

La investigación en salud basada en datos: retos y barreras en RGPD

Jornadas REGIC 2018

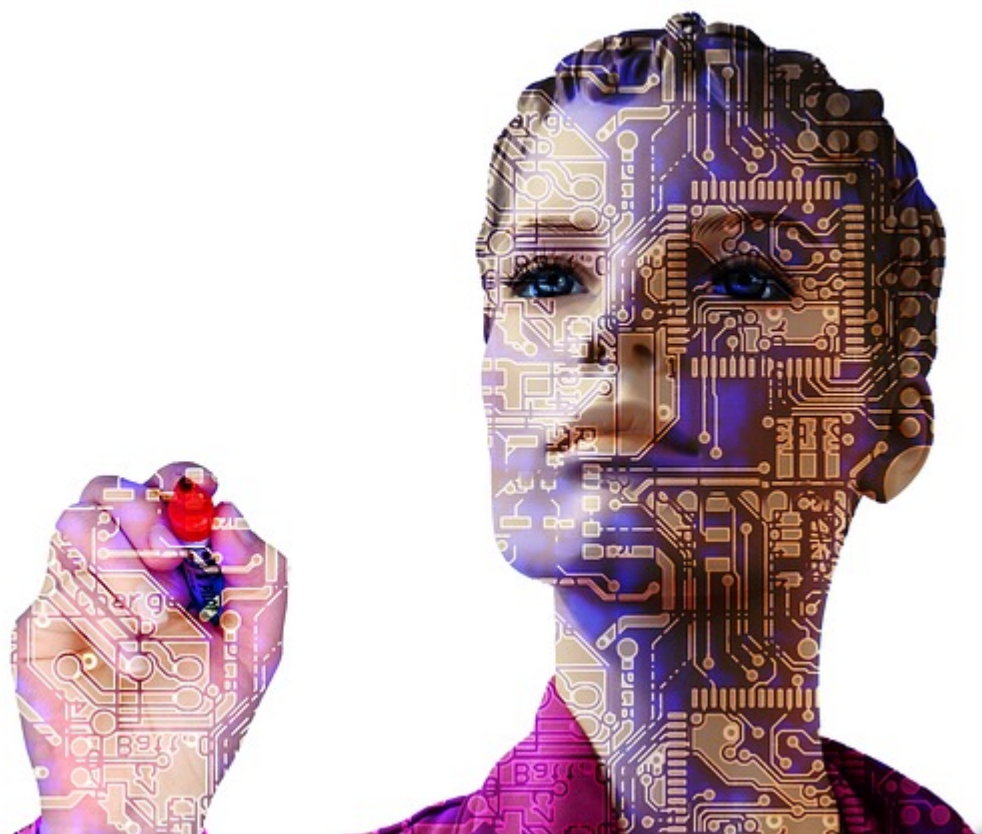
Ricard Martínez Martínez



Càtedra Microsoft
Universitat de València
**Privacitat &
Transformació Digital**

- Un modelo “constitucional”: hablamos de derechos fundamentales.
- Un modelo de “mercado regulado de privacidad”.
- Un modelo más enfocado al tratamiento de los datos personales de los europeos.
- Un cambio de mentalidad en el responsable:
 - la accountability
 - El cliente/interesado en el centro
- Un modelo abierto a los fenómenos de internet.

Tratar datos: Protegemos personas





Types of headache

MIGRAINE



HYPERTENSION



STRESS



GDPR



- El tratamiento de datos personales con fines de investigación científica es legítimo.
 - Investigación básica o fundamental
 - Investigación aplicada.
 - Investigación sector privado.
- Concepto amplio de consentimiento.
- Limitaciones en publicación.
- Los estados miembros pueden regular condiciones.
- Garantías adecuadas:
 - Minimización de datos: proporcionalidad y necesidad.
 - Pseudonimización.
 - Excepciones a los derechos.
- Legitimación de la analítica de datos.

- (33) Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, **debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica** que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.

- [52] Asimismo deben **autorizarse excepciones** a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito [...] o con fines de archivo en interés público, **fines de investigación científica** e histórica o fines estadísticos.
- [53] Las categorías especiales de datos personales que merecen mayor protección **únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para lograr** dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, [...] **fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro** que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. [...] Los **Estados miembros deben estar facultados para mantener o introducir otras condiciones**, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

- (156) El tratamiento de datos personales con (...) fines de investigación científica (...) debe estar **supeditado a unas garantías adecuadas** para los derechos y libertades del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el **principio de minimización de los datos**. El tratamiento ulterior de datos personales con fines de archivo en interés público, **fines de investigación científica** o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la **viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos)**.

