EL ESCUDO PERMEABLE:
DATOS DE SALUD Y RIESGOS DE INTERPRETACIÓN EXTENSIVA EN LAS EXCEPCIONES DEL ARTÍCULO 9 DEL RGPD

Resumen

Este artículo analiza el tratamiento de datos de salud bajo el RGPD, centrándose en la expansión del concepto de dato sanitario y el alcance del régimen de excepciones del artículo 9. Se sostiene una lectura funcional en la que la naturaleza del dato no depende de su origen clínico, sino de su capacidad para revelar el estado físico o mental del individuo, incluso mediante inferencias a partir de información aparentemente neutra.

Desde esta perspectiva, las excepciones dejan de ser supuestos marginales para convertirse en el espacio operativo del tratamiento en el sector salud. Este escenario plantea el riesgo de interpretaciones expansivas que, bajo una legalidad formal, diluyen los límites de protección. El análisis examina las limitaciones estructurales del consentimiento en entornos de reutilización y enriquecimiento de datos, reivindicando el papel de los principios como mecanismos de control material.

Finalmente, se aborda la función del Delegado de Protección de Datos como garante de una aplicación exigente del marco normativo, más allá del mero cumplimiento administrativo. El trabajo concluye que el principal desafío no radica en la falta de regulación, sino en evitar que una apariencia de suficiencia legal sustituya la tutela efectiva de los derechos y la dignidad del paciente.

I. Introducción

"First there is the law" —"ante todo está la ley"— fue la respuesta dada por Mustafa Suleyman, cofundador y CEO de DeepMind, al ser cuestionado por un periodista en una entrevista[1] sobre cómo podía garantizarle al público que sus datos de salud estarían debidamente protegidos.

El caso Royal Free–Google DeepMind constituye un referente constante en el debate académico europeo sobre protección de datos en el sector sanitario, en razón de haberse configurado un caldo de cultivo que incluía tres ingredientes particularmente explosivos: la naturaleza extremadamente sensible de los datos tratados, la escala del tratamiento y la implicación de DeepMind, filial de Google, uno de los mayores conglomerados tecnológicos del mundo.

El propósito de este artículo no es reexaminar lo ya establecido por la doctrina y la jurisprudencia en torno a este asunto. Lo que aquí interesa es algo que la frase de Suleyman pone al descubierto sin pretenderlo: que el cumplimiento formal de la norma no garantiza su cumplimiento real. DeepMind contaba con asesoramiento jurídico en la materia, había suscrito acuerdos con el Servicio Nacional de Salud del Reino Unido (por sus siglas en inglés NHS) y el proyecto fue clasificado como *"direct care"*, categoría que, en el marco del derecho sanitario británico, habilita el uso de datos clínicos sin consentimiento explícito. La Oficina del Comisionado de Información (ICO, por sus siglas en inglés) llegó a una conclusión diferente, al fallar que el tratamiento era ilícito. El hospital no estableció una base jurídica adecuada para la cesión de los datos y los pacientes nunca fueron informados de ello. [2]

---

[1] *SULEYMAN, Mustafa, declaraciones en entrevista "Big Read: What does Google DeepMind want with the NHS?", Digital Health News, 20 de marzo de 2017. Disponible en: https://www.digitalhealth.net/2017/03/deepmind-mustafa-suleyman-interview/*

[2] *ICO, Royal Free – Google DeepMind trial failed to comply with data protection law, 3 de julio de 2017. Disponible en: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/*

El verdadero problema que estas páginas examinan no es el incumplidor que ignora la ley. El riesgo real está en quien cree cumplirla plenamente, convencido por la falsa seguridad que le vende su propio equipo de expertos, al confundir una excepción habilitante con un cheque en blanco.

La Comisionada de Información Elizabeth Denham fue contundente al señalar que el Trust *"podía y debía haber sido mucho más transparente con los pacientes sobre lo que estaba ocurriendo"*. [3] El propio Suleyman lo reconoció públicamente tiempo después, admitiendo que la prisa por innovar les había hecho perder de vista que detrás de cada dato había un paciente, no un usuario de tecnología [4]. ¿Y las consecuencias de aquel fallo? El ICO no impuso sanción económica alguna. Bajo la *Data Protection Act* de 1998, multar exigía acreditar un daño sustancial a los afectados, umbral que el regulador consideró no alcanzado.

