revista valenciana d'estudis autonòmics

2017 | nº 62

Redacció i administració:
Direcció General de Responsabilitat Social i Foment de l'Autogovern.
Conselleria de Transparència, Responsabilitat Social, Participació i Cooperació.
Passeig Albereda, 16. 46010 València
Tl. 96 192 23 44.
E-mail: rvea@gva.es

Distribució i suscripció:
Llibreria de la Generalitat (LliG)
C. Navellos, 8. 46003 València
Tl. 96 392 60 80. Fax 96 391 32 73

Producció:
Tórculo Comunicación Gráfica, S. A.

ISSN: 0213-2206
Dipòsit legal: V-1172-1996

Sumari

Estudis

Jurisprudència

Big data, investigación en salud y

protección de datos personales. ¿Un falso debate? Big data, investigación en salud y protección
de datos personales. ¿Un falso debate? Big data, investigación en salud y protección de datos per-
sonales. ¿Un falso debate? Big data, investigación en salud y protección de datos personales. ¿Un
lso debate? Big data, investigación en salud y protección de datos personales. ¿Un falso debate? Big data,
vestigación en salud y protección de datos personales. ¿Un falso debate? Big data, investigación en salud y
rotección de datos personales. ¿Un falso debate? Big data, investigación en salud y protección de datos per-
nales. ¿Un falso debate? Big data, investigación en salud y protección de datos personales. ¿Un falso debate?
g data, investigación en salud y protección de datos personales. ¿Un falso debate? Big data, investigación
n salud y protección de datos personales. ¿Un falso debate? Big data, investigación en salud y protección de
tos personales. ¿Un falso debate? Big data, investigación en salud y protección de datos personales. ¿Un
lso debate? Big data, investigación en salud y protección de datos personales. ¿Un falso debate? Big data,

Big data, investigación en salud y protección de datos personales. ¿Un falso debate?

Texto de:
Ricard Martínez Martínez[1]
Director de la Cátedra de privacidad
y Transformación Digital Microsoft-Universitat de València

1. Este trabajo se enmarca en el Proyecto de Investigación del MINECO «El impacto del nuevo Reglamento Europeo de Protección de Datos: análisis nacional y comparado». Referencia de Proyecto DER2015-63635-R.

I. Introducción

El impacto de las tecnologías de la información en los tratamientos de datos de salud en el contexto de la investigación ha ocupado un lugar preeminente en el debate científico y jurídico reciente. Tienen la consideración de datos sujetos a especial protección en el conjunto de la normativa sectorial aplicable[2]. El Reglamento general de protección de datos[3] los integra junto a los datos genéticos en las categorías especiales de datos personales. En origen, esta consideración deriva de la voluntad de evitar la discriminación y las prácticas eugenésicas conocidas en nuestra experiencia histórica[4]. El tratamiento de datos de salud puede impactar de manera particularmente significativa en la esfera de derechos de las personas. Así, la información sobre el estado de salud no sólo repercute sobre el derecho a la intimidad, sino que puede afectar en ámbitos como el acceso al empleo, al crédito o al aseguramiento[5].

Sin embargo, la repercusión de las tecnologías de la información puede ser altamente positivo y es necesario abordar su impacto en la salud desde una nueva óptica. Ello obliga a renunciar a un enfoque apriorístico en el que cualquier tratamiento de datos de salud es concebido negativamente. Y este tipo de aproximación no está siendo infrecuente cuando

2. Convenio 108/1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, la 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 la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

3. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

4. Antes y después de la Segunda Guerra Mundial muchas personas fueron discriminadas por razón de su raza o enfermedad aplicándose en distintos países políticas eugenésicas que alcanzaron su más terrible expresión durante el III Reich. ROMAÑACH CABRERO, Javier y ARNAU RIPOLLÉS, Soledad «La visión de la eugenesia en el mundo occidental» en CASABÁN MOYA, Enric (Ed.): *XVI Congrés Valencià de Filosofia*, Universitat de Valencia, València, 2006, pág. 334 y ss.

5. La Memoria explicativa del Convenio 108/1981 subraya que el tratamiento de los datos sensibles puede ser lesivo por sí mismo « 43. While the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests. Categories of data which in all member States are considered to be especially sensitive are listed in this article». (Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data).

hablamos de Big data[6]. El diseño de proyectos para poner a disposición de la comunidad científica volúmenes masivos de datos de salud mediante técnicas de anonimización ha sido puesto en cuestión de modo significativo por la comunidad jurídica.

No se discute el deber de vigilancia que corresponde a la Ética y el Derecho. Sin embargo, la protección de datos no es un derecho de naturaleza absoluta y debe ser objeto de contraste con otros bienes y valores constitucionales relevantes. El empleo de Big data en el ámbito de la investigación, va a encontrar su sustento en la libertad de creación científica del artículo 20 de la Constitución Española. Y no conviene olvidar que nuestra Carta reconoce el derecho a la protección de la salud y la considera un elemento esencial en las políticas de bienestar. En última instancia, la investigación en salud y la política sanitaria se ordena a la preservación del bien constitucional supremo del derecho a una vida digna.

Si admitimos que Big data puede revolucionar la medicina, el debate debería abandonar cierto maniqueísmo dualista[7] para centrarse en identificar «el cómo», y en entender que desde el punto de vista de los investigadores el empleo de esta nueva metodología constituye un im-

6. El Information Commissioner's Office ha captado con precisión el balance entre riesgos y beneficios:

« 32. How Big data is used is an important factor in assessing fairness. Big data analytics may use personal data purely for research purposes, eg to detect general trends and correlations, or it may use personal data to make decisions affecting individuals. Some of those decisions will obviously affect individuals more than others. Displaying a particular advert on the internet to an individual based on their social media 'likes', purchases and browsing history may not be perceived as intrusive or unfair, and may be welcomed if it is timely and relevant to their interests. However, in some circumstances even displaying different advertisements can mean that the users of that service are being profiled in a way that perpetuates discrimination, for example on the basis of race. Research in the USA suggested that internet searches for «black-identifying» names generated advertisements associated with arrest records far more often than those for «white-identifying» names. There have also been similar reports of discrimination in the UK, for instance a female doctor was locked out of a gym changing room because the automated security system had profiled her as male due to associating the title 'Dr' with men.»

INFORMATION COMMISSIONER'S OFFICE: *Big data, artificial intelligence, machine learning and data protection. Version: 2.0*, ICO, 2017, pág. 21. Disponible en https://ico.org.uk/for-organisations/guide-to-data-protection/

7. Con independencia de que se apuesta por la ponderación es significativo el título y subtítulo del artículo de SERRANO, Mercedes: «Big data o la acumulación masiva de datos sanitarios. Derechos en riesgo en el marco de la sociedad digital» en *DS: Derecho y salud,* Vol. 25, Nº. Extra 1, 2015, págs. 51-64. Aunque la autora matiza su punto de vista se suma a aquellos que enjuiciaron negativamente el proyecto VISC+.

perativo moral[8]. Debemos ser capaces de comprender que la transformación digital supone un cambio cualitativo muy relevante superando el empleo de métodos puramente estadísticos y permitiendo una visión holística del ser humano. En 2017 el paciente es bastante más que una persona doliente que narra síntomas, o que un cuerpo objeto de análisis para determinar la dolencia y prescribir medicación. La tecnología permite una visión integral del sujeto que abarca su dimensión genómica, su historia clínica completa, el contexto socioeconómico, y el conjunto de datos disponibles sobre su enfermedad en el sistema de salud nacional y de otros países. El Internet de los Objetos facilita un seguimiento integral mediante teleasistencia y telemonitorización, y permite incidir en la vida cotidiana del paciente orientando su conducta y convirtiéndolo en partícipe del proceso asistencial y en elemento determinante para una buena medicina preventiva. La información acumulada por los sistemas de salud, y la que producen miles de periféricos conectados en tiempo real retroalimenta bases de datos esenciales para la investigación. En este contexto, las herramientas de análisis que proporciona Big data acortan los tiempos en los procesos de análisis de la información y ofrecen nuevas aproximaciones. Y todo ello, puede conducir a un contexto de investigación acelerada, de medicina asistida y participativa.

Este escenario, hace mucho más compleja la tarea del jurista. Muy tempranamente se ha puesto de manifiesto cómo una comprensión plana del derecho a la protección de datos puede comportar problemas[9]. Si reducimos la aplicación al mero silogismo, en presencia de los datos de salud, automáticamente entran en juego un conjunto de límites y prohibiciones que pueden generar un contexto particularmente desfavorable para el avance de la ciencia. Por ello, se ha defendido la necesidad de desarrollar un enfoque cualitativo que sea capaz de poner en valor tanto los riesgos como los beneficios derivados del tratamiento de información personal, e

8. Tim Kelsey, director de pacientes e información del NHS británico afirmaba en 2015 sobre el uso de estas técnicas: «Urgent action is a moral imperative. Patients are put at risk where paper is the currency of clinical practice. The evidence is clear that electronic prescribing systems which support clinicians ensure the right medicine is provided to the right person in the right quantity halve medication errors, yet only 14% of NHS hospital trusts currently deploy these systems.
KELSEY Tim: «Blog NHS. (2015). Urgent action is a moral imperative». Disponible en https://www.england.nhs.uk/2015/09/tim-kelsey-11.

9. Esta fue uno de los argumentos medulares de la tesis doctoral defendida en 2004. Véase MARTÍNEZ MARTÍNEZ, Ricard: *Una aproximación crítica a la autodeterminación informativa*. Civitas, Madrid, 2004 y MARTÍNEZ MARTÍNEZ, Ricard: «El derecho fundamental a la protección de datos: perspectivas», en IDP: *Revista de Internet, Derecho y Política*, Nº. 5, 2007

integrar la interpretación jurídica en el marco del preciso contexto social, económico y tecnológico en el que se desarrollan los tratamientos[10].

¿Cómo valorar el caso de un sujeto geolocalizado y monitorizado a través de una pulsera, un teléfono móvil y una videocámara? Creo que nadie objetará las ventajas que puede proporcionar la monitorización de un paciente crónico coronario y las posibilidades que puede ofrecer la detección precoz de un infarto a la hora de utilizar el medio más idóneo para la recogida del enfermo, para su transporte, y para su viaje y tratamiento posterior. Del mismo modo ¿por qué razón deberíamos por principio desconfiar del uso de las tecnologías de la información y de Big data en la investigación?[11]

El objetivo que debe perseguir el jurista, y al que responde este artículo, consiste en tratar de poner en valor, por un lado la relevancia de la investigación en salud, y por otro evaluar su impacto en la esfera de derechos de los pacientes. Resulta necesario, definir las condiciones jurídicas que faciliten la investigación y salven vidas sin lesionar gravemente los derechos de las personas. Los investigadores en el ámbito de la salud, los

10. Véase mi intervención en el III Congreso Internacional sobre Protección de Datos de la Cátedra Google de Privacidad. MARTÍNEZ MARTÍNEZ, Ricard: «Protección de datos y desarrollo tecnológico en un mundo global», en el *BLOG LOPD y Seguridad*, Disponible en http://lopdyseguridad.es/proteccion-de-datos-y-desarrollo-tecnologico-en-un-mundo-global/.

11. En este sentido resulta un significativo ejemplo el trabajo de Yasmina Soto «Datos masivos con privacidad y no contra privacidad». Se esperaría del abstract un juicio mínimamente ponderado. Sin embargo el tono lo da esta afirmación: « La capacidad actual para almacenar y procesar datos sitúa a la mayoría de la población frente a enormes riesgos volviendo ineficaces los principales mecanismos técnicos y legales que existen actualmente para proteger la privacidad. «Habrá menos intimidad, menos respeto a la vida privada, pero más seguridad», dicen las autoridades. De la mano de este imperativo se instala un régimen de seguridad al que, podemos calificar de «sociedad de control». Actualmente puede decirse que toda la sociedad funciona según el principio del «panóptico»,». A la autora le preocupa PADRIS, sucesor de VISC+, ambos proyectos relacionados con la explotación de datos masivos anonimizados del Sistema Catalán de Salud, en la medida en la que «Empresas que, probablemente, utilizarían los datos para venderlos y obtener un beneficio propio, simplemente deben disponer de los medios para hacerlo y tener interés en rentabilizar la información». Además puesto que en su opinión la normativa que pretende ser implacable tanto en la Unión Europea como en España, «con la vertiginosa evolución tecnológica, en un breve transcurso de tiempo, ha acaecido obsoleta» parece que hay poco qué hacer. No encontrará el lector en este artículo ni un solo dato empírico, ni una mera referencia a las garantías que ofrece la Generalitat, ni al informe sobre cumplimiento de la Autoridad Catalana de Protecció de Dades ni a los compromisos asumidos por la entidad gestora AQUAS para el control ético y jurídico. Agitar la opinión pública, y defender el derecho fundamental a la protección de datos desde el prejuicio y la bandera de un mundo orwelliano es tremendamente sencillo. Sin embargo, puede que los enfermos crónicos, los diabéticos, o los que padecen enfermedades raras no compartan la opinión. Puede que la autora tenga razón: pero no lo prueba. Si los juristas defendemos que la nuestra es una «Ciencia» no podemos jugar en el territorio de la mera opinión, nuestro deber es ceñirnos a las pruebas y ofrecer soluciones viables desde un juicio realista y ponderado desde el conocimiento material. Véase, SOTO, Yasmina: «Datos masivos con privacidad y no contra privacidad», en *Revista de Bioética y Derecho. Dossier Monográfico del XIII Congreso Mundial de la International Association of Bioethics*, núm. 40, 2017, págs. 101-114.

operadores privados, como farmacéuticas y aseguradoras, los reguladores, y los estudiosos del Derecho debemos tener en cuenta que en esta aventura existe un valor central y prevalente: el paciente.

II. Qué es Big data y cómo funciona en salud

No es posible entender las implicaciones que desde un punto de vista jurídico y material plantea el uso de Big data sin una somera descripción de estas tecnologías. El constante crecimiento en las capacidades de procesamiento y almacenamiento que anunció Gordon Moore, no alcanza a superar los severos límites que impone analizar informaciones complejas por su variedad o volumen[12]. Estas carencias vinieron a ser resueltas primero con el empleo de grandes ordenadores para el cálculo computacional y a partir de los años noventa del pasado siglo mediante sistemas de computación distribuida (GRID). Esta tecnología evolucionó hasta el conocido como Cloud Computing o computación en la nube[13]. Hoy podemos conectar clústeres de miles de ordenadores y asociar estas «granjas» en todo el mundo trabajando asociativamente, lo que incrementa de modo significativo las posibilidades tanto de almacenamiento como de procesamiento de información[14].

