2, del mismo texto legal, se sancionará con multas administrativas de 20 millones de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Durante el procedimiento sancionador, que, en su caso, se inicie, o bien en la resolución por la que se acuerde el archivo de las actuaciones previas de investigación, se resolverá sobre el mantenimiento o levantamiento de los efectos de la medida provisional adoptada.

Si bien esta decisión solamente es válida en el ámbito territorial en el que opera la Agencia, España, pero no en otros países en los que actúa la empresa.

Es interesante señalar también que la prestación del consentimiento por parte de los usuarios puede estar afectado por un vicio, ya que el tratamiento de los datos biométricos no ha sido informado de forma adecuada, y ello ha limitado la libertad de decisión del sujeto a la hora de acceder a la venta de los datos de su iris.

La creación también a través de una aplicación de móvil del perfil de identidad digital de las personas para realizar el escaneado del iris y que se les ofrece como contraprestación a ese consentimiento para el tratamiento de los datos biométricos, unos tokens de forma gratuita. Vemos que se obtiene un beneficio económico y la existencia de contraprestación no debería viciar la libertad de prestación del consentimiento. No obstante, hay que tener en cuenta distintos factores como es la edad, la capacidad y madurez para la formalización de un contrato y para comprender de forma adecuada el alcance y consecuencias del acto jurídico que están realizando.

Consideramos que muchas personas, en el caso del escaneo del iris iba dirigido a personas jóvenes, desconocen que incluso el iris se ha utilizado como contraseña, al ser único e identificar a la persona[47], su asociación con información sensible como es el estado de salud, y que la información que se contiene en el iris permanece inalterable[48] y que su

47 Esto lo hemos visto en el ámbito cinematográfico. Por ejemplo, en la película «La búsqueda».

48 Sigo la exposición de BIGAS FORMATJÉ, N. (2024): «El iris, ¿el dato biométrico de moda?». *Noticias. Universitat Oberta de Catalunya*. Disponible en la URL: https://www.uoc.edu/es/news/2024/iris-dato-biometrico-de-moda-worldcoin

identificación como contraseña es una de las más seguras, además de que no se pueden cambiar los datos obtenidos del iris. Con el escaneo del iris se generaba un código que identifica al sujeto. Los datos biométricos de identificación de los sujetos son distintos como puede ser la voz, la forma de realizar los movimientos, que pueden variar a diferencia del iris que se mantiene prácticamente intacto y no se puede modificar y de ahí las consecuencias de la comercialización de dichos datos.

Precisamente la estabilidad de los datos del iris lo convierte en objeto de deseo para hackers, ya que si se obtiene dicha información y se identifica al sujeto se puede suplantar su identidad, usarlo como contraseña, y a diferencia de las contraseñas que podemos introducir de forma manual, no se puede cambiar.

También se ha indicado que la finalidad de escanear el iris de las personas es poder diferenciar en un futuro los avatares de inteligencia artificial de las personas. Lo que se ha denominado "pasaporte de humanidad"[49] pero si no se establecen mecanismos de control adecuados y a estos datos tienen acceso terceros, se podría suplantar la identidad. Por tanto, el tratamiento de estos datos tan sensibles y que dada su inalterabilidad pueden ser objeto de fraude deben ser custodiados a través de una cadena o blockchain.

No dejar de estar claro qué es lo realmente se ha escaneado y si también se ha escaneado la imagen, y los datos faciales del sujeto, y si se ha anonimizado y si es reversible o no. Tampoco se obtiene suficiente información sobre la reutilización de dichos datos, si hay intereses económicos ocultos y si se van a ceder los datos, entre otras cuestiones.

Lo único que queda claro es que se paga en criptomonedas y se ha realizado un consentimiento que se incentiva a cambio de una cantidad económica, y se plantea en este caso lo que ha sido también objeto de debate los donantes de datos para investigación[50].

En el caso que nos ocupa las personas que hubieran participado en la contraprestación tienen derecho a la recuperación de los datos y ejercer los derechos que les amparan como el de supresión o de oposición al tratamiento de los mismos.