Pero la verdadera lección del caso trasciende a sus protagonistas. Y es que puede afectar a cualquier organización sanitaria que invoque las excepciones previstas en la normativa de protección de datos como justificación suficiente, sin el análisis riguroso que esas mismas excepciones exigen. Ese es el objeto de este trabajo.

---

[3] DENHAM, Elizabeth, declaración oficial recogida en *TechCrunch*, 3 de julio de 2017. Disponible en: https://techcrunch.com/2017/07/03/uk-data-regulator-says-deepminds-initial-deal-with-the-nhs-broke-privacy-law/

[4] SULEYMAN, Mustafa y KING, Dominic, *"The Information Commissioner, the Royal Free, and what we've learned"*, blog oficial de DeepMind, 3 de julio de 2017. Disponible en: https://deepmind.google/discover/blog/the-information-commissioner-the-royal-free-and-what-weve-learned/

II. La anatomía del dato de salud

De conformidad con el artículo 4.15 del Reglamento General de Protección de Datos (RGPD), se entienden por datos relativos a la salud aquellos datos personales vinculados a la dimensión física o mental de un individuo cuya naturaleza permita revelar información sobre su estado de salud. Esta formulación, en apariencia simple, introduce un criterio claramente funcional, centrado en la capacidad reveladora del dato. La Directiva 95/46/CE, si bien no ofrecía una definición expresa, abordaba los datos relativos a la salud principalmente desde la perspectiva de su tratamiento, asociándolos en su considerando 33 a contextos sanitarios y a la intervención de profesionales sujetos al secreto profesional, sin desarrollar un criterio autónomo de calificación basado en su potencial informativo.

El factor determinante no es entonces la autoría del registro ni el contexto asistencial en que se genera, sino la capacidad informativa que contiene. Bajo esta lógica funcional, la categoría especial trasciende el ámbito estrictamente clínico, para transformarse en una noción dinámica, donde lo decisivo es el potencial del dato para revelar la condición biológica o mental a través de registros en apariencia administrativos, como una factura de farmacia, el justificante de una cita en cuidados paliativos. [5]

El Considerando 35 refuerza y amplía esta lógica. Mientras el artículo opera como un núcleo conceptual, el considerando despliega un catálogo descriptivo de situaciones que deben entenderse comprendidas en esta categoría, incluyendo identificadores sanitarios, muestras biológicas, tratamientos o estados biomédicos, con la precisión de que ello opera *independientemente de su fuente*. Al afirmar que la

[5] Esta interpretación ha sido respaldada por la jurisprudencia del Tribunal de Justicia de la Unión Europea. En particular, la Sentencia de 1 de agosto de 2022, asunto C-184/20, en la que el Tribunal subraya que la protección de las categorías especiales no puede eludirse mediante datos aparentemente neutros que permitan inferir información sensible.

información queda comprendida con independencia de su origen, el legislador elimina cualquier intento de restringir el concepto a circuitos sanitarios formales. Un dato adquiere naturaleza de categoría especial aunque haya sido generado fuera del sistema sanitario, siempre que permita inferir información sobre la salud.

Este planteamiento muestra el verdadero alcance de la protección. Registros que parecen inocuos, como el conteo de pasos, los patrones de sueño o la frecuencia cardíaca obtenida por dispositivos portátiles, pueden convertirse en datos de salud por la información que permiten deducir. La relevancia jurídica no depende del contexto clínico en que se originan, sino de la capacidad del registro para revelar el estado de salud de la persona. En consecuencia, la categoría especial deja de ser una noción fija vinculada a la fuente y se define por el tratamiento efectivo del dato o por su cruce con otras informaciones.

Bajo esta lógica, la inferencia ocupa un lugar central. El registro no necesita contener información médica explícita; basta con que el análisis o la correlación permitan deducirla. Esta interpretación, recogida por el Comité Europeo de Protección de Datos (CEPD) en sus Directrices 05/2020, confirma que no existe una separación clara entre los datos de bienestar y los de salud. El Comité advierte que registros obtenidos inicialmente con fines de estilo de vida pueden adquirir la condición de categorías especiales cuando se utilizan para extraer conclusiones sobre el estado físico o mental de una persona. La calificación jurídica depende, por tanto, de la explotación del dato y de la naturaleza de los resultados que genere.

III. El régimen de excepciones: la ambigüedad como título habilitante

El artículo 9 del RGPD parte de una premisa sencilla: el tratamiento de categorías especiales de datos personales está prohibido. La norma refleja una lógica de cautela frente a este tipo de información, situando su uso fuera del marco ordinario.