Superado el problema de capacidad y proceso se exige ser capaces de analizar múltiples fuentes de información con estructuras y contenidos diferenciados. Aquí es donde entra en juego Big data, definido como «un paradigma para hacer posible la recopilación, el almacenamiento, la gestión, el análisis y la visualización, potencialmente en condiciones de tiempo real, de grandes conjuntos de datos con características heterogéneas»[15].

Por tanto disponemos de tecnologías que facilitan el análisis masivo de información caracterizadas por lo que se han denominado las 3V del Big data: velocidad, variedad y volumen. Esta tecnología permite analizar un volumen masivo de datos, con una enorme velocidad en la recogida y procesado de la información y al mismo tiempo puede afrontar el análisis de

12. Más adelante se incluyen algunos ejemplos relevantes. En todo caso, a nivel global véase «What Happens in an Internet Minute in 2017?» Disponible en http://www.visualcapitalist.com/happens-internet-minute-2017/

13. Sobre los aspectos jurídicos de esta tecnología véase, MARTÍNEZ MARTÍNEZ, Ricard (ed.): Derecho y cloud computing. Aranzadi, Cizur Menor (Navarra), 2012.

14. Véase CABALLERO, Rafael y MARTÍN, Enrique: *Las bases de Big Data*. Catarata, Madrid, 2015.

15. Directiva UIT-T Y.3600 de la Unión Internacional de Telecomunicaciones.

una gran variedad de datos. Adicionalmente se unen por algunos teóricos dos V adicionales, la correspondiente a la posibilidad de crear valor en el uso de estas tecnologías[16], y en segundo lugar la llamada veracidad. Es decir, la capacidad de obtener información verídica y útil para la toma de decisiones, aunque evidentemente esta última V es más bien discutible.

No obstante debemos entender que no se trata sólo de disponer de grandes volúmenes de datos sino de herramientas que permitan obtener información útil. Para ello se hace necesario comprender algunas características adicionales[17]. Se ha definido Big data como una «estadística del todo». Es un entorno no constreñido por la necesidad de elegir una muestra, lo que al menos teóricamente permite eliminar el sesgo que comporta toda elección. La segunda cuestión relevante deriva de la capacidad de combinar el conjunto de datos que usualmente nos parecería natural, o aquellos de los que disponemos, con conjuntos o subconjuntos de datos aparentemente distantes o distintos de los que habitualmente utilizaríamos. Ello permite responder a preguntas del tipo ¿sería posible ofrecer seguros de salud en función del análisis de las preferencias alimentarias manifestadas por los usuarios y por sus redes de amigos en espacios sociales de internet?[18].

En tercer lugar, entran en juego un conjunto de desarrollos, denominados *machine learning*, que permiten que las máquinas analicen grandes volúmenes de datos a partir de determinados algoritmos de programación. Algunos de ellos supervisados, es decir con reglas de aprendizaje predefinidas de modo que se ha programado tanto el *input* como el esperable *output*. Pero también los hay no supervisados en los que el programa se diseña para que analice conjuntos de datos e identifique patrones[19]. *Ma-*

16. Véase Porter, Michael E: «What Is Value in Health Care?» en *The New England Journal of Medicin*e, December 23, 2010, págs. 2477-2481. Y MARJANOVIC Sonja, GHIGA,Ioana MIAOQING Yang and KNACK Anna: *Understanding value in health data ecosystems: A review of current evidence and ways forward*. Santa Monica, CA: RAND Corporation, 2017.Disponible en https://www.rand.org/pubs/research_reports/RR1972.html.

17. Para un análisis muy comprensible véase MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth: *Big Data*. Turner, Madrid, 2013.

18. Las respuestas que se ofrecen desde los expertos parecen ser afirmativas hasta el punto de afirmar que el dato más sensible es el código postal. Así lo afirma el prestigioso investigador Julio Mayol. Véase este debate breve en Twitter en el que afirma que las variables de código postal y educación están por delante de la genética a la hora de definir expectativas de vida. Disponible en https://twitter.com/juliomayol/status/876341254644269057.

19. Véanse ejemplos en el blog divulgativo de Phillips sobre innovación «Machine Learning: Inteligencia Artificial aplicada al diagnóstico médico». Disponible en http://www.compartein-novacion.philips.es/innovacion-en-healthtech/articulos/machine-learning-inteligencia-artificial-aplicada-al-diagnostico-medico. Y en BBVA «Las cinco tribus del 'machine learning'». Disponible en https://www.bbva.com/es/las-cinco-tribus-del-machine-learning/

chine learning es el soporte necesario para que, a través de herramientas de inteligencia artificial las inferencias obtenidas a partir de los modelos de análisis, sirvan para predecir y anticipar eventos futuros. La cuestión, es que la necesidad de programar uno o diversos algoritmos ordenados orientar nuestro análisis define casi una aporía. Si hasta hoy la investigación partía de una premisa que buscaba la confirmación de una hipótesis, el resultado práctico de un análisis de Big data puede comportar un resultado inesperado y cuya razón última no alcancemos a identificar. Es decir tenemos el «qué», pero se nos escapa el «por qué». Finalmente hay que sumar al fenómeno varios elementos esenciales que están incidiendo en el uso de Big data[20]:

- El uso de los llamados datos masivos interactúa con realidades en red, es funcional al complejo entramado en red que caracteriza no sólo a las redes sociales en todas sus dimensiones, sino también a múltiples fenómenos de orden físico.
- Uno de los resultados determinantes de este tipo de herramientas consiste en ofrecer algo más que los *datawharehouse*, o los sistemas de *bussiness intelligence*, no ofrece resultados estáticos, es capaz de proporcionar patrones dinámicos. Y ello tanto para identificar tendencias, como desviaciones. De ahí que el Big data pueda ser una herramienta indispensable para el control del fraude en el uso de servicios o beneficios vinculados a la salud...
- El ejemplo que acabo de citar plantea sólo una parte de una compleja ecuación. Big data no sólo mira al pasado, Big data se asocia a la predictibilidad y apunta al futuro.

Precisamente por ello, tanto la obtención del patrón, como sobre todo su aplicación pueden generar dudas esenciales de índole ética y jurídica[21].

20. Originalmente referidos en otro trabajo. MARTÍNEZ MARTÍNEZ, Ricard: «Ética Ética y privacidad de los datos», en *Monográfico sobre Big Data de la Revista FRA* nº14 (Diciembre 2015), págs. 86-91. Intervención disponible en video en http://www.fundacionareces.tv/watch/bigdata?as=-53d296758d85927a508b46dc.

21. MARTÍNEZ MARTÍNEZ, Ricard: «Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos.», en *Revista Dilemata*, núm. 24, 2017, págs. 151-164. Disponible en http://www.dilemata.net/revista/index.php/dilemata/article/view/412000105

1. Fuentes de información

En los últimos decenios los sistemas de salud han generado grandes volúmenes de datos de todo tipo[22]. En este sentido, el informe «Big data en salud digital» expone con detalle cómo los registros electrónicos de salud y los registros personales de salud pueden contener información particularmente relevante[23]. Los primeros contribuyen a facilitar la tarea de los profesionales para prestar la mejor atención posible proporcionando información para evaluar la condición de salud del paciente[24]. Los registros personales pueden incluir tanto el resumen de la información e historia clínica del paciente como la administrativa, e información adicional como la procedente de *wearables*. Además facilitan la interacción del paciente con el Sistema de Salud ofreciéndole la posibilidad de acceder a sus registros; ver resultados de sus pruebas; o renovar prescripciones farmacéuticas. El citado informe ofrece un interesante resumen de fuentes relevantes para Big data en salud[25]:

22. Eduard Martín refiere la existencia de nuevas tipologías de datos: «Los datos «nuevos» o de transición rápida: que son los datos que no podemos obtener fácilmente a través de la observación humana, ya sea por física pura, ya sea por desconocimiento o incapacidad. Muchas veces estos datos mutan rápidamente, son difícilmente relacionables fuera de su propio contexto, y son susceptibles de «amontonarse» en grandes cantidades. Estos datos, además, no se pueden poner fácilmente en relación, y son susceptibles de grandes cambios(..)

La realidad del que conocemos como big data es la capacidad de manejar grandes cantidades de datos de diferente índole como hemos visto, pero también la potencia de poder ponerlos en conexión —independientemente de su naturaleza física— para que nos aporten «información» de valor añadido».

MARTIN LINEROS, Eduard: «El trinomio dato-información-conocimiento» en VV.AA: *Manual sobre utilidades del big data para bienes públicos*. Entimema, Madrid, 2017. Págs. 38 y 44.

23. San Segundo Encinar, Jose María (Dir.). *Big data en salud digital*. Fundación Vodafone, MINETAD, RED.ES, Madrid, 2017, p.9.

24. Entre otras funcionalidades despliegan las siguientes:
- Los registros de información e historia clínica incluyen, entre otros, el registro de la historia médica, los síntomas, los resultados de los tratamientos terapéuticos, las constantes vitales, las imágenes radiológicas, los parámetros médicos básicos, los test y pruebas o las razones de la cita médica.
- Los sistemas de ayuda al diagnóstico incluyen funcionalidades como los sistemas de ayuda al diagnóstico sobre contraindicaciones; el registro de las interacciones en medicamentos o guías clínicas y mejores prácticas.
- La gestión administrativa del paciente incluye aspectos como el registro de datos administrativos o de facturación.
- Los aspectos de apoyo farmacológico incluyen tanto los listados de fármacos como el registro de prescripciones.

SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). *Big data en...* Op. Cit. Pág. 9.

25. SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). *Big data en...* Op. Cit. Pág. 16.

- **La web y las redes sociales (social media)**[26]: la generación e interacción de datos de social media como Facebook, Twitter, o Linkedin, además de la información de sitios web de salud o las aplicaciones de *smartphones*.
- **Los datos de máquina a máquina:** la información proveniente de las lecturas de los sensores, medidores y otros dispositivos[27].
- **Las grandes transacciones de datos:** reclamaciones de atención médica y otros registros de facturación cada vez más disponibles en formatos semiestructurados y no estructurados.
- **Los datos biométricos:** huellas dactilares, genéticos, escáner de retina, rayos X y otras imágenes médicas, la presión arterial, el pulso y lecturas de oximetría, de pulso y otros tipos similares de datos.
- **Los datos generados por los seres humanos:** datos no estructurados y semiestructurados, tales como registros médicos electrónicos (Electronic Medical Records, EMR, por sus siglas en inglés), notas de los profesionales sanitarios, correos electrónicos y documentos en papel[28].

Por otra parte los expertos apuntan a un nuevo modo de concebir los datos disponibles para cualquier sistema. Históricamente, en el mundo de las bases de datos relacionales, las organizaciones miraban hacia adentro. *Data Wharehouse* y posteriormente *Business Intelligence*, permitían el análisis y explotación de los datos de la organización. Hoy disponemos de la posibilidad de cruzar los datos con fuentes internas no relacionales y con fuentes externas de todo tipo. Por ejemplo, las herramientas de telemedicina, o el propio paciente y su entorno social[29]. A todo ello pueden

26. VAN DER GOOT Erik, TANEV Hristo y LINGE Jens P.: «Combining Twitter and Media Reports on Public Health Events in MedISys», en *International World Wide Web Conference*, Seul, 2014. Disponible en http://www2013.wwwconference.org/companion/p703.pdf

27. GEMO Monica, LUNARDI Davide y TALLACCHINI Mariachiara: *Wearable Sensors and Digital Platforms in Health: empowering citizens through trusted and trustworthy ICT technology. TRUDI Deliverable 3.1.* Scientific and Technical Research Reports Publications, Office of the European Union, 2015.

28. Basta con verificar el contenido de la historia clínica, de acuerdo con la Ley 41/2002 reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, para entender el volumen de información disponible en nuestro sistema de salud. Si a ello añadimos, la información relacionada con las recetas médicas, electrónicas o no, análisis y pruebas diagnósticas o ensayos clínicos, puede fácilmente entenderse que el volumen de información disponible es sencillamente inabarcable a una escala no automatizada.

29. Ester Dyson señala que «La Salud Digital depende, al menos, de dos tipos de datos: Big data, para asociar las diferentes vivencias, genotipos, fenotipos y otros datos con las enfermedades posteriores o los tratamientos con sus curas. Y los datos menores, para tratar a los individuos de forma personal, entendiendo sus circunstancias y actitudes... y parámetros de salud. (...)Aunque las herramientas digitales per se no basten ¡nosotros también necesitamos a las personas! pueden ser útiles para todas estas tareas, sobre todo si usan los «datos menores» que permiten aprovechar Inteligencia Artificial por detrás para entender la situación y el marco mental de cada persona». FUTURE TRENDS FORUM: *Salud digital.* Madrid 2016, pág. 11. Disponible en https://www.fundacionbankinter.org/ftf/tendencias/salud-digital.

añadirse datos no necesariamente personales muy relevantes, como por ejemplo variables climáticas, demográficas, económicas y sociales. Ello ofrece por primera vez en la historia una mirada holística que va más allá del enfermo que narra su dolencia[30].

2. Aplicaciones tecnológicas a la medicina

Las tecnologías de la información y las comunicaciones han proporcionado las herramientas necesarias para la provisión a distancia de servicios de salud[31]. Estos servicios responden a tres tipologías; 1) servicios de asistencia remota; 2) servicios de gestión administrativa; 3) servicios de telesalud no clínicos, e integran distintas prestaciones. Algunas suponen la digitalización de servicios tradicionales, como el diagnóstico y el seguimiento. Otras han incorporado en los últimos años nuevos modelos de relación con el paciente: la simplificación de la gestión administrativa, la desaparición del papel, o campañas de prevención y concienciación mediante el teléfono

30. En 2015 un informe de la Fundación Innovación Bankinter señalaba cómo «El sistema sanitario es otro gran vertebrador que está notando la llegada del Big data. De momento lo hace como un espectador más, como si la cosa no fuera con él. Pero mientras actúa como convidado de piedra todo a su alrededor se mueve y **cambian las relaciones entre pacientes, cuidadores y profesionales sanitarios** dentro y fuera del sistema, en las comunidades de proximidad (físicas o cibernéticas) y en la unidad familiar. También lo hace el autocuidado a nivel individual, con la toma de conciencia de nuestros hábitos y de cómo podríamos mejorarlos a partir de aplicaciones y dispositivos de medición de actividad y de marcadores de salud. Aunque no quiera darse cuenta, el sistema sanitario ya se está reinventando».
FUTURE TRENDS FORUM: *Big data. El poder de los datos (Resumen ejecutivo).* Fundación Innovación Bankinter, Madrid 2014, pág. 11. Disponible en https://www.fundacionbankinter.org/ftf/tendencias/bigdata.