IV. CONCLUSIONES

Los datos de salud como datos sensibles y dentro de los mismos los datos biométricos son especialmente protegidos por la normativa aplicable porque su tratamiento puede afectar a los derechos y libertades de los sujetos.

La utilización de los datos de salud no puede generar un menoscabo en los derechos subjetivos, y tampoco un sesgo de carácter discriminatorio por el contenido de los mismos.

Existe un claro desconocimiento de la importancia de los datos de salud y como hemos visto en el caso de los datos biométricos muchas personas han escaneado su iris a cambio de una contraprestación económica. La falta de conciencia de las consecuencias que ello puede conllevar supone un hándicap para la concienciación de que los datos personales tienen que protegerse.

La legislación presta especial atención a estas categorías de datos y pone unos límites muy claros para su protección, pero, a pesar de ello, los sujetos realizan acciones dentro del principio de autonomía de la voluntad que ponen en peligro sus propios derechos y libertades fundamentales.

Consideramos que diversas prácticas de comercialización de los datos, en este caso que hemos analizado, biométricos no son lícitas, ya que no se proporciona suficiente información al sujeto, se le incentiva con una contraprestación y se produce el denominado "efecto llamada" con lo que la voluntad puede estar viciada por el error en sí.

Cuestiones como el uso de esos datos sensibles, el acceso a terceros, y en el caso del escaneo del iris, la suplantación de la identidad nos sitúa en la línea de problemas no resueltos con la práctica realizada y que ponen en peligro los derechos subjetivos. Más aún cuando estamos ante colectivos muy vulnerables, como los menores de edad, y la prestación del consentimiento sin suficiente información, por lo que puede adolecer un vicio en la prestación del mismo.

La actual regulación de la inteligencia artificial por Reglamento (UE) 2024/1689 debe ser puesta en relación con la normativa de protección de datos, ya que la utilización de sistemas de inteligencia artificial pueden utilizar datos protegidos y es preciso, también, atender a su calificación con sistema de alto riesgo.

[Con acceso el 18.4.2024], que refleja las opiniones de Eduard Blasi y Jordi Serra Ruiz.

49 BIGAS (2024).

50 RAMÓN FERNÁNDEZ, F. (2022d): «Inteligencia artificial y donante de datos para investigación: ¿utopía o realidad?». En *El Derecho ante la tecnología: innovación y adaptación*, Colex, págs. 151 y sigs.

V. BIBLIOGRAFÍA

ABAD AMORÓS, Mª. R. (2003). "El carácter sensible de los datos biométricos". *Datospersonales. org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, págs. 1-4.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2012). Dictamen 3/2012 sobre la evolución de las tecnologías biométricas del Grupo de Trabajo del artículo 29, 00720/12/ES. WP193. Disponible en la URL: https://www.aepd.es/sites/default/files/2019-12/wp193_es.pdf [Con acceso el 24.4.2024].

• (2020). *Informe jurídico 0036/2020*. Disponible en la URL: https://www.aepd.es/documento/2020-0036.pdf [Con acceso el 24.4.2024].

• (2024). *Acuerdo de adopción de medida provisional correspondiente al EXP202312448*. Disponible en la URL: https://www.aepd.es/documento/co-000297-2023-medida-provisional.pdf [Con acceso el 24.4.2024].

AGUIAR, L. (2022). "Los desafíos de la inteligencia artificial aplicada a productos médicos". *Indufarma: industria farmacéutica*, (20), págs. 28-31. Disponible en la URL: https://indufarma.com.uy/indufarma-julio-2022/ [Con acceso el 14.4.2024].

ANDREU MARTÍNEZ, B. (2023). "Datos de salud y bien común: hacia la construcción de un mercado europeo de datos sanitarios". En B. Andreu Martínez y A. Espinosa de los Monteros Rodríguez (Coord.), *Tecnología para la salud: una visión humanista desde el biodererecho*, Plaza y Valdés, págs. 209-240.