El propio precepto introduce, sin embargo, los supuestos en los que esa prohibición se levanta. No son precisamente escenarios marginales. En la práctica, constituyen el espacio donde se articula el tratamiento de datos relativos a la salud.

Es en ese terreno donde la prohibición adquiere sentido, no como una regla aislada, sino en relación con las condiciones que permiten su levantamiento.

En el ámbito sanitario, el tratamiento se admite cuando es necesario para fines de diagnóstico, asistencia o gestión de servicios de salud, cuando responde a razones de salud pública o cuando se inserta en actividades de investigación. No describen supuestos excepcionales en sentido estricto. Se trata de ámbitos en los que el tratamiento constituye una condición de funcionamiento.

Aquí aparece la ambigüedad que da título a este apartado. Las excepciones no siempre operan como límites estrechos. En determinados contextos, se convierten en verdaderos títulos habilitantes de alcance amplio. Su formulación facilita lecturas extensivas que, aun manteniéndose dentro del marco normativo, desplazan el rigor con el que debería operar la prohibición.

El riesgo se hace más visible en las letras g), h) e i) del artículo. La referencia al interés público esencial, a la medicina preventiva o a la gestión de servicios sanitarios introduce conceptos cuya delimitación no siempre es precisa. Cuando estas categorías se interpretan de forma extensiva, el ámbito de aplicación de la excepción se expande

con ellas. Proyectos orientados a la optimización de recursos o al análisis masivo de información pueden quedar amparados bajo estas fórmulas, desplazando la necesidad de recabar el consentimiento del interesado.

El precepto introduce, no obstante, elementos de contención. El apartado 3 exige que el tratamiento se realice por profesionales sujetos a secreto profesional o bajo su responsabilidad. Esta exigencia remite a un marco de control tradicional, pero no elimina la amplitud de los supuestos habilitantes.

En este contexto, el consentimiento explícito ocupa una posición menos central de lo que podría parecer. El artículo permite el tratamiento cuando el interesado lo ha otorgado, pero al mismo tiempo prevé que el Derecho de la Unión o de los Estados miembros pueda impedir que la prohibición sea levantada por el propio titular.

Esta previsión cuestiona la idea de disponibilidad del derecho. El consentimiento deja de ser, en todos los casos, un criterio suficiente de legitimación. Existen situaciones en las que la protección del dato se sitúa fuera del alcance de la decisión individual.
Incluso cuando el consentimiento resulta admisible, su eficacia encuentra límites en el contexto en el que se presta. La exigencia de que sea informado no se satisface únicamente con la comunicación formal de una finalidad. En entornos donde el tratamiento puede dar lugar a inferencias o a usos no evidentes en el momento de la recogida, el alcance de lo que el interesado comprende queda necesariamente acotado. La decisión se adopta sobre aquello que se le explica, pero no siempre alcanza a las posibles derivaciones del tratamiento.

Dicha limitación adquiere especial relevancia en situaciones de vulnerabilidad. En contextos como la participación en estudios experimentales por parte de pacientes con patologías graves, la voluntad puede verse condicionada por factores que no

responden a una elección plenamente libre. El ordenamiento responde a esta circunstancia limitando la eficacia del consentimiento y sometiendo el tratamiento a controles adicionales, normalmente a través de exigencias éticas y autorizaciones específicas.

A lo anterior se añade la facultad prevista en el apartado 4, que permite a los Estados miembros introducir condiciones adicionales o limitaciones respecto del tratamiento de datos relativos a la salud. La consecuencia es una fragmentación del régimen jurídico. El marco europeo no agota la regulación, sino que se completa con disposiciones nacionales que pueden reforzar o restringir el tratamiento.

Para los responsables y encargados, esta previsión introduce una exigencia adicional. La identificación de una excepción en el artículo 9 no resulta suficiente si no se verifica su alcance en el ordenamiento aplicable. En entornos transfronterizos, esta circunstancia añade un nivel de complejidad que incide directamente en la seguridad jurídica.

Este marco, sin embargo, no agota la cuestión. El problema de fondo no se encuentra en la existencia de las excepciones. Su necesidad es evidente. El sistema sanitario, la salud pública y la investigación dependen de ellas. La dificultad aparece cuando se invocan como si bastaran por sí mismas.