31. La OMS define la telemedicina como «la prestación de servicios de atención de la salud, donde la distancia es un factor crítico, por todos los profesionales de la salud que utilizan tecnologías de la información y de la comunicación para el intercambio de información válida para el diagnóstico, tratamiento y prevención de enfermedades y lesiones, la investigación y la evaluación, y para la formación continuada de los profesionales de la salud, todo en aras de avanzar en la salud de los individuos y sus comunidades»
OMS. *Global Observatory for eHealth series-Volume 2: Telemedicine; opportunities and developments in member States.* Washington: OMS, citado en SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). Big data en... Op. Cit. pág. 10.

móvil[32]. Pero la telemedicina no es el único ámbito que ha experimentado una revolución según el Informe sobre Big data en salud[33]:

> La combinación de la genómica y el Big data apunta a que puede convertirse en una nueva revolución de la salud. (...)
> Estos cambios pueden ayudar a mejorar la toma de decisiones clínicas. Por ejemplo, mediante la aplicación de técnicas de Big data se puede predecir con un mayor nivel de certeza si un individuo es más propenso o no a desarrollar una patología en función de sus factores genéticos, permitiendo anticiparse al desarrollo de la misma. Por tanto, se tendería al nuevo paradigma de medicina preventiva, seleccionando, mediante la fármaco-genética, las medicaciones más eficaces para los pacientes.
> Por ejemplo, se calcula que, al ritmo actual, la cantidad de datos de genómica producidos diariamente se duplicará cada 7 meses. En 2025, esa cifra oscilará entre 2 y 40 exabytes por año, estima el equipo, en función de la tasa de duplicación y, en ese mismo año, se espera que 1.000 millones de personas tengan sus genomas completos secuenciados (Schatz, 2015).

Si atendemos a las consideraciones del Informe que se viene citando nos espera una verdadera revolución en ámbitos como la investigación clínica[34], la epidemiología, la monitorización y seguimiento de enfermos crónicos, la operativa clínica, y la farmacología[35].

---

32. El Informe sobre Big data y Salud destaca que «son las propias características del uso de dispositivos móviles las que pueden suponer un cambio radical en el modo en que se obtiene, almacena, procesa y transmite la información médica, permitiendo tanto la puesta en práctica de modelos de atención hasta ahora inexistentes, como las muchas oportunidades de optimización que presenta en aquellos preexistentes. De la misma manera, el uso de mHealth permite una recogida masiva de datos que abre las puertas tanto a una mayor calidad y cantidad de información que resulta básica para desarrollar modelos más eficientes y efectivos de medicina basada en la evidencia, como al análisis masivo de datos mediante tecnologías Big data».
SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). *Big data en...* Op. Cit. Pág 27.

33. SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). *Big data en...* Op. Cit. Pág. 29.

34 El Informe cita distintos proyectos relevantes a nivel Europeo de los que aquí se citan algunos:
- Plataforma para una vida más saludable (DAPHNE).
- Uso de nuevas tecnologías para investigación médica avanzada (Linked2Safety).
- MediSYS: la Comisión Europea ha desarrollado el sistema «MediSys» como una herramienta para escanear y buscar información con el objetivo de reforzar la red de vigilancia de enfermedades transmisibles y la detección temprana de las actividades bioterroristas.

Y también en España:
- SMUFIN (Somatic Mutations Finder) es un nuevo método basado en Big data desarrollado por un equipo de investigadores españoles y publicado en Nature Biotechnology que hace posible la detección rápida y precisa de los cambios genómicos causantes de la aparición y progresión de tumores.
- Help4Mood: su objetivo es crear una herramienta de apoyo al tratamiento de la depresión mediante el seguimiento del paciente durante sus tareas diarias con una serie de sensores no intrusivos.

SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). *Big data en...* Op. Cit. Págs. 36 a 38.

En la misma línea apuntan las previsiones de los expertos convocados por el Future Trends Forum en 2016 para reflexionar sobre salud digital. Para ellos.

> «la digitalización de la salud pretende erigirse en nuevo paradigma que, a través de la innovación tecnológica, mejore el funcionamiento de los sistemas de salud donde el paciente pueda gestionar su salud con un nuevo modelo de interacción entre el médico y el paciente y entre el propio paciente y el sistema».

Entre otras tendencias se señaló el uso de avatares, -representaciones gráficas tridimensionales de los pacientes-, el amplio uso de la información genética en un contexto de medicina preventiva, la implicación con el paciente en el sentido de incidir en su conducta y de su empoderamiento,

---

35. McKinsey habla de una revolución en el sistema de salud norteamericano aceleradora del valor y la innovación que puede plantear beneficios desde el punto de vista del gasto ofreciendo información estratégica en el análisis profundo de la distribución del gasto farmacéutico. Puede contribuir significativamente al desarrollo de herramientas diagnósticas y la elección de dianas terapéuticas. Adicionalmente podrá contribuir al examen masivo de comportamientos del paciente ayudando a reorientar su dieta y hábitos de vida. Finalmente, la apertura de los datos del sistema de salud debería potenciar la innovación y la investigación con un volumen económico potencial de 300.000 a 450.000 millones de dólares de reducción del gasto. Véase KAYYALI Basel, KNOTT David, y Steve KUIKEN Van: «The big-data revolution in US health care: Accelerating value and innovation» en McKinsey Healthcare Systems & Services Practice, junio 2013. Disponible en http://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-big-data-revolution-in-us-health-care.
La misma compañía explica cómo Big data revolucionará la investigación de la industria farmacéutica en un escenario en el que el modelo predictivo aplicado a los procesos biológicos y los medicamentos será más sofisticado. Se acelerará e intensificará la predictividad sobre el funcionamiento de determinadas moléculas y la posibilidad de obtenerlas y modularlas. Se multiplicarán las fuentes que sirvan para identificar potenciales pacientes dispuestos a colaborar en ensayos clínicos, incluidas las fuentes sociales. Los ensayos se monitorizarán en tiempo real para identificar rápidamente síntomas relacionados con su seguridad y condiciones operativas que requieran alguna acción para evitar problemas significativos y potencialmente costosos como efectos adversos. El universo de datos disponible crece, las fuentes se multiplican, y con ello las rigideces vinculadas a conjuntos de datos limitados desaparecen. Todo ello comportaría una mayor velocidad en la investigación, el ensayo y la transferencia, una apertura a la colaboración externa más allá del estrecho marco de un único equipo y a la interacción público/privado. Acelerar los procesos de decisión basados en datos generará nuevos modelos de investigación y nuevos procesos de descubrimiento, se asociará a nuevos sensores como los *smartphones* y las aplicaciones móviles y podrá afinar el foco a partir de evidencias obtenidas del mundo real, elevará la eficiencia de los ensayos clínicos y contribuirá a una mejor gestión del riesgo y la seguridad de los mismos. Véase, CATTELL Jamie, CHILUKURI Sastry y LEVY Michael: «How big data can revolutionize pharmaceutical R&D» en *McKinsey Center for Government*, octubre 2013. Disponible en http://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/how-big-data-can-revolutionize-pharmaceutical-r-and-d.
En idéntico sentido Lita Sans en su Intervención en el Future Trends Forum en 2014 ponía un ejemplo muy gráfico «Watson de IBM, en asociación con la facultad de medicina de Baylor, ha descubierto seis proteínas que modifican la p53—una proteína fundamental en muchos casos de cáncer—, lo cual les ha llevado a descubrir un fármaco nuevo en cuestión de semanas. Esto es destacado, teniendo en cuenta que en los últimos 30 años, la media en la comunidad científica ha sido de un descubrimiento de una proteína diana de este tipo al año». FUTURE TRENDS FORUM: *Big data. El poder de los datos*. Fundación Innovación Bankinter, Madrid 2014, pág. 17. Disponible en https://www.fundacionbankinter.org/ftf/tendencias/bigdata.

y el uso de la inteligencia artificial para la comprensión de enfermedades y diagnósticos complejos. Si bien en este último caso entendiendo que « que las máquinas cognitivas ejercerán en un futuro como asistentes virtuales de diagnóstico médico, y en ningún caso sustituirían la labor de los profesionales»[36]. También se aportaron en este foro cuantificaciones sobre el volumen de datos que se manejan en salud por cada paciente:

- Datos clínicos: 1Tb, 10% de los resultados provienen de la atención sanitaria.
- Datos genómicos: 6Tb, suponen un 30%.
- Otros: 60% se relaciona con datos heterogéneos: medios sociales, datos de smartphones, huella digital.

En opinión de los expertos el problema reside en que el crecimiento del gasto en salud en relación con el PIB es insostenible ante el incremento de las enfermedades crónicas y la digitalización de la salud puede ser clave para conseguir una atención sanitaria de alta calidad a un precio asequible. Puede apreciarse así, cómo la tecnología ha ido cambiando sustancialmente el modo de entender la salud y está modificando los hábitos de los profesionales, de los gestores y de los propios pacientes. Un contexto de esta naturaleza obliga sin duda a plantear nuevos enfoques más allá de los meramente defensivos[37].

3 .El despliegue de Big data

Si consideramos el informe «Big data en salud digital», ya citado, esta tecnología permite tres tipos principales de análisis:

- **Modelos predictivos:** analizan los resultados anteriores para evaluar qué probabilidad tiene un individuo de mostrar un comportamiento

36. Russell Howard por ejemplo considera que « Los médicos del futuro van a estar asistidos por un ordenador para hacer un diagnóstico más preciso, que le permitirá cuidar mejor de la salud de los pacientes, y ahí reside el valor económico de la inversión en Salud Digital. El médico del futuro no se va a basar en decirte que enfermedad tienes, y que opciones de tratamiento existen a tu disposición. El médico del futuro te va a ofrecer una perspectiva de ti, de tu mundo, de lo que te rodea, de tu futuro, así como un índice de probabilidades de lo que va a suceder con tu cuerpo y cómo puedes elegir un camino u otro para mantener tu bienestar en salud».
FUTURE TRENDS FORUM: *Salud digital.* Madrid 2016, pág. 20. Disponible en https://www.fundacionbankinter.org/ftf/tendencias/salud-digital.

37. Es significativa la afirmación del Dr. Julio Mayol. En su opinión, los sistemas de salud en el S. XXI en una profunda crisis financiera desencadenada por el aumento de la población y de la expectativa de vida, la cronicidad de las enfermedades y el incremento del precio de la tecnología. Por ello propone que «Destruyamos, creativamente, el modelo de servicios sanitarios, para reconstruirlo y hacerlo mejor. La ética de la prestación sanitaria no sólo depende de la buena intención, sino también de la calidad de los resultados». Y para ello la salud digital es imprescindible.
FUTURE TRENDS FORUM: *Salud digital.* Madrid 2016, pág. 16. Disponible en https://www.fundacionbankinter.org/ftf/tendencias/salud-digital.

específico en el futuro con el fin de mejorar la eficacia. Esta categoría también incluye modelos que buscan patrones discriminadores de datos para responder a las preguntas sobre el comportamiento del paciente, tales como la detección de fraudes.
(...)

- **Modelos descriptivos:** describen las relaciones entre los datos para poder clasificar a los individuos en grupos. A diferencia de los modelos de predicción que se centran en predecir el comportamiento de un único individuo, los modelos descriptivos identifican diferentes elaciones entre individuos. Pero los modelos descriptivos no clasifican a los clientes según su probabilidad de tomar una acción en particular. Las herramientas de modelado descriptivo pueden ser utilizadas para desarrollar modelos simulando una gran cantidad de agentes individuales pudiendo predecir también acciones futuras.

- **Modelos de decisión:** describen la relación entre todos los elementos de una decisión, incluidos los resultados de los modelos de predicción, la decisión a tomar y el plan de variables y valores que determinan la propia decisión, con la finalidad de predecir los resultados mediante el análisis de muchas variables. Estos modelos pueden ser también utilizados para diferentes procesos de optimización[38].

Cada uno de estos modelos puede ayudar en planos distintos en la investigación en salud y en la gestión de los sistemas sanitarios. El Informe define un conjunto de fases de un proyecto de Big data[39], relevantes desde la perspectiva de la privacidad desde el diseño:

Fase	Objeto	Principio jurídico
Preguntas iniciales	Definir las preguntas que dan lugar al objeto de la investigación. En el contexto actual plantean un problema de predictibilidad[40].	Finalidad, proporcionalidad.
Creación del modelo	— Definir objetivos definitivos así como la estrategia para alcanzarlos. — Integrar un proceso completo para poder capturar, consolidar, gestionar y proteger la información necesaria. — Identificarse los recursos humanos disponibles para llevar a cabo la implementación del modelo.	Finalidad, proporcionalidad, políticas de seguridad y perfiles de los usuarios.
Elección tecnológica	Escoger soluciones de hardware y software adecuadas.	Seguridad, transferencias internacionales de datos, encargado del tratamiento.
Implementación del modelo	— Obtención y almacenamiento de los datos. — Procesamiento. — Visualización.	Legitimación para el tratamiento, consentimiento, calidad de los datos, proporcionalidad, finalidad, veracidad.

38. SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). *Big data en...* Op. Cit. Págs. 19 y 20.

39. SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). *Big data en...* Op. Cit. Pág. 22.

El despliegue de Big data debe ser funcional no sólo a los objetivos del proyecto sino también a los requerimientos normativos que analizaremos en el epígrafe cuarto. Las consecuencias transformadoras de este despliegue pueden ser altamente positivas[41]:

- **Transformación de datos en conocimiento**: Big data permite el análisis no causal de grandes volúmenes de datos que puede estructurar nuevo conocimiento, especialmente en el área de la genómica.
- **Mejora del aprovechamiento de la información**: en Big data, la información no se recoge con una finalidad inmediata. La información, por lo general, es muy sencilla de recoger, por lo tanto, la verdadera transformación consiste en qué hacer con esa información para resolver cuestiones en un futuro.
- **Salto en la investigación clínica:** la propia lógica descentralizada y distribuida de los sistemas de Big data y la creación de mayores repositorios permite una mayor capacidad de análisis. Esto se debe a los nuevos procesos de colaboración científica.
- **Nuevos instrumentos para los profesionales de la salud:** los profesionales médicos tendrán acceso a nuevo conocimiento sobre patologías, tratamientos y fármacos que redundará en una mejor y más precisa provisión de servicios, así como en una mayor preparación para cuestiones epidemiológicas.
- **Promoción del autocuidado de la salud:** la información proveniente de los biosensores favorecerá una ciudadanía más empoderada en el cuidado de su salud.