• (2023). " La necesaria actualización de la Ley de Autonomía del Paciente frente a los retos en la gestión de los datos de salud". En B. Andreu Martínez (Coord.), *Los datos de salud como eje de la transformación digital de la Sanidad*. Comares, págs. 139-159. Disponible en la URL: https://accesoabiertocomares.com/index.php/coa/catalog/book/51 [Con acceso el 25.4.2024].

BIGAS FORMATJÉ, N. (2024). "El iris, ¿el dato biométrico de moda?". *Noticias. Universitat Oberta de Catalunya*. Disponible en la URL: https://www.uoc.edu/es/news/2024/iris-dato-biometrico-de-moda-worldcoin [Con acceso el 18.4.2024].

CASANOVA ASENCIO, A. S. (2023). "Espacio Europeo de datos sanitarios, uso primario y autonomía del paciente". En B. Andreu Martínez (Coord.), *Los datos de salud como eje de la transformación digital de la Sanidad*. Comares, págs. 107-138. Disponible en la URL: https://accesoabiertocomares.com/index.php/coa/catalog/book/51 [Con acceso el 14.4.2024].

COBAS COBIELLA, Mª. E. y PÉREZ COBAS. A. E. (2023). "Medicina personalizada. Retos para el derecho". En C. Gil Membrado (Dir.), *Derecho y medicina: desafíos tecnológicos y científicos*, Dykinson, págs. 129-152.

COMISIÓN EUROPEA (2020). *Estrategia Europea de Datos*. Disponible en la URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es [Con acceso el 18.4.2024].

DE LECUONA RAMÍREZ, I. (2020). "Aspectos ético, legales y sociales del uso de la inteligencia artificial y el Big Data en salud en un contexto de pandemia". *Revista internacional de pensamiento político*, (15), págs. 139-166. Disponible en la URL: https://www.upo.es/revistas/index.php/ripp/article/view/5599 [Con acceso el 13.4.2024].

DE MIGUEL BERIAIN, I. (2023). "El uso de datos de salud para investigación biomédica a la luz de la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios". *Revista jurídica de Castilla y León*, (60), págs. 7-35. Disponible en la URL: https://www.jcyl.es/web/jcyl/AdministracionPublica/es/Plantilla100Detalle/1131978346397/Publicacion/1285279043799/Redaccion [Con acceso el 11.4.2024].

EUROPEAN DATA PROTECTION BOARD (2023). *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement*. Disponible en la URL: https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf [Con acceso el 24.4.2024].

GÓMEZ PIQUERAS, C. (2009). "Disociación/anonimización de los datos de salud". *Revista Derecho y Salud*, volumen 18 (1), págs. 43-56. Disponible en la URL: https://www.ajs.es/sites/default/files/2020-05/DyS-Vol18-01-estudio_03.pdf [Con acceso el 10.4.2024].

GONZÁLEZ REVUELTA, Mª. E. (2023). *Evolución de la historia clínica digital, retos y dificultades: Avances y desafíos en la seguridad de la historia clínica y el acceso a los datos de salud.* Almería. Universidad de Almería. Disponible en la URL: https://repositorio.ual.es/bitstream/handle/10835/14572/01.Tesis.pdf?sequence=1&isAllowed=y [Con acceso el 12.4.2024].

GUILLÉN CATALÁN, R. (2020). "Sujetos responsables por vulneración de las normas de protección de datos. Especial referencia a los datos relativos a la salud". *Revista Boliviana de Derecho,* (30), págs. 40-75. Disponible en la URL: https://dialnet.unirioja.es/descarga/articulo/7521500.pdf [Con acceso el 12.4.2024].

JAREÑO BUTRÓN, M. y ARRATIBEL ARRONDO, J. A. (2023). "Técnicas para el control del tratamiento masivo de datos personales en el sector público sanitario". *Auditoría pública: revista de los Órganos Autónomos de Control Externo,* (81), págs. 180-195. Disponible en la URL: https://asocex.es/wp-content/uploads/2023/05/Articulo-13.pdf [Con acceso el 12.4.2024].