Cuando el análisis se limita a la mera existencia de una base habilitante, sin ponderar con el mismo rigor sus límites y contexto, la excepción deja de operar como un mecanismo de control y pasa a funcionar como una autorización automática. Esta distorsión adquiere especial relevancia si se vincula a la posibilidad de inferir información de salud. Si la naturaleza de salud puede emerger de registros en apariencia ajenos al ámbito clínico, el ámbito de aplicación del artículo 9 se expande y, con él, se multiplican

los supuestos en los que puede invocarse una excepción, desplazando la necesidad de recabar el consentimiento del interesado.

No se trata de fenómenos independientes. La ampliación del concepto de dato y la amplitud de las habilitaciones se refuerzan mutuamente. A medida que uno se amplía, el otro gana terreno. El resultado no es la inaplicación de la norma, sino algo más difícil de identificar: el tratamiento encuentra cobertura en el propio sistema de excepciones, apoyándose en una interpretación extensiva de sus elementos, con la consiguiente pérdida de eficacia de la prohibición inicial como límite.

IV. El tratamiento de datos de salud: más allá de la excepción

El reconocimiento de una excepción en el artículo 9 no agota el análisis jurídico del tratamiento. La existencia de una base habilitante permite el tratamiento, pero no lo legitima de forma incondicional. El marco normativo no se limita a autorizar, sino que impone exigencias que operan con independencia del supuesto invocado. La concurrencia de una de las circunstancias previstas en el precepto constituye apenas un punto de partida, nunca de cierre.

A partir de esa habilitación inicial, el análisis se proyecta sobre las condiciones materiales en que el tratamiento se desarrolla y sobre los límites que persisten. Es en este plano donde se sitúan las tensiones más relevantes. Cuanto más elástico es el alcance de las excepciones, mayor es la necesidad de examinar con rigor el tratamiento. La cuestión deja de centrarse en la posibilidad abstracta de tratar datos de salud para plantearse en términos de cómo y hasta dónde esa actividad resulta compatible con el sistema de garantías.

El control del tratamiento se sitúa entonces en el ámbito de los principios. Es en este plano donde el sistema conserva su capacidad para acotar el alcance de las

excepciones. La minimización, la limitación de la finalidad o la proporcionalidad no operan como formulaciones abstractas, sino como criterios que condicionan de manera efectiva el tratamiento, incluso cuando este se ampara en alguno de los supuestos del artículo 9.

La concurrencia de un supuesto habilitante no resulta suficiente por sí misma. Es preciso justificar, en cada caso, la necesidad del tratamiento y la medida en que este se mantiene dentro de los límites que la norma permite. En esa verificación se determina si el tratamiento se ajusta a las garantías previstas o si, por el contrario, desborda los fines que el sistema pretende preservar.

Sin embargo, el control articulado a través de los principios no restituye plenamente la posición del interesado. Permite delimitar el tratamiento, pero no siempre asegura que el titular conserve una comprensión real de su alcance. Esta limitación se hace visible cuando el tratamiento no se agota en la finalidad inicial de la recogida. En el ámbito sanitario, la información obtenida en un contexto asistencial puede integrarse posteriormente en procesos de gestión o investigación; en tales supuestos, el alcance del consentimiento inicial difícilmente coincide con el conjunto de operaciones que efectivamente se llevan a cabo.

Cuando el tratamiento permite, además, derivar información adicional a partir de los datos disponibles, el contenido de lo consentido queda vinculado a lo que el interesado puede anticipar en ese momento. El desfase entre la decisión inicial y las derivaciones del tratamiento introduce un límite estructural al consentimiento como mecanismo de control. La voluntad del titular se proyecta sobre una finalidad declarada, pero el potencial informativo del dato termina por desbordar su capacidad de previsión.

El sistema admite esta proyección bajo determinadas condiciones, pero su aplicación exige un examen especialmente riguroso. La compatibilidad entre finalidades no puede presumirse a partir de la mera existencia de una base habilitante; debe valorarse en función del contexto de obtención, de las expectativas razonables del interesado y del impacto que el nuevo tratamiento genera.

En este punto, el problema no radica en la ausencia de cobertura jurídica, sino en la forma en que esta se construye. La reutilización del dato puede encontrar amparo en el propio sistema normativo y, sin embargo, distanciarse de la lógica que justifica su protección. Es ahí donde la aplicación formal de las excepciones puede sostener tratamientos conformes en apariencia, pero alejados de la tutela efectiva que el régimen pretende garantizar.