Estos efectos se materializarían en distintos ámbitos como:

- La sostenibilidad del sistema de salud:
- Una mayor calidad en la atención sanitaria.
- Una mejor adecuación de los fármacos.
- Nuevas maneras de hacer medicina, ya que «Big data será el gran impulsor de la medicina del futuro o también llamada «Medicina de las

40. Según el informe: «Como la capacidad del Big data es enorme desde el punto de vista exploratorio, la formulación de las preguntas iniciales de investigación se configura como un elemento clave para la obtención de conocimiento, pero, a su vez, implica un cambio de perspectiva en su realización. Así, mientras queda claro que sin la pregunta adecuada, los datos y el posterior procesamiento de la información apenas tienen utilidad, cabe añadir que Big data permite explorar y ver la realidad de los datos haciendo que un buen análisis sobre los mismos acabe generando nuevas preguntas que deberán buscar respuesta».
SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). *Big data en...* Op. Cit. Pág. 22.

41. SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). *Big data en...* Op. Cit. Págs. 29, 42 a 44, 51.

4P», esto es, hacia una medicina personalizada, predictiva, preventiva y participativa»[42].

- Mejora de la atención a crónicos, personas con discapacidad y personas de edad avanzada.
- Desarrollo de nuevos modelos de atención en salud.
- Desarrollo de nuevos modelos de lucha contra el fraude.
- Lucha contra el fraude.

III. El caso VISC+

En 2015 el Servicio de Salud Catalán anunciaba a la Agència de Qualitat i Avaluació Sanitàries de Catalunya (AQuAS) el encargo[43] de desarrollar las tareas necesarias para arrancar el proyecto VISC+[44]. El Proyecto presentaba sin duda unos perfiles particularmente delicados. Constituía una apuesta significativa por la investigación en salud mediante la puesta a disposición de la comunidad investigadora de una inmensa base de datos, por un esquema abierto a la colaboración público-privada y finalmente por la propia naturaleza de los datos. Ello obligaba a abordar el problema con un enfoque técnico exquisito ya que estaban en juego valores muy significativos.

Era imprescindible un enfoque riguroso que no plantease la cuestión en términos maniqueos de blanco y negro sino que ofreciese soluciones. Ese fue el prisma de la Autoritat Catalana de Protecció

42. El Dr Julio Mayol añade una quinta «P», la Poblacional (para toda la población). Considera que los resultados del uso de Big data en salud, no serán inmediatos, ni necesariamente beneficiosos. En su opinión hay que manejar ciertos retos respecto a su utilización:

«1. Extraer conocimiento de fuentes heterogéneas y complejas.
2. Comprender notas clínicas no estructuras en su contexto correcto.
3. Gestionar adecuadamente gran cantidad de datos de imagen clínica y extraer información útil para generar biomarcadores.
4. Analizar los múltiples niveles de complejidad que van desde los datos genómicos hasta los sociales.
5. Capturar los datos de comportamiento de los pacientes, a través de distintos sensores, con sus implicaciones sociales y de comunicación.
6. Evitar los problemas de privacidad que pueden generar riesgos para los individuos».

FUTURE TRENDS FORUM: *Salud digital*. Madrid 2016, pág. 29. Disponible en https://www.fundacionbankinter.org/ftf/tendencias/salud-digital.

43. RESOLUCIÓN SLT/570/2015, de 16 de marzo, por la que se hace público un encargo de gestión que formalizan el Departamento de Salud, el Servicio Catalán de la Salud y el Instituto Catalán de la Salud con la Agencia de Calidad y Evaluación Sanitarias de Cataluña. Doc Núm. 6482 (1/04/2015). Disponible en http://dogc.gencat.cat/es/pdogc_canals_interns/pdogc_sumari_del_dogc/?anexos=1&language=es_ES&numDOGC=6843&seccion=0

44. El acrónimo se corresponde con la idea de dar «más valor a la información de salud en Cataluña».

de Dades (APDCAT) con un dictamen previo impecable que abordó la cuestión como una evaluación de impacto en la protección de datos[45]. El Proyecto VISC+ fue objeto de análisis por el Observatorio de Bioética y Derecho de la Universitat de Barcelona[46] que cuestionó la orientación del proyecto con planteamientos que no se comparten en su totalidad, pero aportando como valor añadido fundamental un cuestionamiento del marco jurídico que en la práctica se consideró obsoleto e ineficiente.

El Observatorio parte de una premisa que evita todo posible debate posterior: la anonimización es imposible. Para ello se usa el Dictamen 05/2014 sobre anonimización del Grupo de Trabajo del Artículo 29 (GT29)[47]. Y así poco hay que discutir, si «actualmente, está acreditado que la anonimización no garantiza la privacidad de los datos personales, puesto que mediante técnicas de ingeniería informática es posible volver a conectar los datos con la persona a quien pertenecen». Lo que determina una conclusión lógica: «cuestionar la validez de las iniciativas de intercambio de datos sensibles que estén basadas en técnicas de anonimización»[48].

El Observatorio plantea en el documento cuestiones muy acertadas sobre la limitación de la finalidad de los tratamientos, el consentimiento y distintos aspectos en materia de protección de datos personales, pero a la vez trufa sus consideraciones con prejuicios sobre los actores en el mundo de la investigación. Es difícil no compartir la aversión al uso comercial de los datos de salud[49] o la preocupa-

45. Dictamen núm. CNS 34/2014, Disponible en http://www.ara.cat/2014/10/06/1225157474.pdf?hash=036f616875039fc3249f04d1e9bc7bb7bb264c47.

46. LLÀCER, M.R., CASADO, M y BUISAN L (Coords.): *Documento sobre Bioética y Big data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública.* Observatorio de Bioética y Derecho de la Universitat de Barcelona. Barcelona, 2015. Disponible en http://www.bioeticayderecho.ub.edu/es/documento-sobre-bioetica-y-big-data-de-salud-explotacion-y-comercializacion-de-los-datos-de-los.

47. Dictamen 05/2014 sobre técnicas de anonimización, de 10 de abril de 2014 (0829/14/ES WP216).

48. LLÀCER, M.R., CASADO, M y BUISAN L (Coords.): *Documento sobre Bioética y* ... OP. Cit. Págs. 33 y 35.

49. Así afirman que «Por ejemplo, ¿se cedería la base de datos de enfermos de hepatitis C para desarrollar fármacos que después se pretenderían vender a 60.000 € cada tratamiento? Justamente esta cuestión sería la clave que condicionaría hasta qué punto los clientes o usuarios finales del proyecto estarían dispuestos a contribuir. El uso abusivo y opaco de los datos personales relacionados con la salud genera desconfianza en la población que impide que esos datos se empleen de modo legítimo para fines epidemiológicos, de investigación o docencia».
LLÀCER, M.R., CASADO, M y BUISAN L (Coords.): *Documento sobre Bioética y* ... OP. Cit. Págs. 43.

ción ante experiencias previas negativas[50]. Pero precisamente por eso, debe señalarse que algunas de las observaciones planteadas por el Observatorio resultan discutibles, y en especial todas aquellas que realizan un balance entre la investigación pública y la privada como alternativas casi incompatibles, como una especie de batalla entre buenos y malos.

Las conclusiones del documento resultan particularmente valiosas y ofrecen ideas sobre como encauzar jurídicamente un proyecto sobre Big data. Pero ni el Documento, ni publicaciones posteriores, entraron en el detalle de las condiciones de uso fijadas por la Generalitat en la Memoria de VISC+, y en el documento sobre «Garantías éticas para el uso de los datos»[51], ni en cómo se incorporaron o no las recomendaciones de la APDCAT. El resultado práctico fue ofrecer carnaza a todos aquellos dispuestos a entrar en un debate de buenos y malos, que fue el que finalmente triunfó[52] llevando al fracaso el proyecto y cercenando toda posibilidad de desarrollos futuros por un buen periodo de tiempo[53].

50. «la supuesta anonimización de datos de salud y atención sanitaria recogidos por el NHS Information Centre (NHS-IC), entre 2005 y 2013, no ha impedido que diferentes empresas hayan re-identificado a las personas a quienes hacían referencia estos datos, generando perjuicios diversos; por ejemplo en el precio de las primas de riesgo de los seguros».
LLÀCER, M.R., CASADO, M y BUISAN L (Coords.): *Documento sobre Bioética y …* OP. Cit. Pág. 44.

51. Información disponible en http://aquas.gencat.cat/es/projectes/visc/index.html.

52. Véase «El Parlament aprova substituir el VISC+ per un Big Data sanitari de gestió exclusivament pública». Disponible en http://diarisanitat.cat/el-parlament-aprova-substituir-el-visc-per-una-gestio-del-big-data-sanitari-exclusivament-publica/. «La CUP exige la «paralización inmediata» del VISC+». Disponible en https://elpais.com/ccaa/2016/01/27/catalunya/1453924193_849987.html.

53. Desde la honestidad científica no puede sino criticarse el uso maniqueo del debate público-privado en la investigación. En la investigación en salud el trasvase de experiencia en investigación básica del sector público al privado, y a la inversa mediante ensayos clínicos, o la financiación de grupos públicos de investigación con fondos privados es una práctica constante. Podemos estar de acuerdo o no con el negocio farmacéutico, y podemos exigir de los poderes públicos condiciones de negociación que resulten adecuadas y favorecedoras para la ciudadanía. Pero no es esta la cuestión nuclear. Si la investigación en Big data es valiosa debemos ofrecer soluciones jurídicamente viables.

IV. El marco regulador: ¿un problema?

El tratamiento de datos personales relativos a la salud en la investigación se inserta en un contexto regulatorio particularmente complejo cuyo análisis pormenorizado desbordaría con mucho la extensión de este trabajo[54]. En este marco, el derecho fundamental a la protección de datos o la privacidad juegan un papel determinante. Esta relevancia viene dada por la propia naturaleza de la actividad y por un constante y consolidado rechazo, cuando no aversión, a una normativa que se percibe sistemáticamente como una barrera.

Así lo ha constatado el Informe Sobre Big data en salud en relación con las opiniones facilitadas por distintos expertos, incluido el autor de este trabajo[55]:

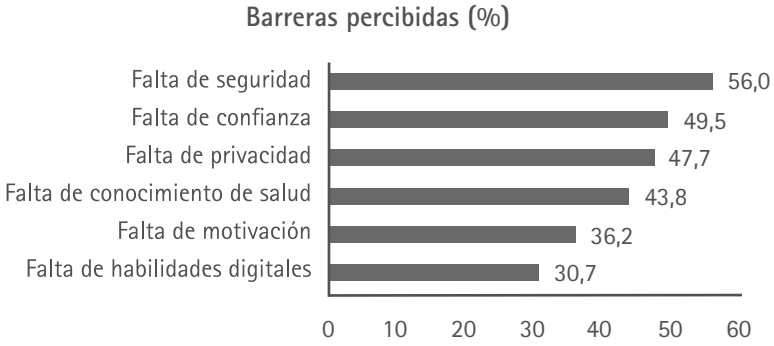
> Big data precisa almacenar una enorme cantidad de datos procedentes, en su mayoría, de los pacientes. Estos datos personales son extremadamente sensibles y será preciso que la normativa que garantice los derechos en este ámbito consiga asegurar la confidencialidad de la información sin que ello suponga un freno para su propio desarrollo. En este sentido, la mayoría de los profesionales consultados muestran una cierta insatisfacción con el actual marco normativo, hasta el punto que para muchos de ellos, es la principal barrera a superar.

54. – Ley 14/1986, de 25 de abril, General de Sanidad.
– Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
– Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
– Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
– Ley 14/2007, de 3 de julio, de Investigación biomédica.
– Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.
– Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los Comités de Ética de la Investigación con medicamentos y el Registro Español de Estudios Clínicos.

55. 55, y 57 a El Informe refiere su coincidencia con los resultados del Instituto de Prospectiva Tecnológica (IPTS) de la Comisión Europea, que en 2012 situaba la percepción de la privacidad como barrera en un 47,7%.

La cuestión es que la «privacidad», o alguno de sus elementos determinantes, se sitúa entre las principales barreras percibidas por los expertos.

Figura 2. Barreras percibidas para la salud digital



Citado por Informe sobre Big data en salud digital, pág. 59[56]

Es destacable cómo para los expertos la desactualización de la Ley Orgánica de Protección de Datos de Carácter Personal es un problema que desde luego el Anteproyecto de reforma presentado por el Gobierno de España no va a resolver[57].

56. En él se señala que:
«En concreto, los problemas de seguridad, confidencialidad y privacidad de la información están relacionados con los siguientes aspectos:
(...)
- Una **mala gobernanza de los datos**, por ejemplo, con las bases de datos en manos privadas sin las suficientes salvaguardas que no redunden en ningún beneficio concreto para el ciudadano.
- El **consentimiento informado** para tratar con la información personal de salud a través de sistemas mal diseñados y que pudiera poner en peligro la seguridad de las personas.

Una adecuada gobernanza de datos para tratar de minimizar los problemas o riesgos asociados con la confidencialidad y la privacidad de los datos deben regirse por los siguientes principios:
- Los datos de salud de los pacientes han de ser propiedad de los pacientes.
- La gobernanza de datos debe basarse en procesos robustos desarrollados para garantizar el respeto de los valores y principios en el uso de los datos, poniendo el máximo énfasis en la minimización de los posibles riesgos asociados.
- El marco normativo debe establecer las garantías adecuadas, permitir el intercambio y puesta en común de los datos anonimizados en tiempo real. (...)»

SAN SEGUNDO ENCINAR, JOSE MARÍA (DIR.). *Big data en...* Op. Cit. Págs. 59 y 60.

57. Así es la Disposición Adicional Novena del Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal establece que «El Gobierno en el plazo de dos años desde la entrada en vigor de esta ley orgánica remitirá a las Cortes un proyecto de ley en el que establecerá condiciones adicionales y, en su caso, limitaciones al tratamiento de datos genéticos, biométricos o relativos a la salud». Véase el texto en http://transparencia.gob.es/servicios-buscador/contenido/normaelaboracion.htm?id=NormaEV08L0-20172401&lang=ca&fcAct=2017-07-17T14:01:17.880Z.