- Los Estados miembros deben establecer **garantías adecuadas** para el tratamiento de datos personales con fines de archivo en interés público, **fines de investigación científica** o histórica o fines estadísticos. Debe autorizarse que los **Estados** miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, **especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento**, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar **procedimientos específicos para que los interesados ejerzan dichos derechos** si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las **medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad**. El tratamiento de datos personales con fines científicos también debe observar **otras normas pertinentes, como las relativas a los ensayos clínicos**.

- [157] Combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. [...] Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros.

- [159] (...) El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. (...) Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas.



- (...) Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable.
- Para determinar si una persona física es identificable, deben tenerse en cuenta **todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.**
- (...) deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.
- Los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable...



- Localizaciones

Investigadores del MIT²⁰ analizaron recientemente un conjunto de datos seudonimizados formado por coordenadas de movilidad espacio-temporales de 1,5 millones de personas a lo largo de un período de 15 meses en un territorio con un radio de 100 km. Este análisis les permitió singularizar al 95 % de la población mediante cuatro puntos espaciales, y a más del 50 % de los interesados con apenas dos puntos espaciales (uno de esos puntos es conocido: normalmente se trata del domicilio o la oficina), con un margen muy estrecho para la protección de la privacidad, aun teniendo en cuenta que las identidades de las personas se habían seudonimizado reemplazando sus atributos verdaderos [...] por otras etiquetas.

supuestamente anónimo y el estilo de escritura de un autor identificado. Los investigadores han determinado el estilo de escritura de más de 100 000 blogs, y hoy en día son capaces de identificar automáticamente al autor de una entrada con un margen de acierto cercano al 80 %. Se prevé que siga aumentando la precisión de esta técnica al combinarla con otras propiedades, como la localización u otros metadatos contenidos en el texto.

3.1.1.3. Defectos de la adición de ruido

A la luz de la Directiva 95/46/CE y de otros instrumentos jurídicos pertinentes de la UE, la anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación. En este proceso, los responsables del tratamiento deben considerar distintos aspectos y valorar todos los medios que puedan utilizarse «razonablemente» para la identificación de los datos (ya sea por el responsable del tratamiento o por terceros).

La anonimización implica un tratamiento posterior de los datos personales. Por tanto, debe satisfacer el requisito de compatibilidad teniendo en cuenta las circunstancias y los fundamentos jurídicos de dicho tratamiento. Por otra parte, aunque los datos anonimizados se

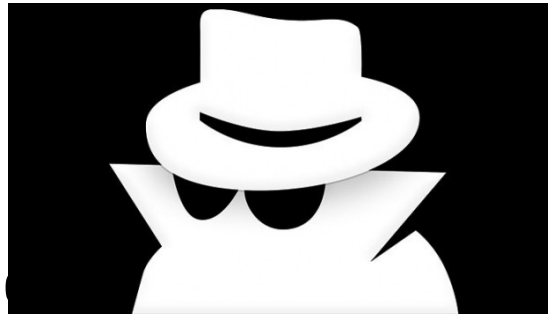
de reidentificación muy famoso es el que se llevó a cabo con la base de datos del proveedor de contenidos de vídeo Netflix. Los investigadores analizaron propiedades geométricas de esta base de datos, que está formada por más de 100 millones de valoraciones de unas 18 000 películas en una escala de 1 a 5 por parte de los usuarios. La empresa hizo pública esta base de datos tras anonimizarla con restricciones internas sobre privacidad. En concreto, eliminó todo tipo de información que pudiera identificar al cliente, excepto las valoraciones y las fechas. Se reemplazó las valoraciones mejorándolas o empeorándolas ligeramente.

Se descubrió que se podía identificar de manera unívoca el 99 % de los usuarios en el conjunto de datos usando 8 valoraciones y fechas con errores de un día como criterio de selección. Aun rebajando los criterios de selección a 2 valoraciones y un error de 3 días, se podía identificar al 68 % de los usuarios¹³.