V. El Delegado de Protección de Datos como garante del sistema

El análisis de la permeabilidad del escudo de protección no puede completarse sin examinar la figura a la que el RGPD atribuye la función de vigilancia interna del sistema: el Delegado de Protección de Datos. Su régimen jurídico, regulado en los artículos 37 a 39 del Reglamento, define un perfil que trasciende el de un simple asesor de cumplimiento. El artículo 39 le asigna, entre otras funciones, supervisar el cumplimiento del Reglamento y de las políticas del responsable, asesorar sobre la evaluación de impacto relativa a la protección de datos y cooperar con la autoridad de control. Esta definición no es meramente administrativa; comporta una posición activa en la verificación material de que el tratamiento se ajusta a las estrictas condiciones que el marco normativo impone.

La independencia funcional del DPD, garantizada por el artículo 38.3, que prohíbe taxativamente que reciba instrucciones en el ejercicio de sus funciones, constituye el presupuesto de su utilidad como garantía. Un delegado que actúa como validador de

decisiones preexistentes o que calibra su criterio en función de las preferencias del responsable no cumple la función que el Reglamento le asigna. Su intervención adquiere sentido precisamente allí donde el marco normativo admite interpretaciones distintas y donde la organización tiene incentivos para optar por la lectura más favorable a sus intereses operativos en detrimento de los derechos del titular.

En el sector sanitario, donde la urgencia asistencial, la escala del tratamiento y el valor estratégico de la información de salud crean presiones sistemáticas hacia la interpretación extensiva de las habilitaciones, la función del DPD se vuelve especialmente crítica. Su posición le permite, y le obliga a introducir una fricción analítica necesaria en los procesos de toma de decisiones.

Esta fricción no consiste en obstruir el tratamiento, sino en desplazar el examen desde la mera facultad de tratar hacia la justificación material de la operación: la necesidad real, la proporcionalidad, el impacto sobre el titular y la adecuación de las salvaguardas adoptadas. Este examen debe alcanzar incluso aquellos supuestos en los que la información no es sanitaria en origen, pero cuya presencia constante en diversos entornos permite inferir patologías o condiciones de salud mediante cruces de datos.

La Evaluación de Impacto relativa a la Protección de Datos (EIPD), regulada en el artículo 35 del RGPD, es el instrumento en que esta función se materializa de forma más visible. La EIPD no debe concebirse como un trámite documental que precede al tratamiento; debe operar como un proceso de análisis de riesgos vivo, capaz de capturar los cambios en las herramientas tecnológicas, como plataformas en la nube o sistemas de almacenamiento compartido, que a menudo amplían el flujo de datos sin una visibilidad plena.

El delegado que concibe la EIPD como un mero documento de archivo ha vaciado de contenido el mecanismo de control más potente que el Reglamento pone a su disposición.

El mismo principio rige los supuestos de reutilización y expansión de finalidades. Cuando la organización pretende integrar información recogida con fines asistenciales en proyectos de optimización o investigación, la función del delegado consiste en someter ese nuevo uso al riguroso examen de compatibilidad que el artículo 6.4 impone.

La habilitación formal de una excepción del artículo 9 no sustituye esta valoración material; la presupone. Medidas como el cifrado de soportes, la autenticación reforzada o la segmentación de perfiles no son decisiones accesorias, sino los elementos que determinan si el tratamiento se mantiene dentro de un entorno controlado.

En organizaciones de menor madurez estructural, el DPD debe asumir además una función pedagógica que el Reglamento no enuncia expresamente, pero que se desprende de la lógica de su posición. Las prácticas informales (uso de dispositivos personales, intercambio de datos por canales no corporativos o ausencia de protocolos de acceso) no siempre responden a una voluntad de incumplimiento. Responden, con mayor frecuencia, a una percepción distorsionada del riesgo que el delegado debe corregir mediante criterios claros. La figura del DPD no es la solución definitiva a la permeabilidad del sistema, pero sí su correctivo institucional más próximo, asegurando que la legalidad sea el umbral mínimo de una responsabilidad que la trasciende.

VI. Conclusiones

El uso de datos de salud bajo el RGPD revela una tensión estructural que este artículo ha denominado "escudo permeable": un sistema de protección que mantiene intacta su arquitectura formal mientras sus límites materiales se erosionan por la

conjunción de dos fenómenos que se refuerzan mutuamente. El primero es la expansión funcional del concepto de dato de salud. La calificación jurídica ya no depende del origen clínico del registro, sino de su capacidad reveladora de la condición física o mental del individuo. Esta interpretación, validada por la jurisprudencia reciente del TJUE, amplía el ámbito de aplicación del artículo 9 mucho más allá de los circuitos sanitarios tradicionales, alcanzando flujos de información aparentemente neutros pero con un alto potencial de inferencia.