Tabla 2. Nivel de acuerdo de los expertos consultados a las hipótesis planteadas sobre barreras y riesgos derivados de la implantación del Big data en salud digital

Hipótesis planteadas	Acuerdo (%)
El grado de coordinación entre la información proveniente de la salud pública y la privada es insuficiente	83,3
Existirá un problema de fa lta de recursos humanos especializados capaces de trabajar con aplicaciones Big data una vez éstas se generalicen	83,3
Aún deben superarse muchos problemas de interoperabilidad de datos, especialmente por lo que respecta a la interoperabilidad semántica	83,3
El mal uso de la información de los ciudadanos puede provocar un fuerte rechazo en la sociedad que frene el desarrollo de las soluciones Big data	75,0
La información proveniente de sistemas Big data no tiene el mismo rigor científico que la derivada de la aplicación de test clínicos controlados	66,7
La no causalidad de los modelos puede llevar a conclusiones erroneas debido a la presencia de variables espurias no detectadas	66,7
Aparición de nuevos riesgos de la información disponible de los ciudadanos, información perdida o robada, preeminencia de los indicadores biológicos por encima del bienestar	66,7
Un exceso de biomonitorización puede acabar provocando una pérdida de autonomía de los ciudadanos sobre sus propias vidas y decisiones	58,3
El marco normativo que rige las cuestiones de privacidad y confidencialidad en España es adecuado para la implantación del Big Data	50,0
Big data acabará favoreciendo a aquellos que están más interconectados digitalmente, aumentando las desigualdades aumentando la 'brecha digital'	16,7

Citado por Informe sobre Big data en salud digital, pág. 66

En este sentido resulta francamente llamativa la opinión manifestada por Vicki Seyfert-Margolis. Fundadora y CEO de My Own Med, Inc. que contrapone la facilidad con que facilitamos datos en redes sociales y la preocupación que nos plantea el tratamiento de datos en el ámbito de la salud[58].

En realidad, no es que la normativa sobre protección de datos sea en sí misma una barrera. Se percibe así desde el desconocimiento de las ventajas que el cumplimiento normativo puede proporcionar en términos de confianza y seguridad. Sin embargo hay que referir ciertos cuellos de botella cuyo concreto enfoque puede ser determinante.

1. El problema de la anonimización

Un argumento recurrente al hablar de Big data consiste en identificar riesgos para la privacidad asociados a la posibilidad de obtener información significativa e incluso capaz de proporcionar herramientas de control social. El antídoto para ello sería la anonimización. Disociar los datos de manera tal que no se no permita la identificación de un afectado o interesado sirve paras eludir riesgos y la aplicación de la normativa. Sin embargo, el Dictamen 05/2014 del Grupo de Trabajo del Artículo 29 (GT29) muestra que ésta no es una operación ni sencilla, ni banal. El

58. «En el momento actual ponemos en duda quién tiene derecho de poseer y usar nuestros datos, y si lo que nos ofrecen a cambio de nuestra contribución es suficiente. Conforme Big data empieza a aplicarse en sanidad (nuestros datos más personales, podría decirse) la cuestión se está planteando como un tema de privacidad. Es irónico que a través de nuestras compras online, participación en redes sociales y la economía de las aplicaciones ya hayamos cedido una cantidad ingente de datos personales. No obstante, la salud es el catalizador que pone en duda el statu quo.

Dado el uso creciente de los sensores en dispositivos wearable (que vestimos), los historiales médicos electrónicos, las aplicaciones relativas a la salud y al bienestar, y hasta la secuenciación del genoma humano; nuestro «yo» más profundo, aquello que nos hace lo que somos, se puede capturar en tiempo real a través de un dispositivo tan sencillo como un reloj o una pulsera, o tan sofisticado como los monitores de glucosa y las bombas de insulina que han automatizado la gestión de la diabetes. Gracias a los datos se sabe dónde vamos, cuánto nos movemos, cuánto dormimos, nuestra frecuencia cardiaca y mucho más, y todo ello se viene combinando con la información de nuestros historiales médicos para definir nuestro estado de salud actual, predecir nuestra trayectoria de salud y evaluar los riesgos. Visto así, es el Big data de la persona, para la persona en su mejor versión, puesto que podemos empezar a soñar con intervenciones de salud en tiempo real y medicina preventiva en contextos hasta ahora inimaginables.

¿Y qué pasa con el contrato social? La pregunta ante nosotros como individuos y como grupo se reducirá a evaluar el riesgo y el beneficio de las decisiones más personales sobre salud, tal y como lo definan los datos. Al plantearnos la vida con Big data y sensores que calculan nuestro estado de salud, es obligatorio preguntarse: ¿cuántos datos más queremos ceder y a cambio de qué?».

FUTURE TRENDS FORUM: *Big data. El poder de los datos*. Fundación Innovación Bankinter, Madrid 2014, pág. 11. Disponible en https://www.fundacionbankinter.org/ftf/tendencias/bigdata. Pág. 35.

punto de partida imprescindible para entender la posición del GT29 es el Considerando 26 de la Directiva 95/46/CE:

> (26) Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, **hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona**; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado;

Para el GT2 la anonimización constituye un tratamiento en sí misma, como tal debería ser compatible con el tratamiento original y contar con un fundamento, una base legal o contractual que la legitime. En esencia la anonimización exige:

- Que no pueda ser establecido vínculo alguno entre el dato y su titular sin un esfuerzo desproporcionado.
- Que sea irreversible.
- Que en la práctica sea equivalente a un borrado permanente.

El problema reside en que no existe un estándar comúnmente aceptado y seguro. Desde un punto de vista jurídico para el GT29 estamos ante un tratamiento ulterior para el que sería necesario:

- Disponer de un fundamento que lo legitime, como por ejemplo el interés legítimo.
- Verificar la relación de compatibilidad entre la finalidad para la recogida inicial y un tratamiento posterior como la anonimización.
- Las expectativas del titular sobre usos posteriores.
- El impacto en el titular de los datos.
- Las cautelas adoptadas por el responsable para salvaguardar los derechos de los afectados.
- El deber de cumplir con el principio de transparencia.

Sin embargo, para el GT29 desde el punto de vista de la protección de datos personales en la anonimización siempre existen riesgos:

- La persistencia de datos que permitan reidentificar.
- La posibilidad de reidentificar mediante inferencias, o por vinculación o relación (link) con otros paquetes de datos personales.
- Confundir pseudonimización y anonimización.
- Creer que la anonimización excluye el cumplimiento normativo sectorial.

Cuando la anonimización presente la menor inconsistencia, cuando mediante técnicas de inferencia, de relación con otros paquetes de datos, cuando la presencia de quasi-identificadores permita la menor reidenti-

ficación operarán en bloque las garantías de la normativa de protección de datos. Si para ello además el estándar viene dado por lo que sea capaz de hacer «cualquier otra persona, para identificar», y este cualquiera son científicos del Instituto Tecnológico de Massachusetts (MIT)[59] podemos entender que se haya afirmado que la anonimización es imposible

2. El principio de finalidad en un contexto cambiante

Se señalaba que en el despliegue de las herramientas de machine learning existen procedimientos de aprendizaje autónomo no supervisado y cómo las fuentes de información pueden trascender la historia clínica en Big data en salud. El resultado práctico de ello podría ser la obtención de información relevante para una finalidad distinta de aquella para la que se obtuvieron los datos. Y ello pone en riesgo de modo significativo todas y cada una de las recomendaciones del GT29 que se acaban de citar.

La finalidad resulta determinante para desarrollar el juicio de proporcionalidad que se exige para asegurar un tratamiento legítimo. ¿Pero qué sucede si investigando sobre diabetes se identifican factores de riesgo conductual que producen efectos relevantes en la hipertensión del paciente? Si se aplica el razonamiento silogístico al que aludíamos más arriba resultaría un incumplimiento de la normativa sobre protección de datos. Por ello, salvo que las autoridades de protección de datos admitan que la investigación científica en salud constituye por sí misma un supuesto de interés legítimo, Big data no será viable en la Unión Europea.

En principio el Reglamento general de protección de datos ofrece en sus considerandos base para sustentar tal afirmación, En principio el Considerando 50 señala que:

> «Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles».

Sin embargo, el considerando 33 es más restrictivo al considerar la investigación basada en el consentimiento:

> (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

59. Véase DE MONTJOYE Yves-Alexandre, RADAELLI Laura, KUMAR SINGH Vivek y PENTLAND Alex «Sandy»: «Unique in the shopping mall: in the reidentifiability of credit card metadata» en Science, 30 JANUARY 2015, VOL 347 ISSUE 622, págs. 536-539.

> o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida[60].

Todo ello dibuja escenarios diversos de posible interpretación. En primer lugar, salvo habilitación legal expresa, -que recordemos tardará de dos a tres años en llegar-, los operadores en Sanidad deberían cuidarse mucho de obtener el consentimiento libre, específico, informado e inequívoco por el que el interesado acepta de modo explícito, ya sea mediante una declaración o una clara acción afirmativa, el uso de sus datos con fines de investigación en salud. Ello implicaría en una interpretación estricta identificar el área concreta de investigación en salud. Un segundo escenario, consistiría bien en entender que consentir para la «investigación en salud» es suficientemente específico, o bien considerar que el uso posterior de los datos para «otros fines de investigación en salud» no es incompatible.

De no manejar este tipo de criterios resultaría una paradoja singular. Si aplicamos el principio de finalidad en sentido estricto, resultaría que tal vez hubiéramos descartado el Sindenafil como principio activo adecuado

60. En cualquier caso, no debe olvidarse la necesidad de cumplir con el conjunto del Reglamento general de protección de datos:
(50) El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. (...) Las operaciones de tratamiento ulterior con (...) fines de investigación científica (...) deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.
Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable. Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto.

para tratar la angina de pecho y jamás habríamos contribuido a remediar la disfunción eréctil «por protección de datos»[61]. El ejemplo es conscientemente jocoso, pero habrá que plantearse qué sucederá cuando usando Big data descubramos cuestiones que siendo para finalidades distintas -e ¿incompatibles?-, pongan de manifiesto la existencia de un riesgo para la vida de personas. ¿Es posible que el Regulador nos ofrezca una respuesta de tipo puramente positivista, que no positivo? ¿Enfrentaremos de nuevo análisis impecables desde un punto de vista jurídico pero contrarios a toda razón científica?[62]

3. La veracidad: la confiabilidad en el algoritmo

Hace unos años Google pareció encontrar una metodología en la que mediante análisis de Big data, se podrían establecer correlaciones que sobre la base de las búsquedas de los usuarios permitieran identificar patrones de localización y extensión del virus de la gripe anticipadamente[63]. Sin embargo, el proyecto no resultó tan certero y veraz como se podría imaginar y fracasó en las previsiones. Se determinó por ejemplo que el algoritmo de Google era bastante vulnerable a un ajuste por exceso de términos estacionales no relacionados con la gripe, como «baloncesto de la escuela.» Se produjeron por pura casualidad, y Google no tuvo en cuenta los cambios en el comportamiento de búsqueda a través del tiempo[64]. No es extraño, por tanto que los expertos se cuestionen la llamada veracidad de Big data

> «...las tres características del Big data, de volumen, de variedad y de velocidad, añadiendo la de veracidad, es decir, no nos vayamos a inventar las cosas, pero vamos a trabajar con datos seguros, porque si tú trabajas con datos malos, obtendrás resultados malos, pero esto te pasa igual con

61. BBC-Mundo: «El Viagra surgió por error». Disponible en http://www.bbc.com/mundo/ciencia_tecnologia/2010/01/100120_1215_viagra_drogas_mes.shtml?MOB

62. Véase en el Blog LOPD y Seguridad: «Datos de salud, balancing test, y riesgo social». Disponible en http://lopdyseguridad.es/datos-de-salud-balancing-test-y-riesgo-social/

63. Véase GINSBERG Jeremy, MOHEBBI Matthew, PATEL Rajan, BRAMME Lynnetter, SMOLINSKI Mark S. y BRILLIANT Larry: «Detecting influenza epidemics using search engine query data» en *Nature* Vol 457, 19 February 2009, doi:10.1038/nature07634 http://dx.doi.org/10.1038/nature07634
Los resultados de Google Flu Trends pueden verse en: https://www.google.com/publicdata/explore?ds=z3bsqef7ki44ac_&hl=en&dl=en#!strail=false&bcs=d&nselm=h&trdim=country&tidim=country:FR&tifdim=country&hl=en_US&dl=en&ind=false

64. Véase LAZER David y KENNEDY Ryan: «What We Can Learn From the Epic Failure of Google Flu Trends» en *Wired Science*. Disponible en https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/ y BUTLER Declan: «When Google got flu wrong» en *Nature News*, volume 494, págs. 155-156.

> ensayos clínicos de la industria farmacéutica que se están inventando o están haciendo de forma clásica, pero mal...»[65]

Ello obliga a reconsiderar nuestra relación de confianza con los algoritmos y a exigir de la comunidad científica un deber extremo de rigor[66]. En este sentido, se comparten plenamente las consideraciones planteadas en el marco del Future Trends Forum:

> Al Big data le han quedado tres para septiembre y corre peligro de suspenderlas si no se actúa en consecuencia. La primera tiene que ver con la limpieza de los datos basura. La segunda, con la comprensión lectora y su aplicación práctica. Y la tercera con la ética y la responsabilidad. Para que estas materias no pasen de reto a obstáculo y nos hagan repetir de curso, hay que hacer una serie de deberes:
>
> **Contextualizar y limpiar.** Es lo primero que hay que hacer con los datos para que sus aportes sean de calidad y no meros declarativos inútiles.
>
> (...)
>
> **Entender y aplicar.** Es la segunda tarea. Una buena comprensión lectora de los datos es clave para transmitirlos adecuadamente.
>
> (...)
>
> **Equilibrar.** Por otra parte, a la hora de recopilar estos datos médicos surge otra incógnita: ¿dónde parar? Esto tiene que ver con la tercera materia pendiente: hacer de contrapeso entre propiedad, privacidad y seguridad en una sensible balanza donde también entra en juego el concepto de propiedad y su delimitación[67].

Cada una de estas estrategias será vital para un cumplimiento normativo adecuado, al que nos referimos a continuación.