- i) ¿Se puede singularizar a una persona?



- ii) ¿Se pueden vincular registros relativos a una persona?



- iii) ¿Se puede inferir información sobre una persona?



- El problema de la identificabilidad potencial:
 - Debe evaluarse previamente la posibilidad de reversibilidad
 - Los medios tecnológicos “no son sólo los propios” son más bien “los disponibles”.
 - Debe ser imposible la vinculación tanto para el responsable como para cualquier tercero.
 - No se trata sólo de recuperar nombre, apellidos dirección., si existe la menor posibilidad de identificabilidad potencial por singularización, vinculabilidad o inferencia: **se aplica la legislación sobre protección de datos.**
 - Si el contexto (tecnología, relación de datos con otros subconjuntos de datos...) entraña riesgos: **se aplica la legislación sobre protección de datos.**
- **LA REVERSIÓN INTENCIONAL INFRACCIÓN MUY GRAVE EN NUEVA LOPD.**
 - p) (nueva) La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

- Procedimiento N° PS/00235/2015
 - ASSEMBLEA NACIONAL CATALANA y ÒMNIMUM CULTURAL
- Procedimiento N° AP/00036/2017
 - AYUNTAMIENTO DE VALENCIA-ENCUESTA FALLERA



**Orientaciones y
garantías
en los
procedimientos de
ANONIMIZACIÓN
de datos
personales**



- Responsable del fichero y de la información.
- Responsables de Protección de Datos o Delegado de Protección de Datos o DPD.
- Destinatario o responsable del tratamiento de la información personal anonimizada.
- Equipo de evaluación de riesgos.
- Equipo de preanonimización y equipo de anonimización.
- Equipo de seguridad de la información y del proceso de anonimización: responsable de seguridad y resto del personal involucrado en tareas de seguridad de la información (operadores de seguridad, responsables de seguridad de la información departamentales o de zona, responsables de sistemas de información, etc.), comité ético, etc.
- INDEPENDENCIA DE FUNCIONES

Un esfuerzo muy exigente



- ¿Cómo aplican en la práctica el artículo 16.3 Ley 41/2002, de autonomía del paciente.
- No inclusión los datos de salud en Ley 37/2007 sobre reutilización de la información del sector público.
 - Remisión a la Ley 19/2013 de transparencia, acceso a la información pública y buen gobierno.
- Diferencias materiales significativas:
 - Investigación “interna”
 - Grupos cerrados con diversos partners.
 - Open Data “limitado”
 - Open data.

Modificación de la Ley 14/1986 General de Sanidad.

Disposición adicional decimoséptima (nueva). Tratamientos de datos de salud.

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

- a) La Ley 14/1986, de 25 de abril, General de Sanidad.**
- b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.**
- c) La 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.**
- d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.**
- e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.**
- f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.**
- g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.**
- h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.**
- i) El texto refundido de la Ley de garantías y uso racional de 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.**
- j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.**

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del 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 sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página 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 esta información por medios electrónicos a los afectados. Cuando éstos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.

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

Artículo 9. Categorías especiales de datos.

1. A los efectos del artículo 9.2 a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

El uso de datos personales pseudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse 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 personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

● Excepciones a los derechos

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:

1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.

2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.

3.º 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.

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos 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.

2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, 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.

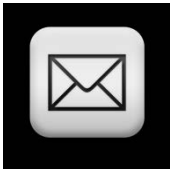
g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

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.

h) 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 los conocimientos que el Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

- ¿Tenemos un problema?
 - Yo no busco encuentro: machine learning no dirigido y cambio de finalidad.
 - La aplicación de patrones obtenidos.
 - ¿De quién son los datos? ¿Son un bien propio de la administración sanitaria?
 - ¿Open data sanitario?
- Aplicar la norma:
 - Análisis de riesgos.
 - Evaluación de impacto relativa a la protección de datos
 - Auto-regulación Reglas Internas Vinculantes para la Investigación.
 - Propuesta para entornos confinados:
 - ✓ Soft Anonymization.
 - ✓ Compromiso contractual
 - ✓ Seguridad equivalente en datos anonimizados

GR@CIAS



ricard.martinez@uv.es ;



@ricardmm; @catedramuv1



VNIVERSITAT
DE VALÈNCIA



Càtedra Microsoft
Universitat de València
**Privacitat &
Transformació Digital**