El segundo fenómeno es la tendencia crítica a tratar las excepciones del citado artículo como si fueran títulos habilitantes autosuficientes. Se incurre con frecuencia en el error de considerar que la mera concurrencia formal de una excepción desplaza el análisis de sus condiciones materiales de legitimación. El estudio de los supuestos previstos en las letras h), i) y j) del artículo 9.2 ha mostrado que su formulación, necesariamente abierta para dar cabida a la complejidad del sector, facilita lecturas extensivas. Estas interpretaciones, sin incurrir en una infracción administrativa aparente, diluyen la prohibición general del tratamiento hasta hacerla funcionalmente irrelevante en la práctica diaria. La clave de este riesgo no reside en la apertura de los supuestos, que posee una justificación legítima, sino en la omisión sistemática del juicio de necesidad y proporcionalidad que cada uno de ellos presupone.

Frente a esta permeabilidad, el sistema jurídico ofrece dos correctivos esenciales que deben operar de forma sincronizada. El primero es la vigencia absoluta de los principios del artículo 5, que condicionan la licitud del tratamiento con independencia de la base habilitante identificada. Su aplicación rigurosa, especialmente mediante el test de compatibilidad en los supuestos de reutilización y expansión de finalidades, es lo único que puede restituir la eficacia de la norma como límite material a la voracidad del dato.

El segundo es la figura del DPD, cuya independencia funcional y posición estratégica lo convierten en el mecanismo de control más próximo al momento en que las decisiones de tratamiento se adoptan. Ninguno de estos correctivos es suficiente por sí solo; es su ejercicio conjunto y proactivo el que el sistema prevé como respuesta institucional ante la asimetría informativa.

El caso *Royal Free–Google DeepMind*, con el que abre este trabajo, ilustra con exactitud las consecuencias de que esta conjunción de garantías no se produzca. Una organización con asesoramiento especializado, bases habilitantes identificadas y procedimientos documentados ejecutó un tratamiento que el regulador declaró ilícito. No se debió a una infracción deliberada, sino a una confusión técnica: suponer que la existencia de la excepción equivalía a la suficiencia del análisis. El escudo existía y era formalmente correcto, pero resultó permeable ante la ausencia de una evaluación de impacto real y transparente.

"First there is the law". Esta afirmación sitúa el cumplimiento normativo como el punto de partida innegociable. Sin embargo, este artículo ha tratado de demostrar que, en el ámbito sanitario, esa condición necesaria dista mucho de ser suficiente para garantizar la tutela efectiva. La legalidad constituye apenas el umbral mínimo de una responsabilidad que la trasciende. Frente a la capacidad de los modelos masivos de datos para desbordar la previsión y la autodeterminación del titular, debe prevalecer un compromiso que precede en veinticinco siglos a cualquier reglamento: la máxima hipocrática de no causar daño. La protección de la privacidad en salud no puede reducirse a la mera ausencia de infracción; exige una lealtad hacia el paciente que impida que la utilidad del dato se sitúe, bajo ninguna circunstancia, por encima de su dignidad y de la confianza depositada en el sistema.

VII. Fuentes y Bibliografía

Normativa y organismos reguladores

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.

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

Data Protection Act 1998 (Reino Unido).

Comité Europeo de Protección de Datos (CEPD). Directrices 05/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, versión adoptada el 4 de mayo de 2020.

Information Commissioner's Office (ICO). Royal Free-Google DeepMind trial failed to comply with data protection law, 3 de julio de 2017.

Jurisprudencia

Tribunal de Justicia de la Unión Europea (TJUE), Sentencia de 6 de noviembre de 2003, asunto C-101/01, Lindqvist.

Tribunal de Justicia de la Unión Europea (TJUE), Sentencia de 1 de agosto de 2022, asunto C-184/20, Vyriausioji tarnybinės etikos komisija.

Doctrina y declaraciones oficiales

Denham, Elizabeth. Declaraciones oficiales de la Information Commissioner en relación con el caso Royal Free y el tratamiento de datos de pacientes, julio de 2017.

Suleyman, Mustafa. Declaraciones en entrevista "Big Read: What does Google DeepMind want with the NHS?", Digital Health News, 20 de marzo de 2017.