---

65. San Segundo Encinar, Jose María (Dir.). *Big data en...* Op. Cit. Pág. 62.

66. Jerry Kaplan señala que los sistemas de Inteligencia Artificial «están diseñados para logar objetivos únicos, sin tener conocimiento ni preocupación por los efectos secundarios. (...) Los intelectos sintéticos, a medida invaden áreas que antes eran dominio exclusivo de los humanos, ajenos al contexto social más amplio, son propensos a comportarse de maneras que la sociedad consideraría repugnantes». KAPLAN, Jerry: *Abstenerse humanos*. TEELL, Zaragoza, 2016, págs. 48 y 49.

67. FUTURE TRENS FORUM: *Big data. El poder de los datos (Resumen ejecutivo)*. Fundación Innovación Bankinter, Madrid 2014, pág. 11. Disponible en https://www.fundacionbankinter.org/ftf/tendencias/bigdata.

V. Una estrategia para el cumplimiento normativo en Big data y Salud

Anteriormente se ha constatado que los expertos perciben la protección de datos como un obstáculo a la investigación en salud. El problema, visto desde la experiencia resulta particularmente grave, en la medida en la que conduce a distintos resultados dañosos. El primero consiste en operar como un elemento desincentivador de modo que en grupos de investigación precompetitivos o sin recursos suficientes puede determinar el abandono de una investigación. En otras ocasiones determina una suerte de autocensura de modo que la tendencia natural del investigador a aspirar al máximo queda coartada. Por último, puede llegar a producir un efecto paralizante cuando las cautelas se acentúan al máximo, generando un asesoramiento jurídico de naturaleza defensiva ordenado a evitar la sanción de la autoridad de protección de datos más que a hacer viable la investigación. Todo ello es evitable o resoluble. Sin embargo, la normativa se convierte en un verdadero obstáculo cuando el regulador, -sea legislador, gobierno o autoridad de protección de datos-, opera desde un enfoque reduccionista, centrado en una visión plana de jurista más apegado al Código, que a la materialidad de los tratamientos con fines de investigación científica[68].

Es indispensable por ello describir sucintamente las herramientas que el Reglamento general de protección de datos pone a nuestra disposición para abordar proyectos de Big data en salud y ofrecer una visión progresiva que parta de hacer viable la investigación en salud cuando aporta valor.

68. La cuestión posee tal relevancia que los Rectores de las Universidades Europeas llegaron a indicar expresamente a la Comisión que la redacción del Proyecto de Reglamento general de protección de datos ponía en peligro la investigación científica en salud:

« ·The LIBE Committee amendments alter dramatically the ability to be able to conduct medical and health research (Art. 81). The precise legal impact of the proposed amendments for scientific research across Europe is still uncertain, but the unintended consequences may be quite dramatic. It is anticipated that «at worst health research involving personal data would be illegal; at best it would be largely unworkable», as indicated in the Wellcome Trust statement».

Véase EUA Statement On the Proposal for a General Data Protection Regulation: A Potential Threat to the Advancement of Scientific Research Using Personal Data. Disponible en http://www.eua.be/Libraries/policy-positions/DPR_EUA_Position_April_2014.pdf?sfvrsn=0.

1. Ética e integridad en la investigación: la responsabilidad proactiva

La ética e integridad son fundamentales para cualquier proyecto vinculado a Big data[69]. Este es un reto ineludible que debe ser afrontado desde el compromiso individual, desde la formación del personal y en la reconsideración de las estrategias a seguir en el marco de los comités de ética. Si la exigente regulación del tratamiento de datos de salud tiene por objeto último evitar la discriminación y garantizar la libertad, la ética es una precondición y su finalidad debe ser la misma, poniendo siempre por delante la dignidad del paciente y el cumplimiento normativo.

En un plano individual la «Declaración sobre integridad científica en investigación e innovación responsable» identifica en Declaraciones previas los principios de honestidad, responsabilidad, justicia (*fairness*) y rendición de cuentas (*accountability*) [70]. Y a la vez propone una interesante metodología de identificación y organización de las diversas infracciones a la integridad científica, diseñada a partir de las etapas del proceso de investigación: enunciar los objetivos, delinear las metodologías y evaluar el impacto. Resulta significativo que con la experiencia previa de alguna de sus autoras en la evaluación del proyecto VISC+ la privacidad no surja ni en una sola ocasión y sí lo haga el plagio. Especialmente teniendo en cuenta que a la fecha del documento ya se disponía de un marco definitivo, el del Reglamento general de protección de datos, que de acuerdo con el principio de protección de datos desde el diseño y por defecto, ofrece criterios viables para cada una de las fases de la planificación de la investigación.

El documento identifica causas de las conductas éticamente censurables que clasifica según los factores que las determinan (individuales, organi-

69. Sobre esta materia véase PUYOL MONTERO, Javier: «Aproximación jurídica y económica al Big Data. Tirant lo Blanch, valencia 2015, págs. 285 y ss.

70. Promovido por las Cátedras Unesco de Bioética de la Universidad de Barcelona (UB) y de la Universidad Católica Portuguesa (UCP), este documento se declara heredero e integrador de distintas Declaraciones: «Declaración de Singapur sobre Integridad en Investigación (2010) —que destaca los principios de honestidad, imputabilidad (accountability), cortesía profesional, justicia (fairness) y buena administración (good stewardship)—, al Código de Conducta para la Integridad en Investigación de la Fundación para la Ciencia Europea / Academias Europeas ALLEA (2010) —que valora la honestidad, confianza, objetividad, imparcialidad e independencia, apertura (openness) y accesibilidad, derecho al cuidado, justicia (fairness) y responsabilidad (responsibility) con respecto al futuro—, a la Declaración de Montreal sobre Integridad en Investigación (2013) —que establece diferentes niveles de responsabilidad de los socios individuales o institucionales en investigación colaborativa transfronteriza—, y a la Declaración sobre Principios en Integridad en Investigación del Consejo de Investigación Global (2013)»
CASADO María, DO CÉU PATRÃO NEVES, Maria, DE LECUONA Itziar, CARVALHO Ana Sofia, ARAÚJO Joana: *Declaración sobre integridad científica en investigación e innovación responsable*. Edicions de la Universitat de Barcelona, Barcelona-Porto, julio de 2016, págs. 49 a 51.

zativos, estructurales). De nuevo, entre ellas brilla por su ausencia la carencia de modelos de cumplimiento normativo responsable. Sin embargo se cita entre los factores organizativos uno particularmente relevante:

> La falta de formación en competencias en materia de ética e integridad científica, teórica y práctica, en la que el ejemplo del supervisor es clave como modelo de comportamiento ético.[71]

La ética individual no es viable en un contexto en el que la carencia de formación del personal implica un rechazo profundo a las políticas de cumplimiento normativo en protección de datos. De una parte, la carencia de personal especializado, el delegado de protección de datos, eterniza el examen de viabilidad jurídica de los proyectos y a veces los hace inviables. De otra, como se afirmó, el investigador acaba percibiendo la cuestión jurídica como un obstáculo insalvable y al delegado de protección de datos como un enemigo interno. Sin una formación básica que comprometa al investigador, el resultado práctico suele ser el abandono del proyecto. Pero también se produce el desarrollo de investigaciones sin conocimiento del equipo de soporte jurídico. En tales casos, el cumplimiento normativo riguroso y las políticas de seguridad brillan por su ausencia, lo que de aplicarse, por ejemplo, el artículo 59.2.a) de la Ley de garantías y uso racional de los medicamentos y productos sanitarios, permite a la Agencia Española de Medicamentos y Productos Sanitarios interrumpir en cualquier momento la realización de un ensayo clínico.
Por lo que respecta a los comités de ética hay que destacar la necesidad de actualizar las prácticas de este tipo de órganos tanto desde el punto de vista de sus competencias, como de su composición e incluso de los protocolos de funcionamiento. Estos comités adquieren gran relevancia en universidades, hospitales y otros centros de investigación al socaire de la Ley 14/2007, de 3 de julio, de Investigación biomédica, y en el entorno de las garantías que se establecen en la investigación con humanos. En este contexto, lo que esencialmente preocupa consiste es garantizar la integridad y la seguridad del paciente en el marco de investigaciones que pueden resultar invasivas. El sistema pivota sobre un doble pilar. Las condiciones que se imponen a la investigación, que deberá asegurar «la protección de la dignidad e identidad del ser humano con respecto a cualquier investigación que implique intervenciones sobre seres humanos en el campo de la biomedicina, garantizándose a toda persona, sin discriminación alguna, el respeto a la integridad y a sus demás derechos y libertades fundamentales». Y, en segundo lugar, la exigencia de un consentimiento informado.

71. CASADO María, ET ALII: *Declaración sobre integridad científica*...Op. Cit. Pág. 53.

De acuerdo con la Ley corresponde al comité de ética «ponderar los aspectos metodológicos, éticos y legales del proyecto de investigación». Desde la experiencia del autor, cuando la tarea del comité consiste en verificar aspectos legales usualmente se limita a constatar la presencia de modelos adecuados de consentimiento informado y muy excepcionalmente las condiciones de aplicación de elementos adicionales como declaraciones de compromiso de cumplimiento del Código Tipo de Farmaindustria[72]. Este tipo de actuación resulta insuficiente para una correcta evaluación de los proyectos de investigación en el ámbito del Big data en salud. En primer lugar, los miembros usualmente carecen de las adecuadas capacidades para verificar el impacto de un tratamiento de información personal mediante analítica de datos. En este sentido, y como puede deducirse del conjunto de este trabajo, «no basta con un impreso para el consentimiento», es fundamental haber:

- Desarrollado una estrategia previa de protección de datos de datos desde el diseño y por defecto.
- Aplicado las herramientas de análisis de impacto en la protección de datos.
- Definido políticas de seguridad.
- Verificado las condiciones de tratamiento anónimo o pseudónimo de los datos.
- Preparado una información adecuada, transparente y fácilmente comprensible facilitadora de la obtención de consentimientos.
- Documentado la existencia de condiciones de cumplimiento normativo general y sectorial del proyecto.

No es por tanto concebible un futuro adecuado para la investigación en Big data y salud sin la integración de la figura del delegado de protección de datos en los comités de ética, y si estos no establecen protocolos de cumplimiento obligatorio que garanticen la llamada protección de datos proactiva o «*accountability*». Pero este principio no sólo debe aplicarse por los responsables de los tratamientos en investigación, también le corresponde a la autoridad de protección de datos personales ofreciendo criterios y soluciones, razonables, viables y ajustadas a la realidad material de la investigación. Si el regulador no es «*accountable*» en su ejercicio cotidiano, si opera desde el autismo o el desconocimiento de la realidad, si no baja a la arena a ofrecer soluciones viables estará cercenando la

72. Código Tipo de Farmaindustria de protección de datos personales en el ámbito de la investigación clínica y de la
Farmacovigilancia. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/index-ides-idphp.php

investigación y con ello todas las oportunidades que para el país y los pacientes pudieran surgir[73].

2. Protección de datos de datos desde el diseño y por defecto y análisis de impacto en la protección de datos

El Reglamento general de protección de datos sitúa estos dos conceptos en el eje de las políticas de aplicación normativa al tratamiento de datos personales en el ámbito de la investigación en salud. El primero de ellos debería articularse a través de la adopción de distintas medidas que recomienda el considerando 78:

> (78) ... Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

El artículo 25 RGPD define este marco de actuación al señalar que «el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados».

Para el despliegue de estas políticas es muy relevante la estrategia de *Privacy by Design* desplegada por la Autoridad de Protección de Datos de Ontario, que define 7 grandes reglas de acción a las que denomina «Principios»[74]:

---

73. Véase en el Blog LOPD y Seguridad: «¿Es posible otra gestión de la privacidad?». Disponible en http://lopdyseguridad.es/es-posible-otra-gestion-de-la-privacidad/.

---

74 CAVOUKIAN Ann: *Privac y by Design Los 7 Principios Fundamentales*. Comisionada de Información y Privacidad Ontario, Canadá, 2011.

1. Proactivo, no Reactivo; Preventivo no Correctivo

(...) PbD no espera a que los riesgos se materialicen, (...) su finalidad es prevenir que ocurran. En resumen, Privacidad por Diseño llega antes del suceso, no después.

2. Privacidad como la Configuración Predeterminada

(...) No se requiere acción alguna de parte de la persona para proteger la privacidad – está interconstruida en el sistema, como una configuración predeterminada.

3. Privacidad Incrustada en el Diseño

La Privacidad por Diseño está incrustada en el diseño y la arquitectura de los sistemas de Tecnologías de Información y en las prácticas de negocios. (...) La privacidad es parte integral del sistema, sin disminuir su funcionalidad.

4. Funcionalidad Total – «Todos ganan», no «Si alguien gana, otro pierde»

Privacidad por Diseño busca acomodar todos los intereses y objetivos legítimos de una forma «ganar-ganar», (...).

5. Seguridad Extremo-a-Extremo – Protección de Ciclo de Vida Completo

(...) la Privacidad por Diseño se extiende con seguridad a través del ciclo de vida completo de los datos involucrados – las medidas de seguridad robustas son esenciales para la privacidad, de inicio a fin. (...)

6. Visibilidad y Transparencia – Mantenerlo Abierto

Privacidad por Diseño busca asegurar a todos los involucrados (...) Sus partes componentes y operaciones permanecen visibles y transparentes, a usuarios y a proveedores. (...)

7. Respeto por la Privacidad de los Usuarios – Mantener un Enfoque Centrado en el Usuario.

(...) Hay que mantener al usuario en el centro de las prioridades.

El despliegue de estos principios implica la adopción de un conjunto de procesos decisionales desde el diseño inicial del proyecto de investigación. El desarrollo sistemático y aplicado de estos principios desbordaría con mucho el objeto de esta publicación[75]. Sin embargo, la combinación de los 7 Principios Fundamentales y el trabajo de detalle desarrollado por el Information Commisioner's Office británico[76], y el Consejo de Europa[77] puede extraerse una mínima bitácora que nos guíe en la navegación:

A. Armar y formar éticamente a nuestros equipos de investigación

Sin un esfuerzo de sensibilización previa y de generación de conocimiento es imposible el cumplimiento normativo y que la privacidad encuentre encaje en la ética de la dignidad humana que guía la investigación en salud.