LATORRE LUNA, L. (2022). "El valor de los datos sanitarios de las Administraciones públicas: ¿Los futuros bienes de dominio público?". *Revista catalana de dret públic*, (65), págs. 46-162. Disponible en la URL: http://revistes.eapc.gencat.cat/index.php/rcdp/article/view/10.2436-rcdp.i65.2022.3834 [Con acceso el 11.4.2024].

MORTE FERRER, R. (2023). "Crítica de la Conferencia de Autoridades de Protección de Datos Alemana a la Propuesta de Reglamento para la regulación del Espacio Europeo de Datos de Salud". *La Ley privacidad* (16).

PÉREZ COBAS, A. E. y COBAS COBIELLA, Mª. E. (2020). "Datos genéticos y datos de salud. Una aproximación a su estudio". *Revista Boliviana de Derecho,* (30), págs. 428-453. Disponible en la URL: https://dialnet.unirioja.es/descarga/articulo/7521512.pdf [Con acceso el 10.4.2024].

PLAZA PENADÉS, J. (2022). "Cuestiones actuales de la inteligencia artificial y el BIG DATA". En L. Martínez Velencoso y M. Sancho López (Dir.), *Protección jurídica de la privacidad. Inteligencia Artificial, Salud y Contratación*, Thomson Reuters Aranzadi, págs. 45-70.

• (2023). "Cuestiones básicas del derecho de protección de datos de carácter personal y su seguridad". *Revista Aranzadi de derecho y nuevas tecnologías*, (63).

RAMÓN FERNÁNDEZ, F. (2020a). "El derecho a la vida y a la protección de la salud en las medidas adoptadas en España como consecuencia de la covid-19. Una reflexión sobre su oportunidad". *Estudios Constitucionales*, volumen 18 (2), págs. 51-86. Disponible en la URL: http://www.estudiosconstitucionales.cl/index.php/econstitucionales/article/view/701/420 [Con acceso el 10.4.2024].

• (2020b). "La sanidad móvil: la protección de datos referentes a la salud y la genética", En F. Ramón Fernández, (Coord.), *Marco Jurídico de la Ciencia de Datos*, Tirant lo Blanch, págs. 197-250.

• (2022a). "Inteligencia artificial y protección de la salud: La necesidad de establecer unos límites en la carta de derechos digitales", En M. J. Blanco Sánchez (Coord.), A. Madrid Parra y L. Alvarado Herrera (Dir.), *Derecho digital y nuevas tecnologías*, Aranzadi, págs. 1027-1048.

• (2022b). "Protección de datos de salud en el ámbito laboral: una perspectiva española", En *Estudos sobre LGPD – Lei geral de proteção de dados. Doutrina e aplicabilidade no* âmbito *laboral*, Editorial Diadorim, págs. 99-111.

• (2022c). "Nuevos retos de la inteligencia artificial: ética y responsabilidad", En L. Martínez Velencoso y M. Sancho López (Dir.), *Protección jurídica de la privacidad. Inteligencia Artificial, Salud y Contratación*, Thomson Reuters Aranzadi, págs. 123-149.

• (2022d). "Inteligencia artificial y donante de datos para investigación: ¿utopía o realidad?, En *El Derecho ante la tecnología: innovación y adaptación*, Colex, págs. 151-172.

SALAZAR ROSADO, C. (2023). "Los desafíos del «datalake» sanitario: ¿cambio de paradigma en el control de los individuos sobre sus datos personales". *Comunicaciones en propiedad industrial y derecho de la competencia,* (100), págs. 43-61.

TODOLÍ, A. (2024). "Reglamento europeo de IA y su coordinación con el Reglamento de protección de datos (Iniciativa interblogs)". *Argumentos en Derecho Laboral*. Disponible en la URL: https://adriantodoli.com/2024/04/18/reglamento-europeo-de-ia-y-su-coordinacion-con-el-reglamento-de-proteccion-de-datos-iniciativa-interblogs/ [Con acceso el 18.4.2024].

VIVAS TESÓN, I. (2023). "Transparencia, protección y control de los datos de salud en la sanidad digital". En Mª. E. Cobas Cobiella y R. Guillén Catalán (Dir.), *Equidad y transparencia en la prestación de servicios*, Dykinson, págs. 223-250.