B. Disponer de políticas preventivas de análisis de riesgos

Es decir, tanto cuando la investigación trate datos personales, cómo cuando se manejen datos anonimizados, parece indispensable desarrollar la evaluación de impacto en la protección de datos al que se refiere el artículo 35 RGPD. Este análisis debería tener particularmente en cuenta cómo se afecta a los derechos y libertades de los sujetos, las condiciones que garanticen la seguridad de la información y en su caso la calidad en las políticas de pseudonomización y/o anonimización que se adopten. Este análisis de riesgos no se agota en sí mismo, su resultado debe arrojar como consecuencia un modelo de cumplimiento normativo y de seguridad que rija durante toda la vida del tratamiento en un proceso de constante retroalimentación.

75. Desgraciadamente, de fronteras adentro las pautas que se nos ofrecen en esta materia son mínimas y la ausencia de criterio determinante. Aunque no desconoce en absoluto el autor la existencia de una publicación promocionada por la Agencia Española de Protección de Datos denominada «Código de buenas prácticas en protección de datos para proyectos Big Data». Sin embargo, de su lectura no se desprende otra conclusión útil distinta de la necesidad de aplicar el RGPD. La Guía ha sido desarrollada por distintos operadores privados y se encuentra disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf.

76. INFORMATION COMMISIONER'S OFFICE: *Big data, artificial intelligence, machine learning and data protection.* Version 2.0, 2017. Disponible en https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

77. CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA: *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data.* Council of Europe, Strasbourg, 2017.

C. Delimitar la finalidad de la investigación

Siempre que sea posible debe fijarse con precisión la finalidad que se persigue con la investigación y el área material afectada. Esta tarea será sin duda ardua, ya que cuando se investigue con datos no anonimizados o «reidentificables» será necesario ser capaces de encontrar un ámbito de finalidad lo suficientemente descriptivo como para acoger las finalidades «compatibles» previsibles. En cualquier caso, el colectivo investigador necesita que los reguladores precisen el sentido que se va a dar la previsión del Considerando 50 RGPD y si en todos los casos el uso de los datos con fines de investigación científica será un tratamiento compatible.

D. Garantizar una adecuada transparencia con el paciente y apostar por el consentimiento como elemento de legitimación de los tratamientos[78]

Aunque la Ley 41/2002 permita la investigación con datos anónimos tanto las previsiones del GT29, como las resoluciones y Guías de la Agencia Española de Protección de Datos, muestran una aproximación estricta al concepto de anonimización hasta el punto de hacerla imposible. De otro lado, se ha afirmado en este trabajo que Big data puede favorecer hallazgos casuales que impliquen un deber ético de reidentificar en aras de preservar la salud del paciente[79]. Por todo ello, sería conveniente desplegar una nueva estrategia en los sistemas de salud públicos, y en la salud privada, ordenados a la captación de consentimientos para la investigación en Big data que alcanzasen a cualquier modalidad de datos, -identificados, anónimos, y seudónimos-, e incluyesen permisos de reidentificación. En este proceso la transparencia, la claridad en la información y la confianza del paciente serían valores cruciales.

E. Tratar adecuadamente cuando no evitar los supuestos que conduzcan a decisiones automatizadas

Como se ha señalado más arriba la fe en el algoritmo no puede derivar en una confianza ciega. Por otra parte, la adecuada visualización y enten-

78. Para la Comisión Europea se trata de dos elementos determinantes. Véase EUROPEAN COMMISSION: Opinión núm. 26. Ethics of Information and Communication Technologies. Brussels, 2012. Pág. 61.

79. No dude el lector, que dicho tratamiento vendría legitimado sin ningún género de dudas por la prevalencia del interés superior de la salud del paciente. Desgraciadamente el Regulador, que con tanta facilidad puede encontrar fundamento para establecer excepciones al deber de informar de los abogados, no suele manifestar tanta flexibilidad en otros ámbitos. Véase Informe sobre Tratamiento por Abogados y Procuradores de los datos de las partes en un proceso. Disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/consentimiento/common/pdfs/2000-0000_Tratamiento-por-abogados-y-procuradores-de-los-datos-de-las-partes-en-un-proceso.pdf

dimiento de los resultados en sistemas de caja negra obligan a extremar el cuidado en esta materia. No parece aconsejable admitir en el estado actual de la tecnología consecuencias automatizadas sin intervención humana que las verifique y asuma la responsabilidad en el proceso de decisión, y siempre con una información muy precisa al paciente sobre el proceso que condujo a la obtención de un determinado resultado.

F. La publicación de resultados y la liberación de los datos deberían ser extremadamente cuidadosas con el cumplimiento normativo

Una interpretación adecuada del principio de protección de datos desde el diseño y por defecto, y de las previsiones del artículo 89.1 RGPD, obligan apostar por una anonimización bastante estricta en la publicación de los resultados. Este último precepto dispone que siempre que los fines propios de la investigación puedan alcanzarse «mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo». Por ello, sin perjuicio, de lo que se señala a continuación en materia de anonimización, está debería ser la opción más clara cuando se compartan datos en entornos abiertos.

3. Consentimiento: el compromiso del paciente y la comunidad. La investigación como finalidad legitimadora

El citado Informe sobre Big data en salud ha puesto de relieve la aparición de un nuevo modelo de paciente participativo[80]:

> El ePaciente es una persona que hace uso de los servicios de salud en condiciones plenas utilizando las TIC de manera eficiente y significativa. Los ePacientes reúnen información sobre su dolencia, su diagnóstico o su tratamiento y utilizan las TIC para tratar cualquier aspecto o preocupación por su salud y comunicarse con algún actor del sistema sanitario de una forma no física, a través de la consulta online y otros medios. Algunas de sus características más relevantes son:
>
> - El ePaciente quiere ser más participativo en la relación con su médico, está más comprometido y es mucho más activo, proactivo, partícipe y responsable, sobre todo a la hora de tomar decisiones. Habitualmente comparte su aprendizaje con otros pacientes.
> - El ePaciente está comprometido con su enfermedad; desea controlar lo que le sucede y para ello tiene en Internet una gran herramienta de información y asesoramiento.
> - El ePaciente a veces elige a su médico a través de las valoraciones u opiniones en Internet y, muy habitualmente, en las redes sociales.

80. SAN SEGUNDO ENCINAR, JOSE MARÍA (Dir.). *Big data en...* Op. Cit. Pág. 47.

- Otra de las prácticas habituales de los ePacientes es la de buscar información contrastada. Así, el 19% de los pacientes consulta estudios de facultativos sobre su enfermedad (Pew Internet, 2011).

En líneas parecidas, en el marco del grupo de trabajo sobre «Médicos y Pacientes» del Future Trends Forum dedicado a Big data se señalaba un elemento muy interesante:

> «Tanto para profesionales sanitarios como para pacientes la integración de estas tecnologías supone un cambio de cultura y de comportamiento y también del rol que juegan en la atención. **No solo se ve afectada la relación entre médico y paciente sino dentro de la familia y de la comunidad**. «El papel de las comunidades -tanto físicas como en internet- es un factor de cambio decisivo porque gracias a los datos pueden darse cuenta de que algo falla y pueden actuar para modificar comportamientos poco saludables de sus integrantes»»[81].

Desde un punto de vista sociológico parece evidente que el paciente del Siglo XXI en España será una persona familiarizada con las redes sociales y la tecnología. Que se interesa por las políticas preventivas en salud, aunque sea con la mera banalidad de usar un programa que mida cuanto camina al día, y que suele ser alguien que busca en internet información sobre las patologías. Por tanto, se trata de una nueva generación de usuarios de la sanidad receptivos a colaborar en investigación y cuyo compromiso con los valores comunitarios es fácilmente previsible en un país con las más altas tasas de donantes de órganos, sangre y médula. Parece de sentido común apostar por un diseño de la investigación en salud con Big data cimentado sobre la base del consentimiento informado[82] y el compromiso ciudadano.

4. El contexto de la anonimización

A lo largo de este trabajo se ha abordado el entendimiento normativo de la anonimización como una de las barreras más significativas para el uso de Big data en la investigación en salud. El regulador se ha preocupado que la exigencia del máximo rigor en esta materia se incorporase a las definiciones de la Ley 14/2007, de 3 de julio, de Investigación biomédica. Hemos concluido que en el enfoque del GT29, y de más de un colectivo de juristas, la anonimización es más un deseo que una realidad. Y por otra parte, la Guía de la Agencia Española de Protección de Datos sobre

81. FUTURE TRENDS FORUM: *Big data. El poder de los datos…* Op. Cit. Pág.40.

82. Como señala Antoinette Rouvroy, la transparencia debe ser máxima incluyendo información sobre si los datos serán anonimizados y si existe el riesgo de reidentificación. ROUVROY Antoinette: «Of Data and Men» *Fundamental Rights and Freedoms in a World of Big Data.* Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Council Of Europe, Strasbourg, 2016.

«Orientaciones y garantías en los procedimientos de anonimización de datos personales» no permite albergar grandes esperanzas en un cambio de criterio[83]. Tomemos dos ejemplos de la misma.

En primer lugar, el epígrafe 3.1 define el equipo de trabajo y recomienda tener en cuenta ciertos perfiles:

- Responsable del fichero y de la información.
- Responsables de Protección de Datos o Delegado de Protección de Datos o DPD (figura que establece el RGPD).
- 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.

Pero no se trata únicamente de recursos humanos. El Regulador en un trabajo técnicamente impecable señala que el proceso de anonimización es complejo y requiere de una pre-anonimización, una fase subsiguiente en la que eliminar o enmascarar las variables de identificación remanentes, el empleo de algoritmos de cifrado y sellos digitales, y a ser posible una anomización por capas. Por otra parte, al igual que el GT29 se incluyen y recomiendan técnicas como la generalización, adición de ruido, o la segregación de datos. Y de ser posible, hay que disponer en el mundo físico de metodologías de separación de los distintos *data set* que se vayan generando. En la práctica, esto conduce a un proceso de anonimización en dos fases en la que la pre-anonimización se realiza en origen, y la anonimización irreversible acudiendo a la contratación de terceros de confianza.

---

83. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. Madrid, 2016. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php.

Resulta muy interesante por su enfoque práctico orientado a salud U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES (HHS): *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, 2012. Disponible en https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

Y NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS: Letter to the Secretary – Recommendations on De-identification of Protected Health Information under HIPAA, 2017. Disponible en https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf

La disponibilidad de personal y recursos que ello exige resulta sencillamente inalcanzable para la investigación básica en la mayoría de las universidades de este país y me atrevería a decir que en gran parte de los hospitales y sistemas de salud. Así que, mientras que el Observatorio de Bioética y Derecho de la Universitat de Barcelona se permite cuestionar el recurso al sector privado en investigación en Big data en relación con el proyecto VISC+, las exigencias del regulador hacen insostenible el modelo para los grupos de investigación de tamaño reducido de las universidades públicas.

Y podría decirse, empleando una seguramente poco afortunada metáfora futbolística, que aquí el problema reside en que los reguladores «pitan el peligro». Desde la honestidad intelectual, debe reconocerse que se aceptan sin restricción alguna todas y cada una de las cautelas del GT29 y la AEPD cuando se trata de liberar datos disponibles para el conjunto de la comunidad científica. Aquí sin ninguna duda nuestra vara de medir debe coincidir con la del Considerando 26 de la Directiva y hay que actuar teniendo en cuenta las máximas capacidades de reidentificación de cualquier tercero.

Pero ¿qué sucede cuando la investigación no desborda los límites del hospital o de la relación contractual con un tercero? En tal caso, es cuando el aparato sancionador actúa de modo altamente disuasorio. Como ha demostrado el caso Omnium[84], para la Agencia Española de Protección de Datos que se traten materialmente o no los datos es irrelevante: basta con la mera identificabilidad. Es decir, en el marco de una investigación masiva con datos en salud un Hospital estaría incumpliendo la LOPD y el RGPD si segrega los identificadores en una base de datos diferenciada, y genera con los datos de las historias clínicas un data set para investigación. Esto sería un supuesto de pseudonimización y al no haber aplicado garantías de irreversibilidad sería absolutamente irrelevante si se reidentifica o no. La cuestión es que en este modo de entender la anonimización puede caerse con enorme facilidad en un tipo infractor muy grave consistente en tratar datos especialmente protegidos sin consentimiento del afectado de modo puramente objetivo, sin culpa o dolo por parte de los responsables o investigadores.

Sin embargo, podría haber otro modo de entender esta cuestión. El Gobierno Obama presentó en al menos dos ocasiones un proyecto de ley

84. Procedimiento sancionador PS/00235/2015, instruido por la Agencia Española de Protección de Datos a las entidades
ASSEMBLEA NACIONAL CATALANA y ÒMNIUM CULTURAL. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2015/common/pdfs/PS-00235-2015_Resolucion-de-fecha-18-11-2015_Art-ii-culo-7.2-9-LOPD_Recurrida.pdf.

de protección de datos, el «Consumer Privacy Bill of Rights Act»[85]. En la versión de anteproyecto del Gobierno de 2015, -«Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015», se incluía una interesante excepción al concepto de dato personal:

> (2) Exceptions.—
>
> (A) De-identified data.—The term «personal data» shall not include data otherwise described by paragraph (1) that a covered entity (either directly or through an agent)—
>
> (i) alters such that there is a reasonable basis for expecting that the data could not be linked as a practical matter to a specific individual or device;
>
> (ii) publicly commits to refrain from attempting to identify with an individual or device and adopts relevant controls to prevent such identification;
>
> (iii) causes to be covered by a contractual or other legally enforceable prohibition on each entity to which the covered entity discloses the data from attempting to link the data to a specific individual or device, and requires the same of all onward disclosures; and
>
> (iv) requires each entity to which the covered entity discloses the data to publicly commit to refrain from attempting to link to a specific individual or device.

Es decir cuando existe un compromiso público de no reidentificación aplicando los debidos controles para evitarla, -por ejemplo cuando se adoptan medidas para en el seno de una institución los investigadores no puedan acceder al *data set* que contiene los datos de identificación-, o cuando la ley o un contrato prohíben la reidentificación, sencillamente, se presume que de acuerdo con la buena fe a nadie se le ocurrirá identificar a los afectados. Por tanto, en un escenario de este estilo, el tipo infractor sólo se perfeccionaría cuando exista una conducta que en un plano volitivo o material tuviese por objeto reidentificar. Y en tal caso, la función protectora del derecho fundamental a la protección de datos no se vería menoscabada y a la vez sería posible el uso de datos disociados con fines de investigación bajo estándares más accesibles a los operadores.

85. La Administración Trump ha eliminado prácticamente todo rastro de las propuestas del Gobierno Obama. Ello obliga a remitir al lector a fuentes en ocasiones secundarias. Sobre el anuncio de esta iniciativa véase, https://www.whitecase.com/publications/article/white-house-re-introduces-consumer-privacy-bill-rights-act. Respecto del anteproyecto debe acudirse a https://assets.documentcloud.org/documents/1678354/cpbr-act-of-2015-discussion-draft.txt y en lo relativo al proyecto finalmente tramitado, https://www.congress.gov/bill/114th-congress/senate-bill/1158/text#toc-id403c8e008cb24c28a0e6e69704034837.

No obstante, conviene ser rigurosos y subrayar que las medidas de seguridad deberían ser suficientes y altamente exigentes, y que el estándar alto de anonimización se mantendría cuando se liberasen datos a la comunidad científica.

5. Políticas públicas, Big data e investigación en salud

A lo largo de este trabajo, se han abordado de modos muy distintos las barreras que la normativa puede plantear a la investigación con datos masivos de salud. A costa de reiterar argumentos, resulta interesante reproducir las consideraciones identificadas en un evento de Future Trends Forum sobre salud digital antes citado[86]:

> ¿Estamos dispuestos a facilitar nuestros datos personales y sanitarios?
>
> Actualmente, la legislación vigente en materia protección de datos no permite utilizarlos. En este sentido, uno de los grandes retos de la sociedad es obtener un marco regulador válido para el uso de Big data en el ámbito sanitario.
>
> Para Michal Rosen- Zvi, los médicos comprometidos con el juramento hipocrático, deben ofrecer siempre los mejores cuidados al paciente. «Esto significa que, si hay que ofrecer lo mejor, hay que hacerlo con cualquier método o tecnología que sea posible».
>
> (...)
>
> Sara Chan afirma categórica que «los datos salvan vidas» y que el valor del Big data para la salud de las personas es innegable «saber cuántas veces abres la nevera puede servir a las decisiones médicas».
>
> Pero al mismo Chan advierte de que «el manejo de toda esa información exige un contrato social porque lo que cada persona hace con sus datos, afecta a otros y es un asunto ético, y es importante saber cómo se gestionan los beneficios que pueden tener para la investigación, para qué y para quién se investiga, quién tiene el control».

Los expertos en privacidad deben abordar esta materia con extremo cuidado. Las herramientas jurídicas son muy limitadas y la dificultad en el enfoque máxima. Para empezar, la propia consideración de la anonimización como garantía y herramienta de exclusión de la aplicación de la normativa sobre protección de datos, ha sido puesta en cuestión por el

86. FUTURE TRENDS FORUM: *Salud digital.* Op. Cit. Págs. 32 y 33.
Para Noemí Brito la clave está en balancear innovación, competencia y protección de los derechos de las personas. Véase BRITO, Noemí: «Acceso, privacidad y ética pública en la era del big data, en VV.AA: *Manual sobre utilidades del big data para bienes públicos.* Entimema, Madrid, 2017, pág. 90 y ss.

Working Party cuyo Dictamen 05/2014 sobre técnicas de anonimización apunta a la imposibilidad de anonimizar. Por otra parte, se detectan reticencias en la colaboración con el sector privado que no pueden resultar adulteradas por el sesgo ideológico del investigador o el experto que las analice. Y finalmente, debemos plantearnos si el aparataje jurídico disponible resulta suficiente.

Nuestra tarea será crucial. Si la comunidad profesional, o el regulador, aborda esta materia desde el rechazo situará una vez más a España en el contexto del territorio hostil, en un lugar en el que no instalarse ni actuar. Si por el contrario se adopta una óptica laxa podríamos caer en algo peor, en el sacrificio de los derechos fundamentales.

Es el momento del análisis riguroso para el despliegue de políticas públicas capaces de hacer compatibles la privacidad, la investigación científica, la mejora de los sistemas de salud. Y hay que hacerlo sin posiciones apriorísticas, conciliando todos los intereses en presencia y desde el conocimiento de la realidad.

Por tanto, se impone un análisis profundo centrado en el conocimiento preciso de la realidad social, tecnológica y científica que permite una aproximación centrada en el caso que provea de soluciones operativas. En Big data ya no estamos ante el fácil expediente ludita o maniqueo del sí o del no, del bueno o del malo, nos enfrentamos ineludiblemente al reto de explicar «el cómo», y ésta es nuestra incómoda y apasionante responsabilidad.

Bibliografía

• AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. Madrid, 2016. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php.

• BUTLER Declan: «When Google got flu wrong» en *Nature News*, volume 494.

• BRITO, Noemí: «Acceso, privacidad y ética pública en la era del big data, en VV.AA: *Manual sobre utilidades del big data para bienes públicos*. Entimema, Madrid, 2017.

• CASADO María, DO CÉU PATRÃO NEVES, Maria, DE LECUONA Itziar, CARVALHO Ana Sofia, ARAÚJO Joana: *Declaración sobre integridad científica en investigación e innovación responsable*. Edicions de la Universitat de Barcelona, Barcelona-Porto, julio de 2016, págs. 49 a 51.

• CAVOUKIAN Ann: *Privac y by Design Los 7 Principios Fundamentales*. Comisionada de Información y Privacidad Ontario, Canadá, 2011.

• CABALLERO, Rafael y MARTÍN, Enrique: *Las bases de Big Data*. Catarata, Madrid, 2015.

• CATTELL Jamie, CHILUKURI Sastry y LEVY Michael: «How big data can revolutionize pharmaceutical R&D» en *McKinsey Center for Government*, octubre 2013. Disponible en http://www.mckinsey.com/industries/pharmaceuticals-and-medical-products/our-insights/how-big-data-can-revolutionize-pharmaceutical-r-and-d.
• CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA: *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*. Council of Europe, Strasbourg, 2017.
• DE MONTJOYE Yves-Alexandre, RADAELLI Laura, KUMAR SINGH Vivek y PENTLAND Alex «Sandy»: «Unique in the shopping mall: in the reidentifiability of credit card metadata» en Science, 30 JANUARY 2015, VOL 347 ISSUE 622, págs. 536-539.
• EUROPEAN COMMISSION: Opinión núm. 26. Ethics of Information and Communication Technologies. Brussels, 2012. Pág. 61.
• FUTURE TRENDS FORUM: *Big data. El poder de los datos*. Fundación Innovación Bankinter, Madrid 2014. Disponible en https://www.fundacionbankinter.org/ftf/tendencias/bigdata.
• FUTURE TRENDS FORUM: *Salud digital*. Madrid 2016, Disponible en https://www.fundacionbankinter.org/ftf/tendencias/salud-digital.
• GEMO Monica, LUNARDI Davide y TALLACCHINI Mariachiara: *Wearable Sensors and Digital Platforms in Health: empowering citizens through trusted and trustworthy ICT technology. TRUDI Deliverable 3.1*. Scientific and Technical Research Reports Publications, Office of the European Union, 2015.
• GINSBERG Jeremy, MOHEBBI Matthew, PATEL Rajan, BRAMME Lynnetter, SMOLINSKI Mark S. y BRILLIANT Larry: «Detecting influenza epidemics using search engine query data» en *Nature* Vol 457, 19 February 2009, doi:10.1038/nature07634 http://dx.doi.org/10.1038/nature07634
• INFORMATION COMMISSIONER'S OFFICE: *Big data, artificial intelligence, machine learning and data protection. Version: 2.0*, ICO, 2017. Disponible en https://ico.org.uk/for-organisations/guide-to-data-protection/
• KAPLAN, Jerry: *Abstenerse humanos*. TEELL, Zaragoza, 2016, págs. 48 y 49.
• KAYYALI Basel, KNOTT David, y Steve KUIKEN Van: «The big-data revolution in US health care: Accelerating value and innovation» en McKinsey Healthcare Systems & Services Practice, junio 2013. Disponible en http://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/the-big-data-revolution-in-us-health-care.
• KELSEY Tim: «Blog NHS. (2015). Urgent action is a moral imperative». Disponible en https://www.england.nhs.uk/2015/09/tim-kelsey-11.

• LAZER David y KENNEDY Ryan: «What We Can Learn From the Epic Failure of Google Flu Trends» en *Wired Science*. Disponible en https://www.wired.com/2015/10/can-learn-epic-failure-google-flu-trends/
• LLÀCER, M.R., CASADO, M y BUISAN L (Coords.): *Documento sobre Bioética y Big data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*. Observatorio de Bioética y Derecho de la Universitat de Barcelona. Barcelona, 2015. Disponible en http://www.bioeticayderecho.ub.edu/es/documento-sobre-bioetica-y-big-data-de-salud-explotacion-y-comercializacion-de-los-datos-de-los
• MARJANOVIC Sonja, GHIGA,Ioana MIAOQING Yang and KNACK Anna: *Understanding value in health data ecosystems: A review of current evidence and ways forward.* Santa Monica, CA: RAND Corporation, 2017.Disponible en https://www.rand.org/pubs/research_reports/RR1972.html.
• MARTIN LINEROS, Eduard: «El trinomio dato-información-conocimiento» en VV.AA: *Manual sobre utilidades del big data para bienes públicos*. Entimema, Madrid, 2017.
• MARTÍNEZ MARTÍNEZ, Ricard: *Una aproximación crítica a la autodeterminación informativa*. Civitas, Madrid, 2004
• MARTÍNEZ MARTÍNEZ, Ricard: «El derecho fundamental a la protección de datos: perspectivas», en IDP: *Revista de Internet, Derecho y Política*, Nº. 5, 2007
• MARTÍNEZ MARTÍNEZ, Ricard: «Ética Ética y privacidad de los datos», en *Monográfico sobre Big Data de la Revista FRA* nº14 (Diciembre 2015), págs. 86-91.
• MARTÍNEZ MARTÍNEZ, Ricard: «Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos.», en *Revista Dilemata*, núm. 24, 2017, págs. 151-164. Disponible en http://www.dilemata.net/revista/index.php/dilemata/article/view/412000105
• MARTÍNEZ MARTÍNEZ, Ricard: «Protección de datos y desarrollo tecnológico en un mundo global», en el *BLOG LOPD y Seguridad*, Disponible en http://lopdyseguridad.es/proteccion-de-datos-y-desarrollo-tecnologico-en-un-mundo-global/.
• MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth: *Big Data*. Turner, Madrid, 2013.
• NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS: Letter to the Secretary – Recommendations on De-identification of Protected Health Information under HIPAA, 2017. Disponible en https://www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2017-Ltr-Privacy-DeIdentification-Feb-23-Final-w-sig.pdf
• PORTER, Michael E: «What Is Value in Health Care?» en *The New England Journal of Medicine*, December 23, 2010, págs. 2477-2481.
• PUYOL MONTERO, Javier: «Aproximación jurídica y económica al Big Data. Tirant lo Blanch, valencia 2015, págs. 285 y ss.

• ROMAÑACH CABRERO, Javier y ARNAU RIPOLLÉS, Soledad «La visión de la eugenesia en el mundo occidental» en CASABÁN MOYA, Enric (Ed.): *XVI Congrés Valencià de Filosofia*, Universitat de Valencia, València, 2006.
• ROUVROY Antoinette: «Of Data and Men» *Fundamental Rights and Freedoms in a World of Big Data*. Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Council Of Europe, Strasbourg, 2016.
• SAN SEGUNDO ENCINAR, JOSE MARÍA (Dir.). *Big data en salud digital*. Fundación Vodafone, MINETAD, RED.ES, Madrid, 2017.
• SERRANO, Mercedes: «Big data o la acumulación masiva de datos sanitarios. Derechos en riesgo en el marco de la sociedad digital» en *DS: Derecho y salud,* Vol. 25, Nº. Extra 1, 2015, págs. 51-64.
• SOTO, Yasmina: «Datos masivos con privacidad y no contra privacidad», en *Revista de Bioética y Derecho. Dossier Monográfico del XIII Congreso Mundial de la International Association of Bioethics*, núm. 40, 2017, págs. 101-114.
• U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES (HHS): *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, 2012. Disponible en https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html
• VAN DER GOOT Erik, TANEV Hristo y LINGE Jens P.: «Combining Twitter and Media Reports on Public Health Events in MedISys», en *International World Wide Web Conference,* Seul, 2014. Disponible en http://www2013.wwwconference.org/companion/p703.pdf

Resumen

El uso de Big data ha supuesto un cambio cualitativo profundo para la investigación en salud. Ofrece la oportunidad de explotar décadas de datos de millones de pacientes acumulados en las bases de datos de los sistemas de salud y explotar la información disponible para tareas como identificar patrones, simular experimentos y analizar grandes volúmenes de datos personales. Esta tecnología puede suponer un cambio de paradigma para la investigación en salud y la gestión de la sanidad, pero plantea interrogantes desde el punto de vista del derecho fundamental a la protección de datos. El artículo propone un foque proactivo que concilie los intereses en presencia y contribuya al desarrollo de la investigación en salud.
PALABRAS CLAVE: Big data, investigación, salud, protección de datos, privacidad, Reglamento general de protección de datos.

Col·laboren en este número:

Ainhoa Lasa López: Profesora Contratada Doctora de Derecho Constitucional y Vicedecana de Calidad y Políticas de Igualdad de la Universidad de Alicante.

Luis Manent Alonso: Abogado de la Generalitat en la Conselleria de Sanidad Universal y Salud Pública.

Ana Isabel Marrades Puig: Profesora Contratada Doctora de Derecho Constitucional de la Universitat de València.

Luis Alfonso Martínez Giner: Profesor Titular de Derecho Financiero y Tributario de la Universidad de Alicante.

Ricard Martínez Martínez: Director de la Càtedra Microsoft-Universitat de València sobre Privacidad y Transformación Digital. Doctor en Derecho.

Vicent Moreno i Baixauli i **Sandra Serrano i Mira**: President d'Escola Valenciana y Periodista.

Alba María Nogueira López: Profesora Titular de Derecho Administrativo, acreditada al Cuerpo de Catedráticos de Universidad de la Universidad de Santiago de Compostela.

Fernando de Rojas Martínez-Parets: Profesor Contratado Doctor de Derecho Administrativo de la Universidad Miguel Hernández de Elche.

Joaquín Tornos Mas: Catedrático de Derecho Administrativo de la Universidad de Barcelona y Abogado.

Francesc Xavier Uceda Maza: Delegado del Consell para el Modelo Social Valenciano. Vicepresidencia y Conselleria de Igualdad y Políticas Inclusivas.